IMail Server

User's Guide

Software Version 7.0

Ipswitch, Inc.

©1995-2001 Ipswitch, Inc. All rights reserved.

IMail Server 7.0 User's Guide for Windows NT/2000

This manual, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the expressed prior written consent of Ipswitch, Inc.

The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. also assumes no liability for damages resulting from the use of the information contained in this document.

IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products and their brands or company names, are or may be trademarks or registered trademarks, and are the property of their respective companies.

The following are copyrights of their respective companies or organizations: The spelling portions of this product are the property of WinterTree Software, Dictionary Copyright © 1999 Wintertree Software Inc.; code derived from RSA Data Security, Inc. MD5 Message-Digest Algorithm, All rights reserved Copyright 1991-2 RSA Data Security, Inc.; SSL implementation in this product is based on the SSLeay libraries written and copyrighted by Eric Young (eay@cryptsoft.com) crypto/cryptlib.c Copyright 1995-1998. Portions of the implementation are copyrighted by RSA Data Security, Inc. All rights reserved. This product also includes software written by Tim Hudson(tjh@crytpsoft.com).

Printing History

March 1995	First Editon
March 1996	Second Edition
August 1996	Third Edition
June 1997	Fourth Edition
January 1999	Fifth Edition
December 1999	Sixth Editon
January 2000	Seventh Edition
June 2001	Eighth Edition

Ipswitch, Inc.
81 Hartwell Ave
Lexington, MA 02421-3127

http://www.ipswitch.com
Phone: 781-676-5700
Fax: 781-676-5710

Contents

Preface . . . . . **xiii**
What This Package Includes xiv
The Ipswitch Products xiv
Visit Our Web Site xvi
Please Send Us Your Comments xvi
Getting Technical Support xvi
Downloading Patches and Upgrades xvi

Chapter 1: Overview **1**
What is IMail™ Server? 1
Introduction 1
Licensing Options 2
System Requirements 2
New in Version 7.1 2
Services 2
User Interface 2
Web Messaging 3
Features 3
User Interface 3
Services 3
Web Messaging Administration 4
Web Messaging Enhancements for Users 4
IMail Web Calendaring 5
Basic Services 5
SMTP 5
SMTP Security 5
POP3 6
IMAP4 6
Web Messaging 7
Web Calendaring 7
Additional Services 8
Standard Features 10
User Registration and Maintenance 10
Mailing List Creation and Maintenance 10
Mail Forwarding 11
Vacation Support 11
Finger “Plan” Support 11
Mail Delivery Rules 11
Automated Mail Accounts 11
Multiple Host (Domain) Support 12
Privacy-Enhanced POP Support 12

Forwarding of Mail to a Beeper or Pager 12
Unknown Local User Processing. 12
Anti-spamming Features 13
Optional Capabilities 13
IMail Client for Windows. 13

Chapter 2: Installation 15
Before You Begin. 15
Checking Your Primary Host Name 15
User Registration and Authentication 16
Installing IMail Server for the First Time. 17
Installation Procedure 17
Root User ID. 19
Performing an Initial Setup and Test 20
Sending and Receiving Mail in a Test Account 22
Viewing the Basic IMail Server Configuration 23
General Properties 24
The Mail Queue 25
A Quick Look at IMail Server Services. 25
Verifying Services 26
Default Service Ports 26
The IMail Server Directory Structure. 27
Upgrading 28
Upgrading Using External Databases 29
Upgrading Web Messaging 29
Re-Installing IMail Server to a Different Location 30
Removing IMail Server 30

Chapter 3: Configuration 33
Basic Configuration 33
Advanced Configuration. 33
Checking Configuration of the Primary Mail Host 34
Setting Up DNS for the Primary Mail Host 35
Setting Up an Alias for a Mail Host 36
Adding an Additional Mail Host 36
Virtual Hosts with IP Addresses 37
Virtual Hosts Without IP Addresses 37
Configuring a Virtual Host 38
Additional Host Settings 41
Setting Up DNS for Multiple Mail Hosts 43
Changing the IP Address of a Domain 44
Setting Up IMail Server as a Mail Gateway. 45
Setting up a Dial-up Internet Connection 46
Receiving Mail from an Internet Service Provider 46

Setting Up the Server for Dial-up Access 47
Setting Up IMail Server as a Backup Mail Spooler 50
Setting Up "Peer" IMail Servers 51
How Peering Works 51
Setup Procedure 52
Example of Setting Up Peer Servers 53
Using ETRN to Retrieve Mail 54
Adding a Host Based on an External Database 55
Configuring the Primary Host 56
Creating a Host Based on an External Database 56
Configuring the External Database Interface 57

Chapter 4: User Mail Accounts 59
Working with User Mail Accounts 60
Adding User Mail Accounts 60
Importing NT Users 63
Deleting a User Mail Account 64
Finding Orphan Mail Accounts 64
Setting Defaults for New Users 65
Working with Mailboxes 66
Combining Mailbox Names with User IDs 68
Setting Up a Finger Plan 69
Setting Up a Vacation Message 70
Setting Up a Basic Vacation Message 70
Viewing the List of Sender E-mail Addresses 71
Clearing the List of Sender E-mail Addresses 71
Sending a Message in Response to Every E-Mail 71
Entering LDAP Directory Information (Attributes) 72
Forwarding Mail to Another User Account 73
Applying User Settings to Other Users 74
Global Settings for Existing Users 75
Disabling an Entire Domain 75
Adding, Modifying, and Deleting Aliases 75
Types of Aliases 76
Adding an Alias 76
Processing Mail to Users That Don't Exist 79

Chapter 5: Mail Processing Techniques 81
Processing Order 81
Setting Up Delivery Rules 83
Examples 83
Rules Processing 84
Creating an Inbound Delivery Rule 85
Creating an Outbound Delivery Rule for a Host 88

Adding Multiple Conditions to Rules 91
Order of Rules 92
Testing a Delivery Rule 92
Rule Syntax 93
Determining Which Rule Trapped a Message 96
Commonly Used Rule Examples 97
Storing Search Text in External Files 99
Limitations 101
Using the Info Manager 101
Using the Info Manager for a Single Automated Response 101
When to Use a Sub-divided Info Manager Account 103
Sub-areas and Mailboxes 104
Sub-dividing an Info Manager Account 104
Notes about Forwarding 105
Disabling the Info Manager 105
More About the Info Manager 105

Chapter 6: IMail Web Messaging 107
What is Web Messaging? 107
What Can Users Do with Web Messaging? 108
System Requirements 110
Upgrading 110
Web Messaging Security 111
Setting Up Web Messaging 112
Web Address for the Web Messaging Server 112
If You Have Multiple Mail Hosts 112
Using Secure Sockets Layer (SSL) 113
Troubleshooting SSL 116
Configuring the Web Server 117
Advanced Tab 119
Setting Access to Web Messaging Functions 122
Using Remote Administration Functions 123
User Administration 124
Alias Administration 124
List Administration 124
Viewing Monitor Logs and the Spool Directory 124
Managing Virtual Hosts 125
Managing Mailing Lists 125
Setting Rules 125
Editing News of the Day and Welcome Message 125
Spell Checker 125
Installing Dictionaries For Domains 125
Enabling Spell Check 126

Accessing Spell Check 127
Disabling Spell Check 127
Editing Dictionaries 127
Dictionary Explanations 128
The dictionary files are word lists that are in a compressed file format and are not editable.
The user dictionary is editable. 128
Displaying Online Advertisements 129
Customizing Web Messaging 130

Chapter 7: IMail Web Calendaring 131
What is IMail Web Calendaring? 131
What Can Users Do with IMail Web Calendaring? 132
System Requirements 133
IMail Web Calendaring Security 133
Setting Up IMail Web Calendaring 134
Web Address for the IMail Web Calendaring Server 134
If You Have Multiple Mail Hosts 135
Using Secure Sockets Layer (SSL) 135
Starting an SSL Connection from a Browser 138
Configuring the Web Calendaring Server 138
Setting Access to IMail Web Calendaring 141
Invitations 143
Sending E-mail Invitations 143
Viewing Invitations 143
Accepting Invitations 143
Declining Invitations 143
Displaying Online Advertisements 143
Customizing IMail Web Calendaring 145

Chapter 8: SMTP Server 147
SMTP RFCs Supported 147
Basic Information 147
Logging On 148
Configuring the SMTP Server 149
SMTP Options 149
Using a Remote Mail Gateway 151
Advanced Options 151
SMTP Security 152

Chapter 9: Security and Antispamming 153
Background on SMTP Protocol Security 153
Security Strategies 154
Mail Relay Options 154
Validating Incoming Mail 155

Access Control Options 156
Changing the SMTP Welcome Message 156
Setting SMTP Security Options 156
Setting Mail Relay Options 157
Setting Access to Local Mail Groups 161
Validating Incoming Mail 162
Setting Access to the SMTP Server 163
Copying Inbound and Outbound Mail 164

Chapter 10: POP3 Server 165
Logging On 165
Configuring the POP3 Server 166
Logging Options 167
Other Options 167
Advanced Options 168
To change the Welcome Message for POP3: 168
Setting Access to the POP3 Server 168

Chapter 12: LDAP Server 171
The IMail Server LDAP Implementation 171
Full LDAP Directory Support 173
Supplying LDAP Information for Unregistered Users 173
Accessing LDAP Information from Microsoft Mail Clients 173
Populating the LDAP Database 174
Logging On 174
Configuring the LDAP Server 175
Logging Options 176

Chapter 11: IMAP4 Server 177
The IMail Server IMAP4 Implementation 177
IMAP4 Server Support 177
Full IMAP4 Client Support 178
Mailbox Management 178
Public Mailboxes 179
Logging On 179
Configuring the IMAP4 Server 180
Logging Options 181
Advanced Options 181
To change the Welcome Message for IMAP 4: 182

Chapter 13: Whois Server 183
Logging On 183
Configuring the Whois Server 184

Chapter 14: Finger Server 187
Logging On 187
Configuring the Finger Server 188
Logging Options 189

Chapter 15: Password Server 191
Configuring the Password Server 191
Logging Options 192
Logging On 192

Chapter 16: The Monitor Server 195
Configuring the Monitor Server 196
Changing Monitor Settings in the Control Panel 198
Working with Notifications 199
Defining Any Type of Notification 199
Defining Beeper Notifications 200
Using an External Beeper Program 202
Defining Pager Notifications 202
Defining E-mail Notifications 205
Putting a Notification on the Notifications Tab 206
Enabling Notifications 207
Disabling Notifications 208
Configuring the Web Administration Capability 208
Setting Access to Web Administration 209
Using the Web Administration Capability 210
Personal Account Options 212
System Administration 212
Host Administration 213

Chapter 17: List-Server Mailing Lists 215
Features 215
Types of List-Server Mailing Lists 216
Using Passwords and Posters Lists 216
Open Lists (Anyone Can Post) 216
Subscriber Lists 217
Moderated Lists 217
Posting to a List 218
Using a Password 218
Requesting Information and Subscribing 218
Format of Requests 219
Commands for Requesting Information 219
Commands for Subscribing and Unsubscribing 220
Commands for the Use of Subscribers 220
Commands for the Use of the List Owner (or Moderator) 220

How the List Server Works 221
Creating a List-Server Mailing List 221
Setting Advanced Options 224
Setting Security 226
Setting Up Digest Mode 228
To set up digest mode for a list-server mailing list: 229
Digest Scheduling 230
Adding and Removing Subscribers and Unknown Users 231
Setting Up an Alias to Remove an Unknown User 231
Setting Up an Alias to Delete a User by Forwarding 232

Chapter 18: Sending Mail to a Pager or Beeper 235
Adding a Beeper or Pager Alias 235
Defining a Pager Alias 236
Defining a Beeper Alias 236
Sending a Message to a Pager/Beeper 237
"Forwarding" a Message to a Pager 237
Sending a Message to a Beeper When Mail Arrives 237

Chapter 19: IMail Administrator Remote Connection Capability 239
Requirements for Connection 239
Password Server Setup 239
Connecting to a Remote Server 239
Connecting Back to the Local Machine 240

Chapter 20: Mail to Fax 241
Installing IMail Fax Support 241
Setting the Modem Port 242
Adding a "Mail to Fax" Alias 243
Creating and Modifying Fax Cover Pages 245
Setting Up and Using Dynamic Dialing Aliases 246
Setting Global Properties for All Dynamic Aliases 248
Setting Access and Dialing Restrictions 249
Sending Mail to a Fax Alias 252
Attachments 252
Sending Mail to a Dynamic Dialing Alias 253
Viewing the Fax Queue Files 253

Appendix A. File Locking 255

Appendix B. Backups 257
Backing Up the IMail Server Configuration 257
Using IMail Administrator to Back Up the Registry 257
Using a Command Line Utility 257

Using Regedit 258
Backing Up IMail Server System Files 258
Backing Up User Mail 258

Appendix C. Command Line Applications 259
Adding Aliases (addalias.exe) 260
Basic Command Syntax 260
Adding an Alias to the Default Domain 261
Adding an Alias to a Specific Domain 261
Deleting an Alias 261
Importing a Windows NT Group as a Group Alias 261
Return Codes 261
Using a Text File 261
Adding Virtual Hosts (adddomain.exe) 262
Basic Command Syntax and Example 262
Adding Users (adduser.exe) 263
Basic Command Syntax 263
Adding a User ID 265
Deleting a User ID 265
Return Codes 265
Using a Text File 265
Disabling Web Options 266
Sample File 266
Sending Mail (imail1.exe) 267
Command Syntax 267
Deleting Old Messages (immsgexp.exe) 268
Basic Command Syntax 268
Example 268
Populating the LDAP Database (ldaper.exe) 268
Basic Command Syntax 268
Sending Mail to All Users (mailall.exe) 269
Basic Command Syntax 269
Examples 269
Backing Up IMail Server Configuration (regback.exe) 270
Basic Syntax Command 270
Delivering Mail (smtp32.exe) 270
Processing Rules for smtp32 (and imail1) 271
Cleaning the Spool Directory (isplcln.exe) 272
Basic Command Syntax 272
Example 272

Appendix D. Spool, Queue, and Log Files 273
Files in the Queue 273
Beginning Character in File Name 273

File Extensions 274
Attachments 275
Troubleshooting 275
Log Files 275
The Log Files 275
Typical Log Files 276
Large Log Files 277
Disabling Logging 277

Appendix E. Default Registry Values 279
Global Settings 279
Finger Server 279
IMAP Server 279
LDAP Server 280
Password Server 280
POP3 Server 280
SMTP Server 281
Whois Server 281

Appendix F. Special Registry Values 283
Deleting an IP Address No Longer in Use 283

Appendix G. Changing the Look and Feel of Web Messaging. 285
Web Files and Web Directory Structure 285
Web Directories for Multiple Hosts 287
Changing Text, Background Colors, Buttons, and Logos 287
Editing the Welcome Message 288
Editing the News of the Day 288
Changing Button Labels 288
Customization Using the butontxt.ini File 289
Changing Text in Messages 289
Using Files with Multiple Hosts 289
Editing Web Templates 290
Web Templates and Their Associated Web Pages 290
Customizing a Web Page 291
Which Pages Use Which Templates 292
E-mail Web Pages 292
Personal Information Web Templates 293
Administrator Web Templates 294
Help Pages 296
IMail Tags 298
Tag Syntax 299
Types of Tags 299
ParseExtensions 300

ParseExtensions Directory Location 300
Adding ParseExtensions to the Registry 301
List of graphic files in the Web Directory. 301

Appendix H. Changing the Look and Feel of Web Calendaring. 303
Web Files and Web Directory Structure 303
Web Directories for Multiple Hosts 304
Changing Text, Background Colors, Buttons, and Logos 305
Editing the News of the Day 305
Changing Buttons 306
Using Files with Multiple Hosts 306
Editing Web Templates 306
Web Templates and Their Associated Web Pages 306
Customizing a Web Page 307
Which Pages Use Which Templates 308
Calendar Web Pages 308
Help Pages. 309
IMail Tags 311
Tag Syntax. 311
Types of Tags 312
List of Graphic Files in the Web Directory 312

Appendix I: Mail Servers and the DNS 315
What is DNS?. 315
How the Mail Server Uses DNS 316
Setting Up Mail Server Records in the DNS 317
Your Local Network's DNS server. 317
Example of a Basic Configuration 318
Sample DNS Records 320
Other Configurations. 320

Glossary 321
Index 329

Preface

IMail Server is an electronic mail server system that is based on Internet standards and runs on Microsoft Windows NT/2000. IMail Server provides Simple Mail Transfer Protocol (SMTP) for sending and receiving mail over the Internet or over an internal TCP/IP network.

IMail Server supports any mail client that uses the Post Office Protocol, Version 3 (POP3) or Internet Message Access Protocol (IMAP4). Web Messaging lets users access their mail from any web browser; they do not need to have a mail client. Additionally, users can now use Web Calendaring to store schedules, set appointments, and receiving date reminder information all in one location.

IMail Server is self-monitoring — a monitor server lets you monitor SMTP, POP3, IMAP4 and other services, receive notification when a service is down, and automatically restart the service. IMail Server also includes a list server for creating and managing mail discussion groups, as well as servers for LDAP, Finger, and Whois information.

The Web Administration capability of the Monitor server lets the system administrator monitor the IMail Server system using a web browser on any remote system and perform system maintenance functions. It also allows users to change their user settings from a web browser.

The Mail to Pager/Beeper capability can forward messages to a pager, or notify you by beeper that mail has arrived.

As an option, you can purchase a Mail to Fax add-on. For more information, see “Optional Capabilities” on page 13.

What This Package Includes

IMail Server includes the following:

- A CD-ROM containing:
  - The IMail Server installation program, which installs the complete IMail Server software
  - Web Messaging, Web Calendaring and Mail to Pager/Beeper applications
  - One IMail Client.
  - An evaluation copy of WS_Ping ProPack.
  - License agreement
- This manual, the *IMail Server User's Guide.*
- The *IMail Server Getting Started Guide*.

The Ipswitch Products

Other Ipswitch products include:

- **IMail Server Mail to Fax**

  IMail Server's Mail-to-Fax Option is an add-on (not included in base price) that allows system administrators to create special aliases that route messages directly to a fax machine. This option allows ISPs, for example, to set up e-mail accounts for customers who do not have a PC or Internet access and want to receive e-mail messages via a fax machine. With this option, other users could send fax messages from their desks by sending e-mail to a special account on a local server that faxes it to the recipient.

- **WhatsUp™ Gold Network Monitoring Tool**

  WhatsUp Gold is a graphical network monitoring system designed for today's multi-protocol enterprise networks. It monitors critical devices, applications, services, and initiates visual or audible alarms along with a choice of pager, beeper, e-mail or voice notifications.

Its LogManager and SNMP Viewer provide easy troubleshooting and real-time monitoring of utilization levels. Performance reports show historical trends for resource capacity planning. WhatsUp Gold also comes with a built in web server and can be administered for any standard web browser.

- **WS_FTP™ Pro FTP Client**

  WS_FTP Pro is a Windows-based file transfer client application that is used to transfer files between your local PC and a remote FTP server.

  WS_FTP Pro provides two powerful Windows interfaces for connecting to remote hosts and transferring files. SSL encryption protects your valuable information when you connect to an SSL compliant FTP server. This keeps your confidential information secure during transfer over the Internet.

  The Scheduling feature lets you schedule your queued jobs to transfer files on the dates and times you choose.

  The “Bonus Utility Pack” that ships with WS_FTP Pro 6.0 includes the WS_FTP Find Utility, the WS_FTP Scripting Utility, and the WS_FTP Synchronize Utility.

- **WS_FTP Server**

  WS_FTP Server is a full-featured FTP server for Windows NT/ 2000 systems. WS_FTP Server lets you create FTP sites that make files and folders on your PC available to other users. WS_FTP Server offers many features not found in most commercial servers today, including automatic resumption of interrupted transfers.

  SSL encryption protects your valuable information while it is being transferred over the Internet, when you connect with an SSL compliant FTP client

  Customized Site Commands simplify server and data management. Administrators can now automate routine tasks with custom scripts that reside on the server and can be activated remotely through the WS_FTP Client.

  WS_FTP Server can automatically create FTP accounts for IMail Server users if IMail Server is installed on the same system as WS_FTP Server

- **WS_Ping Pro Pack™**

  WS_Ping ProPack is the ultimate network information tool. It provides everything you need to help track down network problems and to get information about users, hosts, and networks on the Internet or on your intranet. Tools include Info, Time, HTML, Ping, Traceroute, Lookup, Finger, Whois, LDAP, Quote, Scan, SNMP, WinNet, and Throughput.

Visit Our Web Site

For more information about Ipswitch products, to find evaluation versions, or to purchase our products online, visit the Ipswitch web site at: *http://www.ipswitch.com.*

On our technical support pages, you can view the Knowledge Base of technical information about our products and keep up-to-date on product news.

Browse through our Web Messaging Template gallery to get a different look and feel for Web Messaging. You can also visit our user created utilities page for a list of useful programs.

Please Send Us Your Comments

We welcome your feedback on this product and its documentation. Please send your comments and suggestions to the following e-mail address: *feedback@ipswitch.com*.

Getting Technical Support

E-mail support is always available for the current version. A service agreement is required for telephone support beyond the warranty period, and for major upgrades. For more information about Ipswitch Technical Support and service agreements, go to the Ipswitch web site at *www.ipswitch.com/support/index.html***.**

Downloading Patches and Upgrades

If a software patch is created to fix a bug in the currently shipping

version of a product, Ipswitch will make the patch available on our web site.

Product upgrades to extend capabilities are also made available on our FTP and web sites. A valid service agreement for IMail Server includes major product upgrades for twelve months.

Check our web site for current software patches and upgrades. To download software from the Ipswitch web site:

1 In your web browser, go to:*www.ipswitch.com/support/patches-upgrades.html.*

2 Read the introductory information about patches and upgrades at the top of the page.

3 Under **IMail Server**, click the appropriate link.

4 Follow the instructions on your screen.

Chapter 1: Overview

This chapter introduces IMail Server and describes its components, capabilities, and major features. In addition, you will find system requirements and an introduction to new and enhanced features.

Note

For updated information since this manual was printed, see the Release Notes (*Ntimsvc.txt)* located in the IMail top directory.

What is IMail™ Server?

IMail Server is a comprehensive electronic mail solution designed for today's evolving Internet and corporate intranet messaging requirements. Easy to install and administer, IMail Server significantly reduces both the initial cost of mail implementation and the on-going cost of administration. Its easy-to-use features improve productivity and provide a robust alternative to proprietary systems or complicated UNIX-based Internet mail.

Introduction

IMail Server provides:

- Up to 250 user accounts, up to 1000 user accounts, or unlimited user accounts (depending on license)
- Full integration with the Windows NT/2000 user database
- Ability to base user mail accounts on an external database

IMail Server e-mail can be read with:

- Any POP3 mail client
- Any IMAP4 mail client
- Any web browser

This Internet standards based client/server architecture provides system administrators with complete flexibility in setting up a total mail solution that easily accommodates disparate and/or geographically dispersed mail clients.

Licensing Options

IMail Server offers several licensing options. Licensing is available in the following three configurations:

- Up to 250 users
- Up to 1,000 users
- Unlimited users

System Requirements

IMail Server is designed for the Windows NT/2000 operating system. It is *not* compatible with Windows 95, Windows 98, or Win32s.

The system requirements for IMail Server are:

- Intel (Pentium processor or higher)
- Microsoft Windows NT 4.0 (SP1) or higher; Windows 2000, including Pro, Server and Advanced Server.
- Network interface card installed and configured to use Microsoft's TCP/IP for Windows NT/2000 OR a dial-up TCP/IP connection
- 200 MB disk space (for a 30-user workgroup)
- At least 32 MB of memory (64 MB is recommended)
- A static IP address.

It is recommended that the NTFS (rather than FAT) file system be used for increased operability and security.

New in Version 7.1

Services

- New "Advanced" tabs for IMAP, POP3 and SMTP, contain options that were previously only accessible through the registry, such as welcome messages.

User Interface

- Sub-mailbox settings allow administrators to decide what to do with mail that is addressed to a sub-mailbox. Administrator's can choose to create the sub-mailbox, bounce the message, or send it to the user's Inbox. This setting is configurable per domain.

- Administrator's can limit the size of outgoing messages.
- Users and Administrators will now be notified through e-mail when their mailboxes are near capacity.
- Improved inbound delivery rules, and the ability to create outbound delivery rules for a host. All rules support multiple conditions.
- A new X-IMail-Rule line is placed in the header of all locally delivered messages that are captured by a rule to identify which rule caught the message.
- If you have IMail Anti-Virus Server installed, you can enable/disable virus scanning, per domain, in IMail Administrator and in IMail Web Messaging.

Web Messaging

- Web Messaging now supports 128 bit SSL.
- Enhanced Web Messaging templates that support inbound and outbound rules, multiple conditions, sub-mailbox creation settings, and advanced SMTP options.
- Fifteen new dictionaries for use with the Spell Checker.

Features

User Interface

- Web Calendaring utility, which is accessible through any browser.
- Remote management console provides for connections to remote IMail servers.
- Web Options tab for each host, provides domain level management of SSL, IMail Web Calendaring and the Spell Checker. This allows administrators to enable these features per domain rather than globally.

Services

- SSL authentication and user lockout policies create a secure method of sending and receiving e-mail.
- Determination of whether an incoming message is too large is based on *total* size of *all* mailboxes in a user's account.
- Support for APOP authorization when user logs on to their mail

account (or into a sub-mailbox) using POP3.

- For monitoring of services, the administrator can set the time-out value, in addition to how often to check the service.

Web Messaging Administration

- Security options allow flexibility in managing user security levels. Administrators can either force users to use SSL, give users the option of using SSL, or not provide the option at all. For added security, IMail Server can temporarily suspend a user if they fail a login too many times.
- Ability to modify Web Messaging templates.
  - Template set with *.gif* and .cgi files; old template set still supported.
  - Support for “include” tags that let you include a file in your web templates.
  - Support for definable button text (butontxt.ini) for different domains.
- ParseExtensions utility provides the ability to include IMAIL tags in your personal files. Use ParseExtensions to parse the IMail tags for any included file, regardless of its file extension.
- Web Messaging allows an administrator to view server statistics and real-time server activity, such as the number of users logged in, and the amount of data sent and received.
- Uses Cascading Styles Sheets (CSS) in order to provide easily alterable font styles, and quick click features. The HTML code follows DOM level 1 specs, and CSS level 1 specs.

Web Messaging Enhancements for Users

- Spell checking capability.This feature is available on the Compose, Reply-To, Forward and Draft pages.
- Link to IMail Web Calendaring enables users to open a calendar without logging in again.
- Support for mailbox searching in To/From/Subject/Content in a selected mailbox or all mailboxes. The results of the most recent search are preserved.

IMail Web Calendaring

- Ability to keep a schedule — including events, tasks and notes.
- E-mail invitations to others are sent to invitees when event is added, cancelled or modified.
- E-mail reminders
- Link to IMail Web Messaging enables users to access their mail accounts without logging in again.

Basic Services

IMail Server consists of a number of services that run on Windows NT/2000. The basic service that enables the Windows system to send and receive mail is the Simple Mail Transfer Protocol (SMTP). The services that allow access to mail by client systems are Post Office Protocol Version 3 (POP3) and the Internet Message Access Protocol Version 4 (IMAP4).

SMTP

The SMTP server sends and receives mail from other Internet hosts using the Simple Mail Transfer Protocol (SMTP). The SMTP server processes all incoming and outgoing mail. Outgoing mail is spooled until the SMTP server can confirm it has arrived at its destination. Incoming mail is spooled until users access it by using a POP3 or IMAP4 mail client. Spooling allows the transfer from client and server to occur in the background.

SMTP Security

IMail Server provides support for alternate SMTP, POP3, and IMAP4 authentication methods to provide a more secure means of sending user IDs and passwords across networks. This allows users to send mail from an IP address that has not been identified to IMail Server.

You also have the ability to control access to the SMTP server, by specifying an IP address or set of IP addresses that are either granted or denied access. This is useful when you know the IP Address of a mail sender that is making unauthorized use of your mail server.

You can also thwart spammers by exempting specific e-mail addresses or domains through the use of the Kill file. This file lets you specify a mail address or a particular mail host from which you do not want to

accept mail.

Mail relay options provide additional security, such as Relay for local hosts only, Relay for local users only, Relay Mail for Addresses and No Mail Relay. For more information on SMTP, see “Chapter 8: SMTP Server” on page 147.

POP3

Post Office Protocol version 3 (POP3) is the most common protocol for communicating with a mail server (otherwise known as a post office) to retrieve messages for a user. POP3 servers hold mail for users until they connect to download their messages.

POP3 clients typically use the “off-line” method of accessing the mail server: the mail client periodically connects to the server, downloads the messages to the client computer, and then disconnects from the server. Thus, mail messages are stored only temporarily on the server computer; they are automatically deleted from the server computer when downloaded to the client computer.

In the “online” access method, an open connection is maintained between the client and the server. Messages are left on the mail server computer and users can read mail on the server without downloading.

The POP3 Server lets any POP3 (Post Office Protocol, Version 3) mail client communicate with IMail Server. Supported POP3 clients include Internet Explorer, Netscape Messenger or Communicator, Eudora, Pegasus, NuPOP, Z-Mail, and UNIX mail.

For more information on POP3 see “Chapter 10: POP3 Server” on page 165.

IMAP4

Internet Message Access Protocol version 4 (IMAP4) is a method of accessing electronic mail messages that are kept on a (possibly shared) mail server. It allows a client e-mail application to access messages remotely as if they were local. For example, e-mail that is stored on an IMAP server can be accessed from a home computer without having to transfer the message or files between the computers.

The IMAP4 Server lets any IMAP4 mail client communicate with IMail Server. Supported IMAP4 clients include Netscape Communicator and Internet Explorer 4.0 and above.

Like POP3, IMAP4 uses SMTP for communication between the e-mail client and server. For more information on IMAP4 see “Chapter 11: IMAP4 Server” on page 177.

Web Messaging

Web Messaging allows users to access their mail on the IMail Server system from any web browser on the Internet. Users can then maintain an address book, use BCCs (“blind carbon copies”) and use delivery rules to process incoming mail. Users can also manage mailboxes by sorting messages in various ways, and creating “Sent” and “Deleted” mailboxes. Web messaging is also equipped with a Spell Checker with a customizable user dictionary.

Web Messaging administrators can manage virtual hosts, aliases, users and list-server mailing lists from a web browser. Web Messaging administrators can use HTML templates to customize, by host, the look and functionality of the web pages where users access mail and edit their settings.

Web Messaging also supports online advertising. This could be used by Internet Service Providers who want to display banner ads at the top of the Web Messaging mail screens and sell online advertising space on their mail server. For more information on Web Messaging see “Chapter 6: IMail Web Messaging” on page 107.

Web Calendaring

IMail Web Calendaring is a web-based calendar that allows you to keep multiple schedules accessible through an intuitive web interface. IMail Web Calendaring provides a user-friendly interface for storing schedules, appointment setting, recording notes and tasks, and receiving e-mail reminders that contain the date, time, and description of the appointment. Users can also send e-mail requests to other people inviting them to appointments or events.

Because it is web-based, IMail Web Calendaring allows the user remote access through any web browser connected to the Internet.

Like IMail Web Messaging, IMail Web Calendaring also supports online advertising. For more information on Web Calendaring see “Chapter 7: IMail Web Calendaring” on page 131.

Additional Services

In addition to the above basic servers, IMail Server also provides the following server programs that run as services on Windows NT/2000:

- **A Lightweight Directory Access Protocol (LDAP) version 3 server**

  The LDAP server provides remote access to IMail Server user information through any LDAP client application. IMail Server user data includes standard LDAP information such as the user's name, organization, mailing address, and telephone number. LDAP Version 3 is supported. For more information see "Chapter 12: LDAP Server" on page 171.

- **A list server**

  Mailing lists are used widely on the Internet as a means of sharing information about a topic. The list server lets you set up automated mailing lists. List-server mailing lists can receive mail and resend the mail to all the users on the mailing list.

  The list server also supports moderated and unmoderated lists, as well as the ability to group messages into a digest and periodically send the digest as a single message. For more information see.

- **The Monitor server**

  IMail Server provides self-monitoring via a Monitor server that polls each of the IMail Server services. The Monitor server can be configured to send an e-mail, beeper, or pager notification when a service goes down or comes back up; it can also automatically restart a service that has gone down.

  In addition, you can use this server to monitor other services (DNS, NNTP, WWW, Telnet, and FTP), the default gateway, and disk space, from either the local or a remote system.

  You can access the Monitor server remotely using a web browser to view the status of monitored services and perform administration functions. For more information see "Chapter 16: The Monitor Server" on page 195.

- **Finger and Whois servers**

  The Finger and Whois servers allow you to publish user information on the Internet. For more information see "Chapter 14: Finger Server" on page 187.

- **A Password server**

  The Password server lets users of older mail clients (such as Eudora and NuPOP) change their passwords remotely.

Standard Features

In addition to sending and receiving mail, IMail Server provides a number of robust features.

User Registration and Maintenance

IMail Server supports up to 250 user accounts, up to 1000 accounts or an unlimited number (depending on license.) It also supports an unlimited number of user mailboxes. Users must be registered in order to have a local mailbox and to allow remote POP3, IMAP4, or web clients to connect to the server to retrieve mail from those mailboxes.

IMail Server lets administrators:

- Add, delete, and maintain user accounts, lists, standard aliases, group aliases, and program aliases
- Set up inbound and Outbound mail delivery rules, vacation processing, Info Manager automated responses, and mail forwarding
- Update Finger, Whois, and LDAP information
- Base IMail Server users on an external database. The basic capability uses the ODBC method, but can be extended to include up to ten different methods.
- Use command line utilities for adding or deleting large numbers of users, aliases, and hosts from text files
- Use command line utilities for deleting old messages
- Use a command line utility to send a message to all users on a virtual host or on the entire server

For more information, see “Chapter 4: User Mail Accounts” on page 59 and “Appendix C. Command Line Applications” on page 259.

Mailing List Creation and Maintenance

IMail Server can create and maintain list-server (automated) mailing lists; these can be either public or private. When a list-server mailing list receives mail, it re-sends the mail to all subscribers on the list; re-

sent mail can be sent one message at a time, or it can be accumulated for periodic sending (“digest mode”). For more information, see “Chapter 17: List-Server Mailing Lists” on page 215.

Mail Forwarding

You can have IMail Server forward new mail for a particular user to another address. For more information, see “Forwarding Mail to Another User Account” on page 73.

Vacation Support

If a user cannot answer mail due to vacation or other absence, IMail Server can automatically send *one* notice to each person who sends mail to that user. This allows people to send many messages to someone on vacation without being flooded with notices that the recipient is away. For more information, see “Setting Up a Vacation Message” on page 70.

Finger “Plan” Support

The Finger protocol is a common Internet tool that allows remote users to see information about users registered on a system. This includes the full name of the specified user, his or her complete e-mail address, and a “Plan” file provided by the user that contains any additional information the user wishes to provide in response to Finger requests. For more information, see “Chapter 14: Finger Server” on page 187.

Mail Delivery Rules

You can create delivery rules to search for particular text patterns in the content of a particular part of a message (To, From, Sender, Subject, entire header, or message body) and re-route the message based on the contents. You can apply delivery rules for a mail host, a list-server mailing list, or for individual users. For more information, see “Setting Up Delivery Rules” on page 83.

Automated Mail Accounts

The Info Manager feature lets you set up an automated response: when mail is received for a user that has enabled the Info Manager, a prepared message is automatically sent back to the sender.

The Info Manager also lets you set up special mail accounts with unique responses for each sub-area. For example, you could create an

info user account for your organization. When someone sends mail to the *info* account, the system can return a response that describes the sub-areas of the *info* account, such as *sales* or *classes*.

Senders can then send a message to *info-sales* and receive back a message related to sales, or to *info-classes* and receive back a message about classes you offer. For more information, see “Using the Info Manager” on page 101.

Multiple Host (Domain) Support

If you want to receive mail for more than one e-mail host on the same Windows NT/2000 system, you can set up multiple virtual hosts. For example, if your mail server provides mail service for your local e-mail host, *mail.petra.com*, and you also want it to provide mail service for another e-mail host, *mail.acme.com*, you can create a virtual host for *mail.acme.com*. For more information, see “Chapter 3: Configuration” on page 33.

Privacy-Enhanced POP Support

Post Office Protocol Version 3 (POP3) is the most common protocol used by mail clients for retrieving messages from a mail server. The user ID and password are encoded so that they cannot be read by standard text editors. However, the encoding is not complex, and this feature should not be confused with security. For more information, see “Chapter 10: POP3 Server” on page 165.

Forwarding of Mail to a Beeper or Pager

IMail Server can route inbound mail to any external program such as preconfigured pager or beeper addresses, or any other application. For more information, see “Types of Aliases” on page 76.

Unknown Local User Processing

IMail Server can perform special processing of mail that is incorrectly-addressed or addressed to users that don’t exist on the local host. This is accomplished through a special alias, *nobody*, which can send mail to a specified program or another user’s mailbox. For more information, see “Processing Mail to Users That Don’t Exist” on page 79.

Anti-spamming Features

IMail Server's built-in messaging controls prevent unauthorized mailings from using the IMail Server as a relay or gateway. You can set up the server to accept only mail that originates from local users or that is destined for local users. (IMail Server lets you define the systems or address blocks that you want to consider as local.) In addition, you can block incoming messages from specified IP addresses if those addresses have been a source of unwanted e-mail. For more information, see "Chapter 9: Security and Antispamming" on page 153.

Optional Capabilities

Mail to Fax. You can purchase a Mail to Fax capability which lets you set up mail accounts that can receive mail from a mail client and forward it to a preconfigured fax phone number. This option also supports "dynamic aliasing" which lets users enter the fax phone number when they create the message.

IMail Anti-Virus. IMail Anti-Virus fully integrates with IMail Server and is powered by Symantec's CarrierScan™ Server, a high performance, scalable, reliable solution to protect against viruses. IMail Anti-Virus provides administrators a powerful all-in-one anti-virus solution that is easy to install and use. Designed to work exclusively with IMail Server, IMail Anti-Virus stops dangerous viruses before they make it to an end-user's e-mail client.

IMail Client for Windows

A special version of IMail Client for Windows is automatically installed on the IMail system. This is provided for those who are administering IMail Server on the NT workstation on which IMail Server is installed; it is useful for reading the "root" mailbox, working with seldom-used accounts, and testing.

Note

The IMail Client application should *not* be used on the IMail Server system to view end-user mailboxes, as this may cause problems with remote access to the same mailboxes (depending on the remote clients being used).

Chapter 2: Installation

This chapter describes the installation of IMail Server. First, it describes what you need to know about the primary host (the system on which you install IMail Server), and what decisions you need to make before running the installation.

Next, a procedure walks you through the steps to get IMail Server up and running. This is followed by a description of the root user ID, a quick test of your installation, an overview of the IMail Server configuration, and the directory structure. The last two sections cover upgrading and removing IMail Server.

It is highly recommended that you read the "IMail Server Getting Started Guide" included with this product before you begin the installation process. Reading this guide will greatly reduce the amount of time needed for installation and configuration, and will prevent unnecessary problems from occurring during setup.

Note

IMail Server requires a static IP address, it will not function using a dynamic IP address.

Before You Begin

As stated above, the primary host is the system on which you install IMail Server. Before you begin the installation, you must (1) check the official name of the primary host, and (2) decide what database the primary host will use to register and authenticate users.

Checking Your Primary Host Name

You should first check the DNS information for the system on which you intend to install IMail Server (the primary host).

To check the DNS information (on Windows NT), double-click the **Network** icon in the Control Panel, select the **Protocols** tab, select **TCP/IP Protocol**, and then click **Properties**. The TCP/IP window appears. Click **DNS** to view the domain information.

To check the DNS information (on Windows 2000), double click the **System** icon in the Control Panel, select the **Network Identification**

tab, then click **Properties**. The **Identification Changes** dialog box appears which displays the domain information.

The **Host Name** and **Domain** *must* be registered in the DNS (Domain Name System) if you want remote hosts to be able to communicate with your system. Your DNS must contain the proper entries for the host name. For more information, see your DNS documentation and “Appendix I: Mail Servers and the DNS” on page 315.

Note

You can use Ipswitch’s WS_Ping ProPack to lookup DNS information. An evaluation version is included on the IMail Server CD. For more information about looking up DNS information using WS_Ping ProPack, see the “IMail Server Getting Started Guide”.

User Registration and Authentication

The primary host can use one of three databases for registration and authentication of users. (Registration is the process by which user mail accounts are created. Authentication is the process by which user IDs and passwords are verified.)

- **IMail Database.** User IDs and passwords for mail accounts are stored separately from either the Windows NT or 2000 user database, or any external database, in a proprietary database in the Windows registry.

  You can also import Windows NT or 2000 users into an IMail user database, without having them linked to the Windows NT or 2000 database. For information on importing Windows NT or 2000 users, see “Importing NT Users” on page 63.

- **Windows NT Database.** This database provides automatic creation of user mail accounts for any user listed in the Windows NT or Windows 2000 user database on your host machine.

  Note that the primary mail host needs access to the Windows NT or 2000 user database for your network.

  To view a current listing of users in your Windows NT or 2000 user database, use the appropriate administrative tool as described in your Windows documentation.

  You will not be able to add or delete users using the IMail Administrator; instead, you must use the appropriate windows

administrative tool (these are different for Windows NT and Windows 2000).

Note

A mailbox and other user files are created for a user when the mail server receives a message for that user, or when a user first accesses the IMail Server through a mail client.

- **External Database.** IMail Server uses an external database to register and authenticate users. Users that you add and delete using IMail Server will be added to, and deleted from, that external database, and vice versa.

Installing IMail Server for the First Time

The IMail Server install program installs the complete IMail Server software. If you need help at any time during the installation, press F1 to display the install help. However, before you start, make sure you have read "Before You Begin" on page 15.

Note

Before you use IMail Server to associate an external database with a host, use the Windows Control Panel to make sure there is a System DSN (Data Source Name) that points to a valid database name. See your Windows NT and database documentation for information on the System DSN.

Installation Procedure

To install IMail Server:

1 Log on to Windows NT as System Administrator, or to an account with System Administrator privileges.

2 Back up your Windows NT registry. (Run *regedit.exe* and select **Export Registry File** from the **Registry** menu.)

3 Do one of the following:

- If you purchased an IMail Server CD-ROM, insert it in the CD-ROM drive. If the installation program does not run automatically, select **Run** from the **File** menu, and enter the CD-ROM path followed by *setup.exe*.

- If you downloaded IMail Server from the Internet, run the downloaded application, *imailec.exe*.

4 **Official Host Name** dialog box. Confirm (or enter) the official host name of your primary system as described in"Checking Your Primary Host Name" on page 15. This will be the "primary host."

5 **Database Options** dialog box. Select the user database option you prefer. For more information, see "User Registration and Authentication" on page 16.

6 **System DSN** dialog box. If you selected **External Database**, you must specify the ODBC System DSN for the database where the user information is stored. IMAILSECDB is the default name that the IMail ODBC link uses.

7 **Choose Destination Location** dialog box. Enter the directory where IMail Server will be installed. This directory should *not* be moved or renamed after installation.

Note

The path and directory must *not* contain spaces.

---

8 **Select Program Folder** dialog box. Confirm or enter the Program Group in which IMail Server will appear (on the **Start** menu).

9 **SSL Keys** dialog box. When asked if you want to install default SSL keys, do one of the following:

- If you already have a third-party SSL certificate, click **No**. After installing IMail Server, run the IMail SSL utility by selecting **Programs** -> **IMail Server** -> **IMail SSL Configuration Utility** from the **Start** menu, and then follow the instructions in Help.
- If you do NOT already have a third-party SSL certificate, but want to run the IMail web server using a "self-signed" SSL certificate, click **Yes**.
- If you would like to read more about SSL before you make a decision, click **No**. (You can always install default keys later.)

10 **Template Options** dialog box. Select the set of web templates that you want to install by default. You can add additional templates (i.e. to virtual hosts) later by manually copying them from the CD.

11 **Dictionary Options** dialog box. Select the dictionaries that you want to install by default. Note that dictionaries can also be installed later.

12 **SMTP Relay Option** dialog box. Select the mail relay setting for your setup.

13 **Start IMail Services** dialog box. The install program displays a list of IMail services; the ones already running on your system are selected. Select any others you want to start by default. (Note that you can also specify default services at any time after the installation.)

14 **Add User** dialog box. You see this dialog box only if you selected the IMail Database option. We recommend you add a few "stand-in" users now so you can test the installation. (Note that you can also add users at any time after the installation.)

If prompted to do so, restart your system when the setup is completed.

Note

If your primary host is based on an external database, see "Creating a Host Based on an External Database" on page 56.

Root User ID

Each host in IMail Server must have user ID of *root* and an alias of *postmaster* in order to comply with the SMTP RFCs. These allow messages to be sent to the server by other hosts, and also allow certain system messages (such as error messages) to be automatically generated.

If the primary host uses the IMail database or an external database, the installation procedure creates a user named *root* and an alias named *postmaster* and points the alias to the user named *root*. The user ID of *root* is automatically registered, however the account is disabled by default.

When using the NT user database, the installation creates a user named *administrator* and an alias named *postmaster* and points the alias to the user name *administrator.*

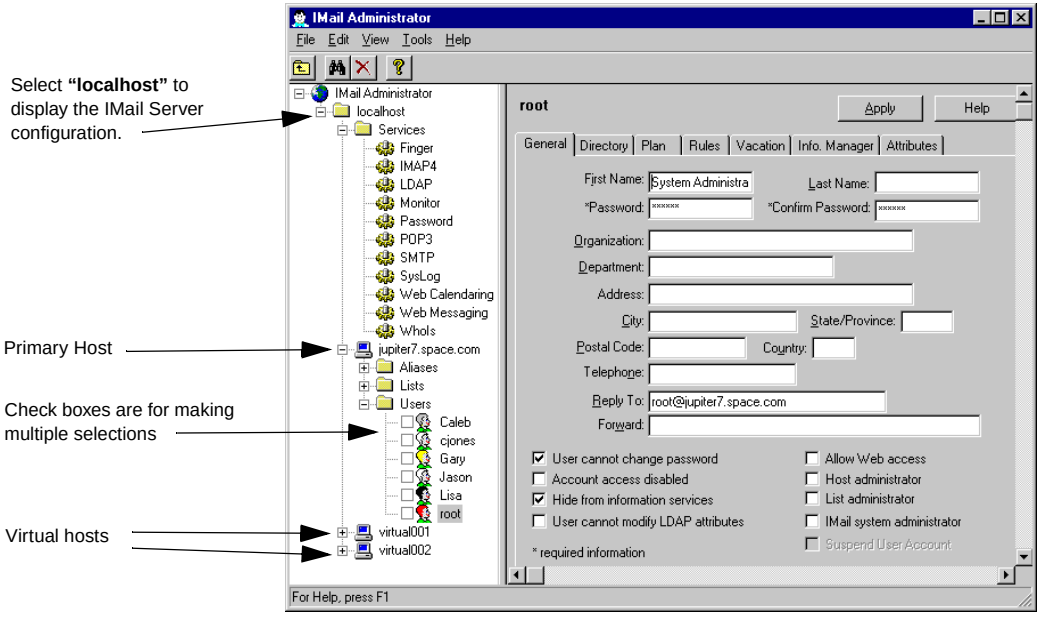
Performing an Initial Setup and Test

To confirm your IMail Server installation, do the following:

1 From the **Start** menu, select **Programs** -> **IMail** -> **IMail Administrator**.

2 The IMail Administrator appears in a split window. The left panel provides access to system defaults, host settings, and access to users, aliases and list-server mailing lists .

Select an item in the left panel to view its properties in the right panel.



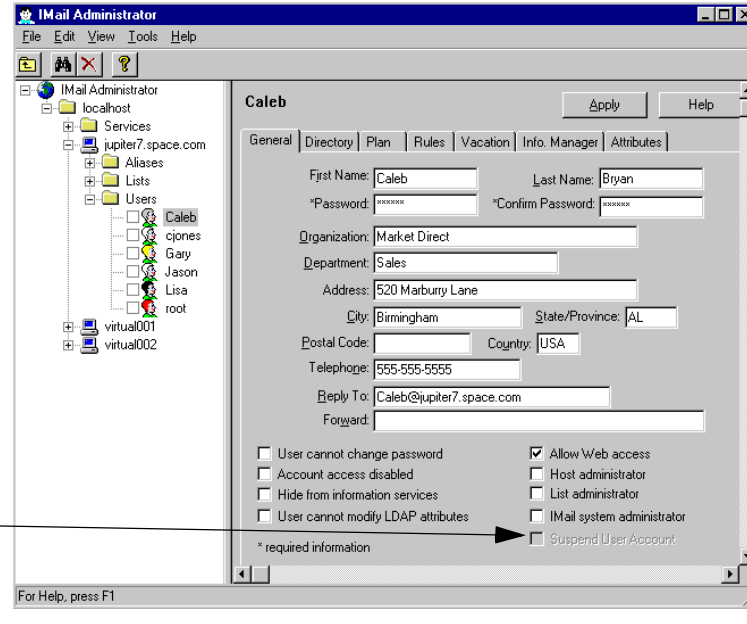
To verify that you can send and receive mail, you should have at least one user for your primary host.

If your primary host uses the IMail user database, you may have created a user during the installation process. Check to see whether users were created in IMail Administrator. In the left panel of IMail Administrator, expand the “localhost” folder, select the primary host, and then expand the Users folder. If you see only the “root” user, you will need to add a test user by performing the following steps.

1 Select the primary host and click the **General** tab.

2 In the right panel, click **Add User**, and then follow the instructions. The User ID must be between 3 and 30 characters, with no spaces. For now, leave **Show Advanced Settings** turned off.

3 Click **Next** and then **Finish** to add the user. The User ID is added to the list of registered users for the primary host. When the new user is selected in the left panel, that user’s properties are displayed in the right panel.



This option is only visible if the account has been disabled.

If your primary host uses the Windows NT or Windows 2000 user database, you should have two default accounts:Administrator and Guest. If you need to add a user for test purposes, add the account in the appropriate Windows administrative tool.

If your primary host uses an external database and the external database is not populated, perform the following steps:

1 In the left panel, expand the primary host and the "**Users**" folder.

2 Select the user "root."

3 On the **General** tab, turn off **Account Access Disabled**.

4 Add a few users as described in the next section.

Any users you have added can now receive mail through IMail Server at the host name specified in your Windows NT/2000 TCP/IP parameters. For example, if you added the user *caleb*, and the host name is *jupiter7.space.com*, the user can now receive mail addressed to *caleb@jupiter7.space.com.*

Note

If you want users on the primary host to get messages addressed to just the domain name, create an alias for the virtual host. For example, if you want the user shown above to get mail addressed to *caleb@space.com*, create a host alias of *space.com* for *jupiter7.space.com*. For more information, see "Chapter 3: Configuration" on page 33.

Sending and Receiving Mail in a Test Account

To send and receive mail in a test account:

1 Check to make sure the mail servers are running: select the "**Services**" folder in the left panel to see if the **SMTP**, **POP3**, and **IMAP4** servers are running. The status of **SMTP** should be "running;" this is automatically started. If the **POP3** and **IMAP4** are not "running," you must start them.

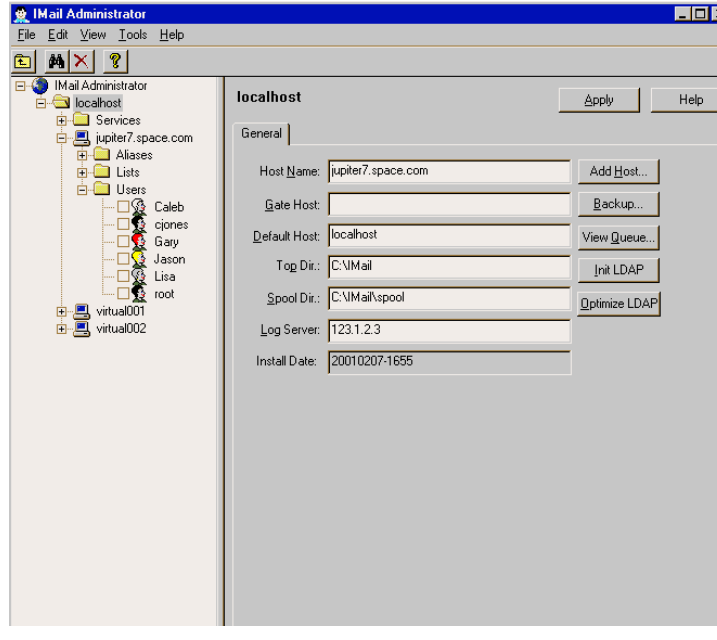
2 Start IMail Client from the **Start** menu. This special version of IMail Client shows the users you added in a drop-down list. Log on using one of the user accounts you created, and send mail to another user. Then check that the mail appears in the second user's *Main* mailbox.

3 If you are connected to the Internet, send mail to *imailtest@ipswitch.com* to test mail service to remote systems. We will reply to your mail. You can also test an account by sending mail to a user on another host and asking for a reply.

4 When you are satisfied that the mail server works properly, you can add more hosts and users as described in subsequent chapters. If your primary host is based on an external database, see "Configuring the Primary Host" on page 56.

Viewing the Basic IMail Server Configuration

In the left panel, select "**localhost**" to view the IMail Server configuration.



You can modify only the **Gate Host** or the **Default Host** properties.

The **Gate Host** box displays the name of another host to send mail to for further delivery when that mail cannot be delivered directly to the destination host. This can be used in conjunction with **Send all remote mail through gateway** on the SMTP tab to force delivery of mail through the gateway host. This is useful for dial-up connections.

Since IMail Server should be able to reach all hosts directly, this field should typically be left blank. See “Chapter 8: SMTP Server” on page 147.

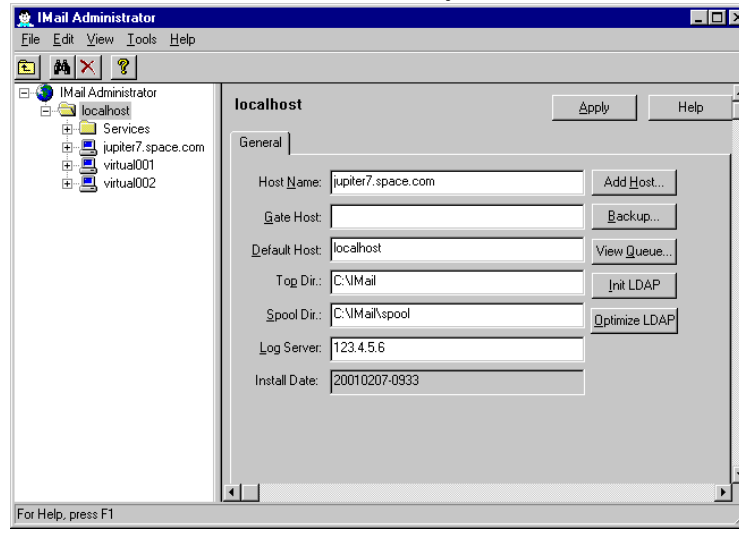
The **Default Host** box displays the host name to which mail should be delivered if the original recipient address contains only a user ID without a host name, and that user ID is not found on the sender’s host. Normally, this field should be left blank or set to “localhost”. Otherwise, mail will be sent to userID@DefaultHost, which may not be the intended recipient. This field can be useful when multiple systems are required to work as one system.

Note

Setting this option incorrectly may cause mail to be sent to unintended recipients.

General Properties

The **General** tab shows host and directory information.



Click the **Add Host** button to display the “Virtual Host Configuration” dialog box. For descriptions of how to add, modify, or delete a virtual host, see the next chapter.

The Mail Queue

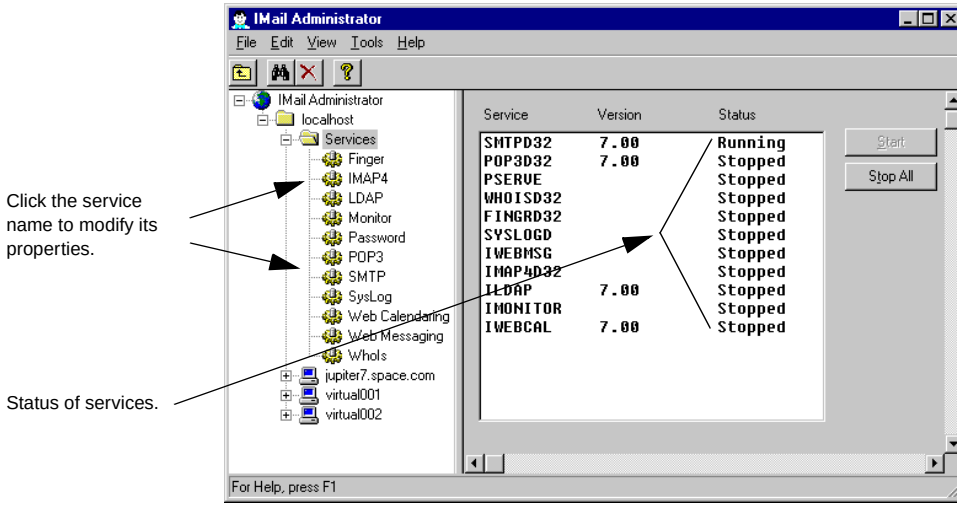
You can click the **View Queue** button on the **General** tab to display the files in the outbound mail queue. Each of the messages waiting to be delivered will have a file. These are listed in the **Filename** list box. Selecting one of these files displays information about that message. You can then delete the message from the outbound queue or force delivery of one or all of the messages. Note that you cannot modify any of the displayed information. For detailed information on the mail queue, see “Appendix D. Spool, Queue, and Log Files” on page 273.

A Quick Look at IMail Server Services

Click the “**Services**” folder to get a quick look at IMail services.

You see the current status of each of the services. Later chapters in this book describe the configuration options available for each of these services.

You configure IMail services by clicking on the service name under the “**Services**” folder and then using the tabs in the right panel to adjust the settings.



Verifying Services

You can modify configurations for each of the services (SMTP server, POP3 server, IMAP4 server, LDAP server, Finger server, Whois server, Password, and Monitor server) by selecting the "**Services**" folder in the left panel and clicking the appropriate Service name underneath it. Make changes to the settings in the right panel.

If you change any parameters, stop the service, wait five to ten seconds and then start the service, or reboot the system after the completion of all changes. Detailed information on each service is covered in later chapters.

Default Service Ports

IMail Server services use the following TCP ports:

SMTP: Port 25 (This can be changed by editing the Windows registry; see "Advanced Options" on page 151.)

POP3: Port 110

IMAP4: Port 143

LDAP: Port 389

Pserve (Password Server): Port 106

Web Messaging: Port 8383 by default (configurable)

Web Messaging SSL Port: 8384

Spell Checker Port: 8385 by default (configurable)

Web Calendaring: Port 8484 by default (configurable)

Web Calendaring SSL: Port 8485

SSL: Port 8384 by default (configurable)

IMonitor Web Administration: Port 8181 by default (configurable)

Web Messaging and Web Calendaring also use several UDP ports. These ports, are used to facilitate communications between Web Messaging and Web Calendaring, such as receiving the User key and sending the User ID and Password.

IMail Web Messaging and IMail Web Calendaring use the following UDP Ports:

Web Messaging: Port 8000

Web Calendaring: Port 8001

The IMail Server Directory Structure

The IMail directory, usually *C:\IMail*, is “the top directory.” You specify this directory during installation, and should never move or change this directory.

In the top directory are all the IMail Server applications and the directories for the primary host.

Each host directory (including the top directory which has the directories for the primary host) contains the following:

- The *Lists* directory contains all the list-server mailing lists as well as the text files that are referenced by group aliases
- The *Spool* directory where messages are processed (“the queue”) and where log files are kept.For detailed information, see “Appendix D. Spool, Queue, and Log Files” on page 273.

Note

Not all host directories have a Spool directory.Only the IMail TopDir has a spool directory.

- The *Web* directory contains templates, ads, and monitor files.
- The *Users* directory contains the users on the host. Within the *Users* directory, each user has a directory.” Within each user’s directory are the user id file (*.uid*); mailbox files (*.mbx*); index files (*.idx*); Finger Plan, Vacation, Rules, Forwarding files (*.ima*)
- The *ldap* directory contains information for LDAP-enabled clients.
- The *cfg* directory contains information for the IMail Client application.

Upgrading

This section is for users who are upgrading from a previous version of IMail Server. IMail Server is automatically installed in the same directory where you had the previous version or evaluation version. This directory should *not* be changed, moved, or renamed.

1 Log on to Windows NT/2000 as System Administrator, or to an account with System Administrator privileges.

2 Make sure the Windows NT/2000 Control Panel is closed, as well as all other applications.

3 Back up the Windows NT/2000 registry key,

`H_KEY_LOCAL_MACHINE\Software\Ipswitch\IMail\`

(Start *regedit.exe*, locate this key and select **Export Registry File** from the **Registry** menu.)

4 Do one of the following:

- If you purchased an IMail Server CD-ROM, insert the CD-ROM in a drive. Select **Run** from the **File** menu, and then enter the CD-ROM path followed by *setup.exe*.
- If you downloaded IMail Server from the Internet, run the downloaded application, *imailec.exe*.

Note

It is strongly reccomended that you stop all IMail services and close the IMail Administrator interface before upgrading.

5 Follow the prompts on your screen. If you have any questions, click the **Help** button, or press F1.

6 If the installation program does not detect SSL keys on your computer, you will be asked whether or not you want to install default SSL keys. Here's how to decide:

- If you already have a third-party SSL certificate, click **No**. After installing IMail Server, run the IMail SSL utility and follow the instructions in Help.
- If you do NOT already have a third-party SSL certificate, but want to run the IMail web server using a "self-signed" SSL certificate, click **Yes**.

- If you want to read more about SSL before making a decision, click **No**. You can install default keys later. For more information, see “Using Secure Sockets Layer (SSL)” on page 113.

7 Restart your system when the installation is completed.

Upgrading Using External Databases

When installing IMail Server v7.0 over an earlier version, in which one or more hosts use an external user database, new columns must be added to the database tables. This is due to additional user-level data which must be stored for use with the new Web Messaging and Web Calendaring features. The new columns must be added to the user table for each IMail Server host that uses an external database.

During the install, IMail Server will determine whether your system currently uses an external database. If the answer is yes, then a dialog is displayed giving you the three following options:

- Click **Yes** to have this install program automatically add the columns to all external database tables used to store IMail Server user settings.
- Click, **No** to continue installation without updating the tables.
- Click **Cancel** if you want to manually add the necessary columns. The required columns can be found in the release notes. You will need to restart this install program when ready.

Note

If you click **No** and install anyway, be advised that IMail Server may not function correctly.

If a custom ODBC driver was used with a previous version of IMail Server, the driver must be modified to use the new columns. Source code for the basic ODBCUser.dll driver (tailored for SQL Server and Access) can be downloaded from the IMail Support Center:

ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/obdcuser7.dll

Upgrading Web Messaging

If you have customized templates you want to continue using, refer to the “Upgrading Customized Templates Document”(Upgrade6to7.txt)

for procedures to upgrade the old templates for use with IMail Server v7.0. This file is located in the *[IMail Top Directory]\Web\New* directory. See also the web messaging topic “Upgrading” on page 110.

Re-Installing IMail Server to a Different Location

When re-installing IMail Server to a different location, the WEBDOCS value in imonitor.ini is not updated. This causes the up.gif and down.gif files in IMonitor to be missing on the Service Status page. IMonitor produces the WEBDOCS value, but does not know when a reinstall has occurred, or when a web directory has been moved. If you change the install location of IMail Server, you MUST update the WEBDOCS field in the imonitor.ini file to point to the new location so the GIFs will be loaded properly.

Removing IMail Server

To remove IMail Server, use the **Add/Remove Programs** applet in the Windows Control Panel. The following happens:

- IMail services are removed from the Control Panel Services
- Everything is deleted in the Windows registry under HKEY_LOCAL_MACHINE/Software/Ipswitch/IMail (but does not remove the Ipswitch key)
- Directories and files created by *setup.exe* are removed if nothing has been added to them. For instance, if you haven’t added any users (and *root* never gets mail), the *Users* directory is removed.

Note

Removing IMail Server as described above does not delete the IMail directory or the subdirectories and files it contains. To remove these, you must delete them manually.

IMail server’s uninstall doesn't remove the following files: *iwebmsg.ini imonitor.ini imail.ini*. This can cause problems with future installations. An example is if an administrator installs IMail Server in a location other than the standard C:\IMail, settings such as the web dir, ports, etc... are retained. So if the administrator then installs IMail Server in the standard location, some values point to the wrong location by default.

If you are reinstalling IMail Server to a new location, these three files (*iwebmsg.ini imonitor.ini imail.ini)* need to be deleted or updated.

Chapter 3: Configuration

This chapter describes how to configure your mail server and the Domain Name System (DNS) records that pertain to mail service. It also describes how to create multiple mail hosts on your mail server and discusses the DNS records required for multiple hosts. In addition, it covers a number of advanced configuration topics.

Basic Configuration

If your mail server will receive mail for one e-mail domain (for example, for mail addressed to *domain.com*), read the sections "Checking Configuration of the Primary Mail Host" on page 34 and "Setting Up DNS for the Primary Mail Host" on page 35. If you need background information on DNS servers, see "Appendix I: Mail Servers and the DNS" on page 315.

Advanced Configuration

Depending on your mail requirements, you may want to read some of the advanced configuration topics:

- You can set up an alias for the official host name (that was entered when installing IMail Server), so that IMail Server can recognize another name as valid. For example, you could set up an alias so that both *user@mail.domain.com* and *user@domain.com* are valid addresses. To set up an alias, see "Setting Up an Alias for a Mail Host" on page 36.
- If the server will receive mail for multiple domains, each with its own set of users (example, for *domain1.com* and *domain2.com*), see "Adding an Additional Mail Host" on page 36.
- If you want your mail server to function as an SMTP mail gateway for proprietary mail systems such as Microsoft Exchange or CC:Mail, see "Setting Up IMail Server as a Mail Gateway" on page 45.
- If you have a dial-up Internet connection from your mail server to an Internet Service Provider (ISP), allowing you to receive mail from an account with your ISP, see "Setting up a Dial-up Internet Connection" on page 46.

- If you want to set up IMail Server as a backup mail server for another server, see “Setting Up IMail Server as a Backup Mail Spooler” on page 50.
- If you want to spread user accounts across two or more physical computers, you can set up “peer” servers. For example, mail sent to *domain.com* is processed by both *host1.domain.com* and *host2.domain.com*. See “Setting Up “Peer” IMail Servers” on page 51 for more information.
- If you want to specify how your mail server relays mail for other servers, see “Chapter 9: Security and Antispamming” on page 153 for information.

Checking Configuration of the Primary Mail Host

After installing IMail Server, you have a single mail host configured — this is the primary mail host. Check the following items in the mail host configuration:

- This primary mail host must have the same name as the host on which you installed IMail Server. This is the official host name that you see when you expand the “**localhost**” folder in the left panel.

  If you do not want to use the official host name of your server as the name of the primary mail host, you can create an alias for the primary mail host. See “Setting Up an Alias for a Mail Host” on page 36 for information.

- The domain name for the local network must be set in your Windows NT/2000 configuration.

  To check the domain name for your local network (in Windows), double-click the **Network** icon in the Control Panel, select the **Protocols** tab, then select **TCP/IP Protocol** in the list, and click the **Properties** button. The “Microsoft TCP/IP Properties” dialog box appears. Click the **DNS** tab to view the domain information.

  To check the DNS information (on Windows 2000), double click the **System** icon in the Control Panel, select the **Network Identification** tab, then click **Properties**. The **Identification Changes** dialog box appears which displays the domain information.

- The DNS server for the local network must appear on the IMail Administrator **SMTP** tab. To check the DNS server setting, click the **SMTP** tab. In the **Domain Name Server address** box, you should see the IP address of your DNS server. This box can have multiple addresses, separated by a space.

Note

You can see your own DNS records (and those of any host) with the Lookup utility in Ipswitch's WS_Ping ProPack, a network information tool. An evaluation version of WS_Ping ProPack is included on the IMail CD, it is also available for download on the Ipswitch website: *www.ipswitch.com.*

Setting Up DNS for the Primary Mail Host

For background information about DNS records, see "Appendix I: Mail Servers and the DNS" on page 315.

You need to make the following entries for your primary mail host in your DNS:

- An MX record for the mail domain (for example, *domain.com*). The MX record identifies the host name of the computer running the mail server (in this case, the IMail Server computer).
- An A record for the host name of the computer running IMail Server. The A record maps a host name to an IP address.
- A PTR record for the IP address of the computer running IMail Server. The PTR record maps an IP address to the host name and is used for reverse lookups.

As an example, the DNS entries for a host for which the official host name in IMail Server is *mail.domain.com* would look like:

```
SOA
$ORIGIN
...
domain.com
     IN MX 10 mail.domain.com (MX record)
     mail IN A 156.21.50.5      (A record)
                                (PTR record)
5.50.21.156.in-addr.arpa.,type = PTR
 host = mail.domain.com
```

A DNS lookup for mail sent to *user@domain.com* would find that the mail must be sent to the host *mail.domain.com*.

Setting Up an Alias for a Mail Host

IMail Server accepts mail addressed to the official host name of the system on which IMail Server is installed. You can set up an alias for the official host name so that IMail Server can recognize another name as valid. For example, if the official host name is *mail.domain.com*, you can receive mail addressed to *user@mail.domain.com*, where *user* is a valid user on the host. If you also want IMail Server to accept mail addressed to *user@domain.com*, you need to enter *domain.com* as an alias for the official host name.

To set up an alias for the official host name:

1 In the left panel, select the mail host. The mail host properties appear.

2 In the **Aliases** box, enter the alias name (i.e. *domain.com*). Separate multiple aliases with a space. This field is limited to 255 characters.

3 Click **Apply** to save the changes.

Adding an Additional Mail Host

If you want IMail Server to receive mail for a second e-mail domain that has its own users, you need to set up a virtual host for the second domain. For example, if your mail server provides mail service for the e-mail domain, *domain1.com*, and you also want it to provide mail service for another e-mail domain, *domain2.com*, you need to create a virtual host for *domain2.com*.

There are two types of virtual hosts:

- Virtual hosts with IP Addresses
- Virtual hosts without IP addresses

Note

Whether you use a virtual host with IP address or a virtual host without IP address, you need to make the proper DNS entries for your mail domain(s). See “Setting Up DNS for Multiple Mail Hosts” on page 43 and your DNS documentation for information on creating

these entries.

Virtual Hosts with IP Addresses

This is usually the recommended way to set up virtual hosts, because all of the capabilities of regular IMail Server hosts are available to virtual hosts with IP addresses. The only limitations of virtual hosts with IP addresses are:

- Each virtual host requires its own unique IP address.
- In Windows NT/2000, this requires the extra step of adding an IP address in the Windows NT TCP/IP configuration in the Control Panel (**Network** applet - > **Protocols** -> **TCP/IP Protocol** -> **Advanced** button.)

Note

If you are using Windows NT 3.5.1 or later, you can add up to five IP addresses in the Network applet. If you need to add more than five addresses, refer to the documentation for Windows NT/2000.

Virtual Hosts Without IP Addresses

Virtual hosts without IP addresses are easier to set up than those with IP addresses. For more information, see “Configuring a Virtual Host” on page 38. The IMail Server computer will assign a virtual IP address for the selected domain. You can then use an MX record in your DNS to point the virtual host to the primary host (which has a real IP address). There are several limitations of virtual hosts without IP addresses:

- So that IMail Server can tell which virtual host the user is associated with, when the user logs on, they must enter the entire *userid@hostname.com* string for their user ID. Some mail clients will not be able to connect to the virtual host to read mail. This problem exists because some mail clients either have length restrictions for user IDs, or they clip the user ID at the @ sign. You can set up the virtual host to use a different character to separate the user ID from the hostname, but then you must tell users use this character in their logon user IDs (for example, *userid#hostname.com*). To change the character, see “Appendix G. Special Registry Values.”

- The LDAP, Whois, and Finger servers do not work with virtual hosts without IP addresses.

Virtual hosts without IP addresses are recommended when you have a shortage of IP addresses, or when you want to forward all mail for a domain to a user at another domain. As an example of the latter:

- Your primary domain is called *abracadabra.com*
- You want all mail sent to *merlin.com* to be forwarded to *info@abracadabra.com*
- To accomplish this, set up a virtual host without an IP address for *merlin.com* and do not create any users for *merlin.com*
- Set up a *nobody* alias for *merlin.com* pointing to a user ID on *abracadabra.com*
- All mail to any user at *merlin.com* will be sent to the specified user at *abracadabra.com*

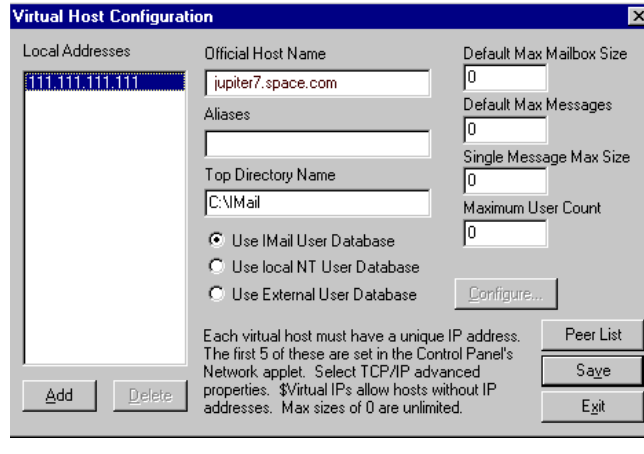
Configuring a Virtual Host

To configure a virtual host (assuming "Use Wizards" is turned off):

1 Select the "**localhost**" folder in the left panel.

2 Click the **Add Host** button.

The "Virtual Host Configuration" dialog box appears.



The **Local Addresses** list box shows all IP addresses set up in the Windows NT/2000 TCP/IP properties as well as any virtual IP addresses assigned by the IMail Server.

3 Select the IP address for the virtual host (in the **Local Addresses** list box) or click the **Add** button to assign a new virtual IP address to use for the new mail domain.

4 In the **Official Host Name** text box, enter the name of the mail host.

The name you enter here will be used to address mail to the users on the virtual host. For example, if you enter *mail.domain2.com* as the mail host name, any users you add to the virtual host will receive mail at *user@mail.domain2.com*.

5 In the **Aliases** text box, specify alternate host names for which you want the computer to accept mail. For example, if your mail host name is *mail.domain2.com*, you can set an alias of *domain2.com* so that IMail Server accepts mail addressed to *fred@mail.domain2.com* and also *fred@domain2.com*. Multiple aliases are separated by a space. This field is limited to 255 characters.

6 In the **Top Directory Name** text box, enter the name of the directory where the directories for users, lists, and web files for this virtual host will be stored.

In most cases, you will use a different directory for each virtual host that you create. It is possible for virtual hosts to share a single directory but then users that have the same names will actually share the same mailbox.

7 Select the type of user database you want to use for this host.

Use IMail User Database
Use Local NT User Database
Use External User Database

For a description of these options, see "User Registration and Authentication" on page 16.

8 Enter the default parameters for mailboxes and messages. These parameters apply to all users on the virtual host.

Default Max Mailbox Size. Enter the default maximum size in bytes (characters) for the total of all mailboxes in a user's account. If the total size exceeds the maximum, any new mail is returned to the sender. Enter zero for an unlimited size. For more information see "Additional Host Settings" on page 41.

Default Max Messages. Enter the default maximum number of messages (the total for all mailboxes) that will be allowed in a user's account. If the maximum is exceeded, any new mail is returned to the sender. Enter zero for an unlimited number. For more information see "Additional Host Settings" on page 41.

Single Message Max Size. The default maximum size (in bytes) for a single message sent to the server. If a message exceeds the maximum, it is returned to the sender. Enter zero for an unlimited size.

Maximum User Count. The maximum number of users that can be registered for the domain. Enter zero for an unlimited number of users.

Note

Note that this does not apply to virtual domains that are based on the Windows NT user database or an external database. Furthermore, the displayed counts of users for domains that use the NT user database or an external database may not be correct.

Click **Save** to save the new virtual host configuration. Click **Exit** to close the "Virtual Host Configuration" dialog box.

9 After you have created the virtual host, you need to add user mail accounts. For information on creating and modifying user mail accounts, see "Working with User Mail Accounts" on page 60.

Additional Host Settings

Once the virtual host has been configured, it will appear in the left panel. Selecting the virtual host in the left panel, displays the host's **General** tab in the right panel. You can use this tab to alter the settings configured during the creation of the virtual host, and to access additional settings. The following options are available on this tab.

The first two items are not editable. They are:

Official Host Name. The name that will be used to address mail to the users on the mail host.

TCP/IP Address. The real or virtual IP address of the mail host.

Top directory. The name of the directory where the directories for users, lists, and web files for this host will be stored.

Host Aliases. Specify alternate host names for which you want the host to accept mail. For example, if the mail host name is mail.domain2.com, you can set an alias of domain2.com so that IMail Server accepts mail addressed to fred@mail.domain2.com and also fred@domain2.com. Multiple aliases are separated by a space.

Default Max Mailbox Size. Enter the default maximum size in bytes (characters) for the total of all mailboxes in a user's account. If the total size exceeds the maximum, any new mail is returned to the sender. Enter zero for an unlimited size.

This value is the default limit used when the Max Mailbox Size value, for a user's account, is set to zero. Changing this value will automatically change the limit for all user accounts on the host with zero for the Max Mailbox Size value. Otherwise, the user's Max Mailbox Size value will override.

Single Message Max Size. Enter the maximum size (in bytes) of a single message. Messages that exceed this size are returned to the sender. Enter zero for unlimited size.

Max Outbound Msg Size. The maximum size of an outbound message. Any message that is larger than the size entered here, will be bounced.

Full Mailbox Notify%. If there is anything entered in this box, the user will be notified when their mailbox is within a certain percentage of being full. For example, if 80 is entered in this box, the user will receive an e-mail when their mailbox is 80% full. The user will get a maximum of one message a day, for three days.

The e-mail message that is sent to the user is configurable. The text for this message can be customized by creating a *Notify.txt* file which should be placed in the top directory of the domain. If there is no *Notify.txt* file, the notification will contain the standard text as follows:

"User<!--imail.user--> Host <!--imail.host--> Your mailbox is nearly full, please remove some messages. If you have any questions, see your system administrator." The two tags will be replaced with the User ID and the domain.

Full Mailbox Notify Address. Enter the address of an additional address where an e-mail will be sent when a user's mailbox is almost full. For example, this could be the system administrators address.

Default Max Messages. Enter the default maximum number of messages (the total for all mailboxes) that will be allowed in a user's account. If the maximum is exceeded, any new mail is returned to the sender. Enter zero for an unlimited number.

This value is the default limit used when the Max Messages value for the user's account is zero. Changing this value will automatically change the limit for all accounts on the host which have zero for the Max Mailbox Msgs value. Otherwise, the user's Max Mailbox Msgs value will override.

Max Users. Enter the maximum number of users that can be registered for this mail host. Enter zero for an unlimited number. The box next to this setting displays the number of users that exist on the host.

Note

This setting does not apply to virtual domains that use the NT user database. The displayed counts of users for domains that use the NT user database may not be correct.

Virus Scanning. If you have IMail Anti-Virus installed, you will see a Virus Scanning option, which allows you to enable and disable virus scanning for the current domain only. If you do not have IMail Anti-Virus installed, you will not see this option.

Sub-mailbox Creation. This setting allows the administrator to specify what to do when a message arrives for a user and is addressed to a sub-mailbox which does not exist. Select one of the following actions:

- **Create.** Creates the sub-mailbox and delivers the message.
- **Send to Inbox.** Does not create the sub-mailbox. Instead the message is delivered to "main".
- **Bounce.** Bounces the mail as an invalid user.

In the User Database Type area, select one of the following:

- IMail Database
- NT Database
- External Database

Setting Up DNS for Multiple Mail Hosts

For background information about DNS setup, see “Appendix I: Mail Servers and the DNS” on page 315.

For a virtual host with an IP address, you need to make the following entries in your DNS:

- An MX record for the mail domain (for example, *mail.domain2.com*). The MX record identifies the host name of the virtual host.
- An A record for the host name of the virtual host. The A record maps a host name to an IP address.
- A PTR record for the IP address of the virtual host. The PTR record maps an IP address to the host name and is used for reverse lookups.

As an example, the DNS entries for a virtual host for which the host name in IMail Server is *mail.domain2.com* would look like:

```
SOA
$ORIGIN
...
domain2.com
```

```
     IN MX 10 mail.domain2.com    (MX record)
     mail IN A 156.21.50.10       (A record)
                                  (PTR record
5.50.21.156.in-addr.arpa.,type = PTR
 host = mail.domain.com
```

A DNS lookup for mail sent to *user@domain2.com* would find that the mail must be sent to the host *mail.domain2.com*.

For a virtual host without an IP address, you need to make only one entry in your DNS: an MX record for the mail domain (for example, *mail.domain3.com*). This MX record identifies the host name of the primary mail host. As an example, the DNS entries for a virtual host without IP address for which the host name is *mail.domain3.com* would look like:

```
SOA
$ORIGIN
...
domain3.com
     IN MX 10 mail.domain.com
```

A DNS lookup for mail sent to *user@domain3.com* would find that the mail needs to be sent to the host *mail.domain.com*.

Changing the IP Address of a Domain

Before changing the IP address of a domain, you should first back up your IMail registry to a file in *IMail Administrator/localhost/General/Backup*.

1 If you have not done so ,bind the new IP address to the NIC card in *Control Panel/Network/Protocols/TCP|IP/Properties*.

2 Run Regedit and locate the following key:

HKEY_LOCAL_MACHINE/Software/Ipswitch/IMail/Domains

3 If you see keys for both the old and the new IP addresses then delete the old one. First, make sure that the “Official” value under the new IP address key shows the correct hostname. If you only see a key for the old IP address you can rename that key to the new IP address.

4 Highlight the hostname key associated with that IP address, and make sure its “address” value is set to the correct (new) IP address for that host. If it is not, then change it.

5 You must then, stop and restart all services in order for the changes to go into effect.

Setting Up IMail Server as a Mail Gateway

You can set up IMail Server to function as a mail gateway for another mail server. This means that mail for the other server is sent and received through the IMail Server. Often, people will set up a mail gateway because their mail server uses a dial-up connection and is not always connected to the Internet.

If you want IMail Server to be a gateway for another mail server, the other server must be running SMTP.

To set up IMail Server as a gateway for another mail server, check the following:

- The mail domain (for example, *domain2.com*) for which IMail Server is a gateway does not appear in IMail Server.
- User accounts for the mail domain are on the other server.
- The MX record for the mail domain must point to the IMail Server host. Thus, mail addressed to that domain will come to the IMail Server host. (This MX record is in the DNS used by the other mail server.)
- The IMail Server host must be able to resolve the domain name to the IP address of the other SMTP server. This is accomplished by making an entry for the domain name and IP in the hosts file (*\winnt\system32\drivers\etc\hosts*) on the IMail Server host.
- This works because IMail Server checks the hosts file and IP information before checking the DNS server. IMail Server queues the mail until it is delivered to the other server, or until the Queue Timer setting multiplied by the Number of Tries has elapsed. (The **Queue Timer** and number of tries are set on the **SMTP** tab).

- If you are using any of the "**Relay Mail for**" options on the **SMTP Security** tab, and want to relay outgoing mail for another mail server, the address of the other server must be added by using the "Addresses" button, and entering the remote IP's into the table.

The following example shows how you can set up IMail Server to accept mail for a domain (*domain2.com*) and forward all mail for this domain to another SMTP server. Assume the following:

```
Other mail domain name              domain2.com

Host name of other SMTP server:     other_SMTP_server
IP address of other SMTP server:    156.21.50.240

Host name of IMail Server:          my_imail_machine
IP address of IMail Server:         156.21.50.10
```

When Windows NT/2000 looks up a domain name, it first searches the *\winnt\system32\drivers\etc\hosts* file. So, in the *hosts* file point the domain name to the IP address of the other SMTP server:

156.21.50.240 domain2.com

You can use the ETRN command to manually retrieve mail from the ISP's mail server. See "Using ETRN to Retrieve Mail" on page 54 for more information.

Setting up a Dial-up Internet Connection

You can create a dial-up Internet connection from IMail Server to your Internet Service Provider (ISP), allowing you to receive mail from an account with your ISP.

IMail Server does not perform dial-up functions or spawn off dialing commands. To start your RAS/PPP connection to your ISP, you need to either use a scheduling program or manually start the connection.

IMail Server uses the TCP/IP transport on Windows NT/2000; it does not configure the Windows NT/2000 TCP/IP transport. If you need to set up a RAS/PPP connection, refer to your Windows NT/2000 Help.

Receiving Mail from an Internet Service Provider

IMail Server is designed to work on a 7-day, 24-hour Internet connection, but you can also set up IMail Server to support dial-up connections.

When using a dial-up connection, your inbound mail from the Internet has to be stored somewhere on the Internet, usually with your ISP. Your ISP can store your mail in several ways. Three of the more popular ways that ISPs store mail for users are:

- Method 1: The ISP sets up individual mail accounts on the ISP computers. This method usually makes use of the POP3 mail protocol to read or retrieve mail — each user dials up the ISP and either reads or downloads their mail.
- Method 2: The ISP sets up individual mail accounts on the ISP computers, but the ISP forwards all the mail for your users to your mail server when your dial-up connection is up. This method uses the ISP's Internet domain name.
- Method 3: You have a registered Internet domain of your own, and you register your domain to point to the ISP computer. Your ISP stores your incoming mail and forwards it to your mail server when your dial-up connection is up.

To register your own domain, contact your ISP. In most cases, they will do the work for you. All you have to do is come up with a name.

If you use Method 1, then to use IMail Server, you will have to change to either Method 2 or 3 to receive mail from your ISP. IMail Server cannot log into individual mail accounts on your ISP mail server, retrieve the mail and then parse the mail correctly. An Internet standard for this does not exist.

Setting Up the Server for Dial-up Access

Setting up IMail Server using a dial-up connection is the same for both Methods. Use the following procedure to set up your IMail Server computer:

1 Create mail accounts for users on the IMail Server computer. For more information, see "Working with User Mail Accounts" on page 60.

  If you are use Method 2, the users' names need to be the same on both the ISP's computer and your IMail Server computer.

2 Tell Windows NT/2000 about your e-mail domain name.

When Windows NT/2000 looks up a domain name, it first searches the *\winnt\system32\drivers\hosts* file, then, if there is no match, Windows NT/2000 asks a Domain Name Server (DNS) for the IP address for the domain name.

This creates a problem, as your Windows NT/2000 computer has a different IP address than your ISP's computer. When IMail Server looks at the incoming mail, it will look up the domain name to which the e-mail is addressed. If the domain name points to your ISP's computer (your ISP's IP address), then IMail Server will send the mail back to your ISP's computer (which it thinks is correct). Mail will be bounced back and forth until one of the computers sends the mail message back to the original sender.

To avoid this problem, set up the domain as a virtual host, then add the domain name to which your incoming mail is addressed (either your ISP's if Method 2, or your own if Method 3) to the **Aliases** text box in the "Virtual Host Configuration" dialog box, and make this domain name point to the IMail Server computer's IP address.

For example, if you are using Method 2, and the computers involved have the following addresses and names:

```
ISP's IP address:        156.21.50.1
ISP's domain name:       isp_are_us.com
IMail Server IP address: 156.21.50.240
IMail Server Name:       my_imail_machine
```

You would make the following entries in the *\winnt\system32\drivers\hosts* file:

```
156.21.50.240            my_imail_machine
156.21.50.240            isp_domain_name.com
```

You can have multiple names pointing to the same IP address. This also helps if your computer is receiving mail for multiple domains. Just place each domain name in the hosts file pointing to the IMail Server computer's IP address.

If you are using Method 3, and the computers involved have the following addresses and names:

```
ISP's IP address:        156.21.50.1
Your Domain Name:        my_domain_name.com
```

```
IP address for
       my_domain_name.com:156.21.50.1
IMail Server Name:       my_imail_machine
IMail Server IP address: 156.21.50.240
```

...you would make the following entries in the *\winnt\system32\drivers\hosts* file:

```
156.21.50.240            my_imail_machine
156.21.50.240            my_domain_name.com
```

3 Unless you plan on maintaining a 24-hour/7-day dial-up Internet connection, you need to have your ISP spool all the mail for your company. Then, have your ISP set up their computer to try periodically sending mail to the IMail Server computer.

How often the ISP attempts to send mail to your server depends on how often your dial-up connection is up. Consider the following factors in determining queue times. The first factor is the most important.

- How long will your dial-up connection last (10, 20, 30 minutes)?
- How often will your ISP's computer try to send the spooled mail to your NT computer?
- How often will your NT/2000 computer try to send mail to the Internet?
- How much mail will you receive and send when you make your dial-up connection?

For example, if the connection time will be 20 minutes, and you will have relatively light traffic (50 received and 50 sent) and relatively short messages (no attachments, or large files), you could set up the queue times as follows:

```
Connection Time:                 20
ISP Queue Time:                  15
IMail Server Queue Time:         15
E-mail Quantity:                 50
received/50 sent (short messages)
```

In this example, the Connection Time is the amount of time your IMail Server is connected to the ISP's computer (this would be set in your scheduling program). The ISP Queue Time determines how often the ISP mail computer tries to send mail to the IMail Server). The IMail Queue Time determines how often IMail Server tries to send mail to the ISP or Internet (this is set on the **SMTP** tab).

To be sure your mail gets processed regardless of the connection time, make the queue times less than the connection time. If you expect to receive or send greater numbers of messages, or more lengthy mail than in the example, you can either increase the connection time, or decrease both queue times.

Alternatively, you can use the ETRN command to manually retrieve mail from the ISP's mail server. See "Using ETRN to Retrieve Mail" on page 54.

Remember that IMail Server does not do scheduling. You need to obtain a scheduler to have the connection automatically dial, connect, and disconnect.

Setting Up IMail Server as a Backup Mail Spooler

You can set up IMail Server to act as a backup spooler for a customer's mail server (if the customer's computer is down, the mail for his domain will collect on your IMail Server until his is back up). The customer's mail server must have a static, unchanging IP address.

To set this up, have the customer set his computer up to log into his ISP at intervals where he can catch the queue processing interval (**Queue Timer** setting on the **SMTP** tab) of your server. For example, if your queue timer is set for 30 minutes, have him connect to his ISP once every 20 minutes or so. He has to be online and ready to receive when your timer cycles.

Alternatively, he could Telnet to port 25 (the SMTP port) of your computer and issue the ETRN command with this format:

```
etrn his_domain.com
```

This will dump the queued mail to his computer.

In DNS, your server will be the secondary MX for his domain (lower priority), whereas his server will be the primary MX.

You must also make an entry in your *hosts* file (*\winnt\system32\drivers\etc\hosts*) which associates his IP address with his domain name.

```
his.i.p.address his.domainname
```

This way, IMail Server will attempt to deliver any mail it receives for that domain to his computer (bypassing the MX records in DNS, which point to itself and can create a mail loop).

If you are using IMail's SMTP security to prevent spammers from using your computer as a spam relay, add his server's IP address in the "[addresses]" dialog box in the **Mail Relay Options** on the **SMTP Security** tab.

For example, if the remote host's DNS is set up to receive mail for a primary domain, *mail.widgets.com*, and points to your IMail Server, *mail.domain.com*, as a backup server, then the MX record for the remote host's DNS will look like this:

```
MX
  10 mail.widgets.com
  20 mail.domain.com
```

When *mail.widgets.com* is down, mail is sent to your computer *mail.domain.com*. To relay mail for the *mail.widgets.com* domain, you need to specify its IP address in the **Relay mail for** option and also enter its host name and IP address in the *hosts* file on your IMail Server host.

Setting Up "Peer" IMail Servers

IMail Server lets you set up "peer" servers to allow users for a specific domain to be spread across multiple physical computers. This can be used when the mail traffic on your IMail Server system becomes heavy enough to slow down mail processing. How much traffic your mail server can handle will depend on your computer's hardware configuration.

How Peering Works

Suppose you have two systems set up as peer servers: both systems have IMail Server installed and each server has a portion of the user database for a single domain. When mail comes in for a user in the domain (for example, *user@ipswitch.net*), the sending server does a

DNS lookup and gets the host name and address of one of the two peer servers. The mail is sent to one of the peer servers. If the user is found on the peer server, the mail is delivered. If not, the peer server does an SMTP Verify to see if the user exists on the other server. If it finds the user, it forwards the mail.

Note

Do not select the **Disable SMTP VRFY command** (on the **SMTP Security** tab) when using peer servers. A peer server needs to use this command to verify a user that is on the other peer.

If either peer server is down, the other peer server will receive and hold mail for it until the first server comes back up.

Setup Procedure

You will need to purchase and install a copy of IMail Server Version 4.0.3 or later on each peer server.

To add one or more peer servers for an IMail Server domain:

1 Install a licensed copy of IMail Server Version 4.0.3 or later on each system that will function as a peer mail server.

2 In your DNS server, add MX records for the peer servers. (See the example that follows this procedure.)

3 In the *hosts* file on each of mail servers, make entries for the other servers.

4 On *each* system, use IMail Administrator to set up the Peer List as follows:

- Select **"localhost"** in the left panel. On the **General** tab, click the **Add Host** button. The "Virtual Host Configuration" dialog box appears.
- In the "Virtual Host Configuration" dialog box, select the mail host for which you want to add peer servers. This should be an actual host, not a virtual host.
- Click the **Peer List** button in the lower right of the dialog box. The Peer List dialog box appears.

- In the “Peer List” dialog box, enter the IP addresses of the peer servers. IP addresses for a peer server should be for actual (not virtual) hosts. Enter an IP address into the text boxes and click **Add** to add it to the peer list.
- Make sure that the peer list exists on each computer that receives mail for a domain.

Note

You do not add the IP address of the local system to the peer list; you enter only the other peers. (See the example that follows this procedure.)

5 In the “Virtual Host Configuration” dialog box for each mail server, in the **Alias** box, make sure the primary domain for sending and receiving mail (for example, *ipswitch.net*) is the only entry. The entry in the **Alias** box,. must be the same on all servers. Note that this alias cannot be a primary domain associated with a particular host. Do not enter IP addresses in the **Alias** box.

6 For each mail server, make sure the **Default Mail Host** text box (on the **SMTP** tab) is empty when using peer lists.

Example of Setting Up Peer Servers

For example, suppose you have one domain (called *ipswitch.net*) and three servers. All three servers accept incoming mail on the same priority and all have a portion of the user database. You would make the following entries in your DNS:

DNS entries:

```
-------------
ipswitch.net

IN   MX 10 mail1.ipswitch.net
IN   MX 10 mail2.ipswitch.net
IN   MX 10 mail3.ipswitch.net

mail1      IN  A  1.1.1.1
mail2      IN  A  2.2.2.2
mail3      IN  A  3.3.3.3
```

You create the following peer lists in the IMail Server software on the three servers:

Peer list on mail1:

```
2.2.2.2
3.3.3.3
```

```
Peer list on mail2:
1.1.1.1
3.3.3.3
```

Peer list on mail3:

```
1.1.1.1
2.2.2.2
```

In the *hosts* file on the three servers, make the following entries:

```
Host file for mail1:
2.2.2.2  mail2.ipswitch.net
3.3.3.3  mail3.ipswitch.net

Host file for mail2:
1.1.1.1  mail1.ipswitch.net
3.3.3.3  mail3.ipswitch.net

Host file for mail3:
1.1.1.1  mail1.ipswitch.net
2.2.2.2  mail2.ipswitch.net
```

On *each* of the three computers, make sure:

- The domain (in the form *ipswitch.net*) is the only entry in the **Alias** box in the "Virtual Host Configuration" dialog box.
- The **Default Mail Host** text box on the **SMTP** tab is blank when using peer lists.

Note

You will be unable to use the "nobody" alias, to direct mail for non-existent users, if you use peering.

Using ETRN to Retrieve Mail

There are several cases where you or your customer may want to manually retrieve mail from another mail server:

- If your IMail Server is set up as an SMTP mail gateway or as a backup server for another mail server, then IMail Server stores mail for that domain until the other server is online, or, until the **Queue Timer** setting multiplied by the number of tries has elapsed. (Both values are set on the **SMTP** tab.) The administrator of the other server can retrieve mail manually at any time.
- If your IMail Server dials in to an ISP's mail server, then the ISP's server stores mail for you. You can retrieve it manually at any time.

To retrieve mail manually:

- Use a Telnet program to connect to port 25 (the SMTP port) on the other mail server, and then issue the ETRN command for their domain. For example:

  ```
  ETRN @domain2.com
  ```

  Or

  ```
  ETRN mail.domain2.com
  ```

  The first command retrieves all queued mail for the domain. The second command retrieves all queued mail for the mail host.

Adding a Host Based on an External Database

IMail Server can use an external database to register and authenticate users on a particular mail host. Users that you subsequently add to, and delete from, that host using IMail Server will also be added and deleted from the external database, and vice versa.

Before you use an external database for a mail host, use the Windows Control Panel to make sure there is a System DSN (Data Source Name) that points to a valid database name. See your Windows NT/2000 and database documentation for information on the System DSN.

Once you have verified the System DSN that points to the database you want to use, the next step depends on whether you are creating a new host or converting an existing host to an external database.

Configuring the Primary Host

If you have just installed IMail Server for the first time as described in "Chapter 2: Installation" on page 15, and you have based the primary host on an external database, you are now ready to configure the host.

1 Start IMail Administrator and select "**localhost**" in the left panel.

2 Click the **Add Host** button.

3 Select the primary host in the list.

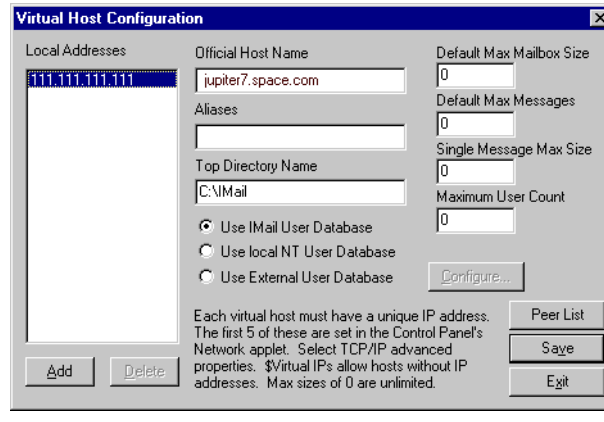
4 Click the **Configure** button. Proceed to "Configuring the External Database Interface" on page 57.

Creating a Host Based on an External Database

To create a virtual host based on an external database:

1 Start IMail Administrator and select "**localhost**" in the left panel.

2 The **General** tab appears. Click the **Add Host** button. You see the "Virtual Host Configuration" dialog box.



3 Click **Add**. A virtual host name (i.e. **$virtual001**) appears in the **Local Addresses** list.

4 Select **Use External User Database**.

5 Click the **Save**.

Note

It is essential to click **Save** *before* clicking **Configure**.

---

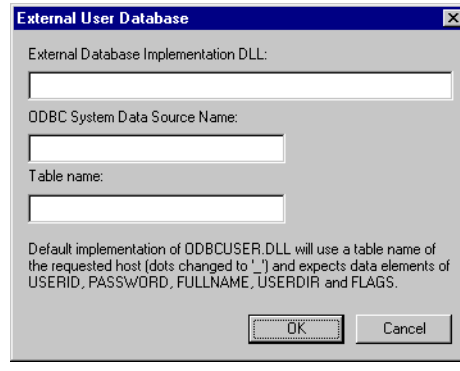
6 Click **Configure**. The **External User Database** dialog appears.

Configuring the External Database Interface

The interface between IMail Server and the external database is accomplished via a dynamic link library (*DLL* file); IMail Server comes with a sample .dll that can be used for this purpose: ODBCUSER.DLL. This *DLL* uses the ODBC method, but can be modified to support *any* external database method. (The complete source code for this *DLL* is provided upon request from Ipswitch.)

Note

When you use an external database, any IMail service you run (except the System Logger Service) must be set up (using the Control Panel **Services** application) so that the account that IMail Server runs under has access to the external database.



To configure the external database interface:

7 Specify the full path to *ODBCUSER.DLL*, or to any *DLL* that supports the functions: GetUserEntry, SetUserEntry, DeleteUserEntry, AuthorizeUser, GetFirstUserEntry, and GetNextUserEntry. (These are defined in the *odbcuser.h* file.)

8 Specify the **ODBC System DSN** for the database where the user information is stored. IMAILSECDB is the default name that the IMail ODBC link uses.

Note

For users using SQL 7.0 or above: In the **ODBC Data Source Name** input the line: *IMAILSECDB; UID=username; PWD=password*. The user name and password need to be the user ID and password for the SQL database and not an IMail Server account.

9 Specify a **Table name** for the data. If the field is blank or contains [default], the host name is used with dots replaced by underscores.

10 Click **OK**.

You can use up to ten different *DLLs* from one IMail Server system. An unlimited number of tables can be accessed by a *DLL*. Each *DLL* can be named anything you wish and the name of the *DLL* must be specified to IMail Server as described in Step 2 above.

Chapter 4: User Mail Accounts

IMail Server provides several tools for administrators to use in creating and maintaining user mail accounts. Administrators can:

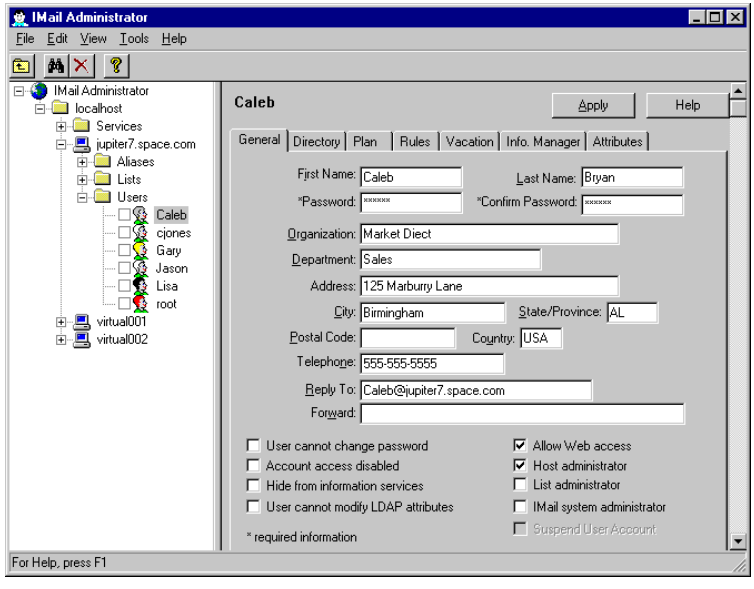
- Add, modify, and delete users
- Add, modify, and delete standard, group, and program aliases
- Forward mail
- Set mailbox size limits
- Set up vacation processing
- Change user information for the LDAP database
- Set user information that is sent in response to Finger requests
- Set up delivery rules for incoming mail (This is covered in the next chapter, “Chapter 5: Mail Processing Techniques” on page 81.)

Normally, you will add and modify user mail accounts using IMail Administrator. In addition to the IMail Administrator, you can maintain user accounts using:

- Web Messaging (if you log on as a host or system administrator). For more information, see “Chapter 6: IMail Web Messaging” on page 107.
- *adduser.exe*, a command line program for adding batches of users whose names and passwords are stored in a text file (for those hosts that use the IMail database or an external database). For more information, see “Appendix C. Command Line Applications” on page 259.

Working with User Mail Accounts

Each user has a user mail account. When you select a user name in the left panel, you see user properties on the right.



Adding User Mail Accounts

If a mail host uses either the IMail Server database or an external database, you can add user mail accounts using IMail Server. (However, if the host uses the Windows NT Database, you cannot add or delete accounts using IMail Server; you can only add and delete users using the Windows NT User Manager.)

To add users one at a time (assuming that **Use Wizards** on the **Tools** menu is turned off):

1 In the left panel, expand the "**localhost**" and mail host folders and select the "**Users**" folder.

2 In the right panel, click **Add User**.

3 In the "New User" dialog box, enter the **User ID** and click **OK**. (A User ID must be between 3 and 30 characters. It must consist of digits and letters only, and cannot contain spaces.)

Note

The user ID can represent a special mail account that doesn't belong to a particular user, but accepts routine mail requests for general information. For ideas on how to use such an account, see "Using the Info Manager" on page 101.

4 Make sure the user's ID is selected in the left panel, and that the **General** tab is visible on the right.

5 Enter the user's **First Name** and **Last Name**.

6 In the **Password** box, enter a **Password** and confirm it. The password must be between 3 and 30 characters.

7 (Optional) Enter the user's **Organization**, **Department**, **Address**, **City**, **State/Province**, **Postal Code**, **Country**, and **Telephone** number.

8 In the **Reply To** box, you can enter an a different e-mail address if you want replies to go to a different address. This box can be used to enter an e-mail address that omits the computer name, if you are sure the rest of the address is a fully-qualified domain name. For example, if the complete e-mail address is *duckie@mail.willow.com*, you can enter *duckie@willow.com*.

Note

This setting is for Web Messaging only.

9 If you want to automatically forward this user's mail to another user account, enter a complete mail address, in the **Forward** box. To forward mail and keep a copy in this user's account, precede the forwarding address by a period and a comma, for example, `.,cecil@flores.com`. Separate multiple addresses with commas. For more information, see "Forwarding Mail to Another User Account" on page 73.

You can also enter a beeper or pager alias here to activate a beeper or pager when the user receives mail. For more information, see "Chapter 18: Sending Mail to a Pager or Beeper" on page 235.

10 Set the following advanced options:

Turn on **User cannot change password** if you do not want the user to change their password from older Eudora or NuPop mail clients. For more information, see “Chapter 6: IMail Web Messaging” on page 107.

- Turn on **Account Access Disabled** to prohibit the user from accessing the account. This allows you disable the account without changing the user's password or removing him from the system. This is used mainly when the host is based on the Windows NT database and not everyone in that database is supposed to have access to e-mail.
- Turn on **Hide from information services** to prevent the distribution of any information about the user through Finger, Whois, or LDAP (if you have any of those servers running).
- Turn on **User can’t modify LDAP attributes** to prohibit the user from modifying their LDAP attributes (name, address, organization, etc.).
- Turn on **Allow Web access** to allow this user to access his/her account via the Web Remote Administration utility (provided the utility is configured) as well as Web Messaging and Web Calendaring.
- Turn on **Host administrator** if you want this user to add, modify, or delete users or aliases (except program aliases) on this mail host. To allow use of the web utilities to administer hosts, **Allow Web Access** must also be selected.
- Turn on **List administrator** if you want this user to add, modify, or delete list-server mailing lists.
- Turn on **IMail system administrator** to allow this user all IMail functions, including the creation and administration of virtual hosts. In order for the system administrator to use the web interfaces for administration, **Allow Web Access** must also be selected.
- **Suspend User Account** will automatically become enabled if a user’s web access becomes suspended. If you wish to re-enable web access for the user, deselect the **Suspend User Account** checkbox.

Note

You cannot suspend a user account by enabling the **Suspend User Account** option. If you wish to suspend a user account, then select **Account Access Disabled**.

11 Click the **Apply** button.

The user ID is added to the list of registered users for the host. The user can now receive mail through IMail Server at the specified host. For example, if you added the user *fred* to the virtual host *petra.com*, the user can now receive mail addressed to *fred@petra.com*.

You can now set up special processing for this user; the options are described in the following sections:

- "Forwarding Mail to Another User Account" on page 73
- "Working with Mailboxes" on page 66
- "Setting Up a Finger Plan" on page 69
- "Setting Up Delivery Rules" on page 83
- "Setting Up a Vacation Message" on page 70
- "Entering LDAP Directory Information (Attributes)" on page 72

Importing NT Users

If a host uses the IMail database for user mail accounts, you can import users from the NT database to add them to the IMail database. When you do this, the imported users are not linked to the Windows NT database and the NT passwords are not imported.

Imported Windows NT users have the same user IDs as in the NT database, but each is given a default password of *password*. However, by default, IMail won't accept user names with the ampersand (&). If any user names have an ampersand character, see "Advanced Options" on page 151.

To import NT users:

1 In the left panel, expand the mail host and select the "**Users**" folder.

2 In the right panel, click **Import NT Users**. You see a dialog box that lists the users in the Windows NT database.

3 Do one of the following:

- To add user and passwords one at a time, select a user, enter a password, and click **Add Selected Users**. Repeat for each user you want to add.
- To add a number of users at one time with the same initial password, select the users you want to add, set the initial password for all the selected users, and then click **Add Selected Users**. The password must be between 3 and 30 characters.

4 When you are finished importing users, click **Exit**.

Deleting a User Mail Account

To delete a user mail account:

1 In the left panel, expand the mail host and "**Users**" folders, and then select the user name.

To select multiple users for deletion, you can select the check boxes next to the name of each user you want to delete.

2 In the left panel, right-click to display the pop-up menu, and then select **Delete**.

Finding Orphan Mail Accounts

When you delete a user, the user's icon no longer appears in the left panel of IMail Administrator, but the user's directory may still remain on the IMail system. This is called an "orphan mail account."

To find orphans and delete their directories from the system:

1 In the left panel, expand the host name, and then select the **"Users**" folder.

2 Click the **Find Orphans** button. The Orphans dialog box lists any orphan user mail accounts.

To delete an orphan's directory and messages, select a user name, and then click **Delete**. To delete *all* orphan directories, click **Delete All**.

3 Click **Close** to close the dialog box.

Setting Defaults for New Users

In IMail Administrator, you can set the defaults to be used by all new user mail accounts. To set default properties for new users, expand the host name and select the **"Users**" folder. The default user properties appear in the right panel.

- **Maximum Mailbox Size.** The maximum size of a user mailbox. This value will be stored as the new user's Max Mailbox Size value when the account is created. To use the host's default value, leave this option set to zero. Changing this setting will have no effect on existing user accounts.
- **Maximum Messages.** The maximum number of messages that can be stored in a mailbox.This value will be stored as the new user's Max Messages value when the account is created. To use the host's default value, leave this option set to zero. Changing this setting will have no effect on existing user accounts.

Note

The **Maximum Mailbox Size** and **Maximum Messages** options for the user are seperate from the **Default Maximum Mailbox Size** and **Default Maximum Message Size**, that are enabled for the Host on the Host's General tab. For information on how these function with relation to each other, see "Additional Host Settings" on page 41.

- **User cannot change password.** Prevents users from modifying their passwords.
- **Account Access disabled.** Disables all user accounts, preventing users from logging in.
- **Hide from information services.** Automatically hides all user information from information services.
- **User can't modify LDAP attributes.** Prevents all users from modifying their LDAP attributes, such as name, address, organization name and phone number.
- **Allow Web Access.** Allows all users to access web functions such as IMail Web Messaging and IMail Web Calendaring.
- **Host administrator.** Allows all users to have host administrator privileges.

- **List administrator.** Allows all users to have list administrator privileges.
- **IMail System administrator.** Allows all users to have system administrator privileges.

These settings will be used by all mail accounts subsequently created on any host in the system. The only exception is the "**set reply to**" setting. This setting applies to existing accounts only. All new user accounts will be set to the Official Hostname of the domain.

Notes:

- It may be necessary to close and re-open IMail Administrator in order to see your changes.
- To change the global settings for *existing* users, you must use the **Global User Changes** button. For more information, see "Global Settings for Existing Users" on page 75.

Working with Mailboxes

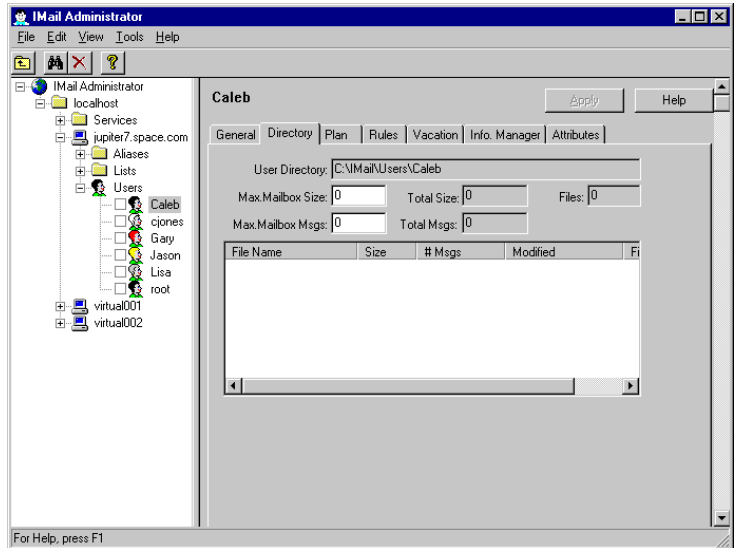
You can manage users' mailboxes by setting limits on mailbox size and message count, and by deleting messages older than a specified date.

Note that IMail Server does not automatically create the mailbox files for users. Mailboxes are not created until the first time the user receives mail or accesses his or her mailbox with a POP3 client. (This prevents the creation of user files for users who never use IMail Server.) Certain settings, such as mail forwarding, vacation processing, delivery rules, and Information Manager auto-responses cannot be made until a user's mailbox files exist.

To view mailbox directories and set limits:

1 In the left panel, expand a mail host and "**Users**" folder, and then select a user. The user properties appear in the right panel.

2 Click the **Directory** tab.



You can view or change the following settings:

User Directory. The user's directory name in the IMail user database. You cannot edit this.

Max. Mailbox Size. This is the maximum size allowed, for *all* mailboxes, in the user's account. If new mail will cause the total size to exceed this maximum, the mail is returned to the sender. Enter zero to use the host defaults; if the host default is also set to zero, the mailbox size is unlimited. For more information about host defaults, see "Setting Defaults for New Users" on page 65 and "Additional Host Settings" on page 41.

Max. Mailbox Msgs. This is the total number of messages for *all* mailboxes, allowed for the user's mail account. If new mail would cause this maximum to be exceeded, the mail is returned to the sender. Enter zero to use the host defaults; if the host default is also set to zero, the mail box size is unlimited. For more information about host defaults, see "Setting Defaults for New Users" on page 65 and "Additional Host Settings" on page 41.

Total Size (information only). The current total size (in bytes) of all mailboxes in the user's account.

Total Msgs (information only). The current total number of messages in all mailboxes in the user's account.

Files (information only). Total number of files in user's account.

3 Click **Apply** to save any changes.

The **Directory** tab also list all mailboxes (*.mbx*) in the user's directory on the IMail Server. For each mailbox, the list shows the *.mbx* file name, the size (in bytes), the number of messages it contains, and the last modified and first modified dates. You can delete or rename mailboxes, delete messages by date, or refresh the mailbox list information. To use the mailbox functions:

1 Expand a mail host and "**Users**" folder, select a user, click the **Directory** tab, then select a mailbox.

2 Select one of the following from the right-mouse menu:

Delete Mailbox. Deletes the currently selected mailbox.

Delete Msg's by Date. Automatically deletes message from the mailbox according to a specified date or age (number of days).

Rename Mailbox. Displays a dialog box in which you can enter a new name for the mailbox.

Refresh. Refreshes the list of mailboxes.

Combining Mailbox Names with User IDs

When addressing mail to a user, a mailbox name can be appended to the user ID by using a hyphen. For example,

dave-music@domain.com

The mailbox name cannot contain hyphens. If a user ID contains a hyphen, IMail Server will check to see if it is a valid user ID. If it is not a user ID, the characters following the hyphen are interpreted as a mailbox name.

If the mailbox name does not exist, it is created on the IMail Server system (but not on the user's system). This is the only method an administrator can use to create user mailboxes.

Users with POP3 mail clients can access alternate mailboxes using the userid-mailbox convention when they log on; for example, the user in the example above could log on as dave-music. Note, however, that only one POP3 mailbox can be accessed at a time.

If a user logs in with an IMAP4 client or with Web Messaging, he will see the mailboxes in the list of available mailboxes.

Setting Up a Finger Plan

The Internet Finger protocol lets Internet users request information that an administrator or user wants to make available; the information must be stored in a "Plan" file. The contents of the file are returned in response to Finger requests from other hosts, provided the system administrator enables Finger and allows the user's Plan to be presented. The Plan contents are displayed in addition to the login user name and other information displayed by the Finger server. (Note that WS_Ping ProPack includes a Finger client.)

IMail Server comes with a Finger server. The system administrator can disable the transmission of any information about any user through the Finger protocol by turning on **Hide from information services** on the user's **General** tab.

To create or modify a Finger Plan:

1 Start IMail Administrator if it is not currently running. In the left panel, select a host name and then a user.

2 Click the **Plan** tab. The Finger properties appear.

3 Enter any information you desire to make publicly available to Finger clients. The information is stored in a file named *plan.ima* in the user's home directory.

4 Click **Apply**.

IMail sends information in response to a Finger request if the file named *plan.ima* exists in a user's home directory; the contents of that file are sent. (However, the system administrator can disable the transmission of any information as described above.)

Once a Finger plan has been set up for one user, the *plan.ima* file can be copied to the home directories of other users. See "Applying User Settings to Other Users" on page 74.

Note

Users can modify their Finger information in Web Messaging by selecting "Change Finger Information" on the Menu page.

Setting Up a Vacation Message

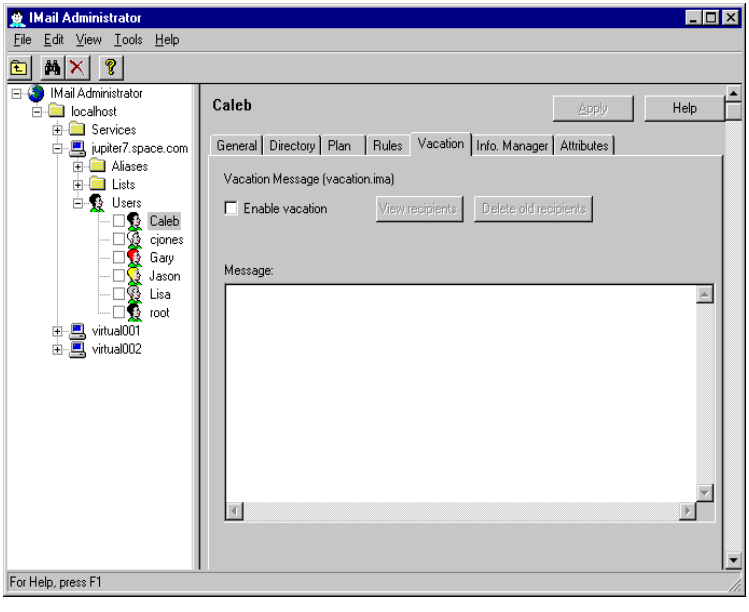
You can set up a vacation message(*vacation.ima*) that will be mailed *once* to each person that sends mail to you. Each time a vacation message is sent, the recipient's e-mail address is saved in a list of recipients, so that IMail Server can track who has already received the vacation message. (If mail is received from an e-mail address that already appears in the recipient list, the vacation message is not sent again.)

Setting Up a Basic Vacation Message

To set up a vacation message:

1 In the left panel, expand a host and the "**Users"** folder, and then select a user. The user properties appear in the right panel.

2 Click the **Vacation** tab.



3 Turn on **Enable Vacation**.

When the user returns from vacation, you can turn off **Enable Vacation**.

4 In the **Message** area, enter the message to send as a reply to mail while the user is away.

5 If a vacation message has already been in use, you have the following options:

- Click the **View Recipients** button to see what e-mail addresses have received the vacation message.
- Click the **Delete old recipients** button to clear the recipients list. (You might do this if the user takes frequent vacations and has a standard vacation message that gets enabled each time: you would **Delete old recipients** each time you re-enable the vacation message for a new vacation.)

6 Click **Apply**.

When you enable the vacation feature, IMail Server stores the message in the *vacation.ima* file. The presence of this file in a user's home directory activates the vacation processing feature. The contents of this file are mailed to those who send mail to the user. Therefore, once a vacation message has been set up for one user, the *vacation.ima* file can be copied to the home directories of other users. See "Applying User Settings to Other Users" on page 74.

Note

Users can also set up vacation messages in Web Messaging by selecting "Change Vacation Message" on the Menu page.

Viewing the List of Sender E-mail Addresses

IMail Server maintains a file (*vacation.snt*) that lists addresses to whom the vacation message has been sent. If you want to view the list, click **View recipients** on the **Vacation** tab.

Clearing the List of Sender E-mail Addresses

If you want to clear the list of sender e-mail addresses in the *vacation.snt* file, click **Delete old recipients** on the **Vacation** tab and the *vacation.snt* file is deleted when you click **OK**.

Sending a Message in Response to Every E-Mail

Instead of sending just one response to each sender (no matter how many messages the sender mails to the vacationing person), you can also send a message in response to *each and every* e-mail received, regardless of whether the sender has been previously notified of the vacation or not. To do this, you use the Info Manager feature as described in "Using the Info Manager" on page 101.

Entering LDAP Directory Information (Attributes)

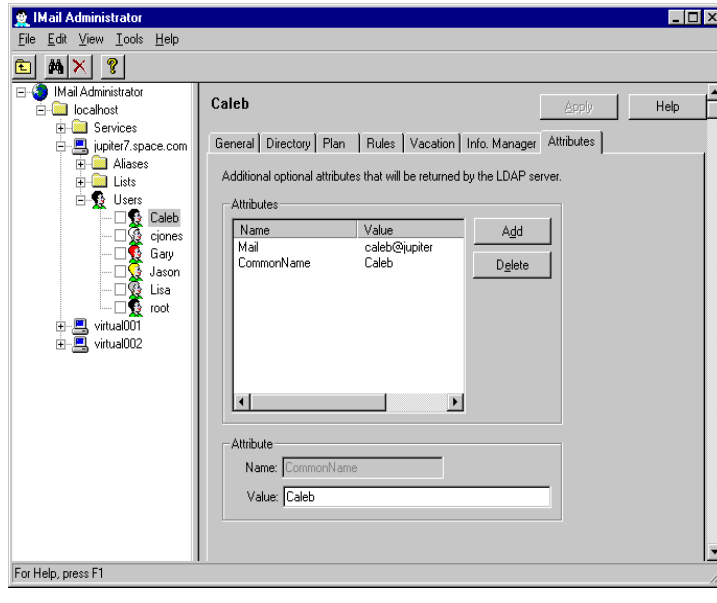
The Internet LDAP protocol enables the publishing of directory information (such as address books) over the Internet. IMail Server provides an LDAP interface to the IMail user database. (The IMail user database includes standard LDAP attributes such as name, address, organization name, phone number.)

LDAP information is made available to any LDAP-enabled client. (For example, WS_Ping ProPack includes an LDAP client and can be used to test the IMail LDAP server.) For more information on the LDAP server and LDAP data, see “Chapter 12: LDAP Server” on page 171.

To enter LDAP information for a user:

1 In the left panel, expand a mail host folder and the “**Users**” folder, and then select a user. The user properties appear in the right panel.

2 Click the **Attributes** tab. You see the following dialog box.



The list contains the most common attributes used in an LDAP entry. Other attributes can be defined by the system administrator or the user. The **Name** box at the bottom of the list shows the currently selected attribute. The **Value** box shows the entry for the currently selected attribute

To add an attribute (for example, shoe_size or marital_status), click **Add** and enter the attribute in the text box.

3 To modify an attribute, select it and edit it in the text box.

4 To delete an attribute, select it, and then click **Delete**.

5 When you have finished making entries, click **Apply**.

Note

Users can also update their own LDAP information in Web Messaging by selecting “Change User Information” on the Menu page.

Forwarding Mail to Another User Account

IMail Server can be set up to automatically forward a user’s mail to another user account. (Users can also set up forwarding in Web Messaging by selecting “Change Mail Forwarding Information” on the Menu page.)

To set up mail forwarding for a user:

1 In the left panel, expand the mail host and “**Users**” folders, and then select a user.

2 Click the **General** tab.

3 Enter an e-mail address in the **Forward** text box.

If you want to send a user’s mail to another user on the same host, enter the simple user ID (*userid* instead of *userid@domain.com*). To send the user’s mail to a different host, enter a complete mail address (*userid@domain.com*).

To leave a copy of a message in the user’s mailbox and forward a copy to another user, precede the address with a period and comma (.,) using the format: .,userid@host.domain. To forward to multiple users, separate each mail address with a comma.

4 Click **Apply** to apply the change.

IMail Server stores the address in a file named *forward.ima* in the user's directory. Once mail forwarding has been set up for one user, the *forward.ima* file can be copied to the directories of other users. See "Applying User Settings to Other Users" on page 74.

To turn mail forwarding off, make sure the text box is empty and click **Apply**.

Note

If a user has Forwarding set, any message that is saved to the Draft folder in Web Messaging will automatically be sent to the Forward address at the same time that it is saved. If you do not want this to occur, make sure that the Forward field does not contain text before saving a message to the Draft folder.

You can also use the **Forwarding** box to have IMail Server either forward a user's mail to a pager, or send a beeper notification that mail has arrived. For more information, see "Chapter 18: Sending Mail to a Pager or Beeper" on page 235

Applying User Settings to Other Users

If you have set up vacation processing, Finger plan information, delivery rules (covered in the next chapter), the Info Manager (also covered in the next chapter), or mail forwarding for one user mail account, you *could* enter the same settings to another user mail account by selecting the other account and entering the appropriate information.

However, because these features are activated by the presence of a particular file in a user's directory, you can also duplicate settings by copying *vacation.ima*, *plan.ima*, *rules.ima* (and any *.rul* files), *main.inf*, or *forward.ima* files from one user's directory to the directories of other users.

Global Settings for Existing Users

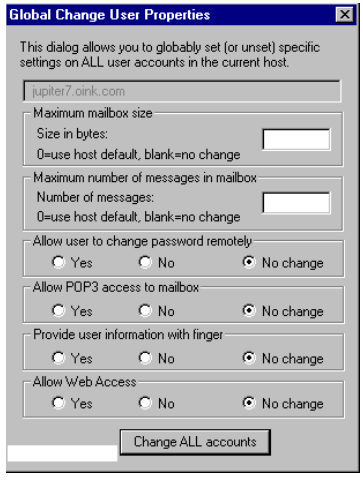
IMail Administrator lets you make global changes to *existing* users.

To set global settings for existing users:

1 Select the **Users** folder under the desired host name.

2 Click the **Global User Changes** button.

You see the following default settings for existing users.



Disabling an Entire Domain

To disable an entire domain (all the users in a domain) at once:

1 Select **No** under **Allow user to change password remotely** to prevent users from changing their passwords from mail clients that allow such changes, or from a web browser.

2 Select **No** under **Allow POP3 access to mailbox**. (IMAP uses the same login ID and password.)

3 Select **No** under **Allow Web Access.**

Adding, Modifying, and Deleting Aliases

An alias is another name for an e-mail address, a number of addresses, or an application. Don’t create aliases that are identical to existing user IDs; mail addressed to an alias that’s identical to a user ID will go

to the user account represented by the alias, not to the account represented by the user ID. For more information on mail processing order, see “Processing Order” on page 81.

To comply with the Internet mail RFC specifications, you must have a *postmaster* alias so Internet mail users can send mail to *postmaster@your_domain_name*. The *postmaster* alias is set up automatically by the IMail Server installation as an alias for the *root* account. You can change the *postmaster* alias to point to a different mail account.

Types of Aliases

You can create four types of aliases:

- **Standard alias**. A standard alias is a name that indicates a single user ID on the same system, up to four user IDs on the same system, a remote mail address, up to four remote mail addresses, another alias, or any combination of these.
- **Group alias**. A group alias is a name that represents a group of up to 50 valid mail addresses.

  Note

  A standard alias will automatically be changed to a group alias if more than four users are added to it. A group alias was called a “list alias” in earlier versions of IMail Server.

- **Program alias**. A program alias points to a program that can accept the mail message for further processing. For example, a program alias could point to a word processor.
- **Beeper/Pager alias**. A beeper/pager alias sends a message to a beeper or pager.

Adding an Alias

You can create aliases one at a time in the IMail Administrator; you can also add a batch of aliases at once. See “Appendix C. Command Line Applications” on page 259.

If you intend to add a group alias, you can prepare the text file before you add the group alias. Enter all the mail addresses you want to include in the group into a text file; enter one address per line followed by a carriage return. Place the file in the host directory.

If you intend to create a program alias, copy the application to the IMail Server system. You can also use a *.bat* file to store the commands you want to use. (In this case, the program alias will point to the *.bat* file, making it easy to edit the *.bat* file at any time without having to change the program alias.)

To add an alias using IMail Administrator (assuming **Use Wizards** in the **Tools** menu is turned off):

1 In the left panel, select the host to which you want to add an alias.

2 Select the **"Aliases**" folder.

3 Click the **Add Alias** button. The New Alias dialog box appears.



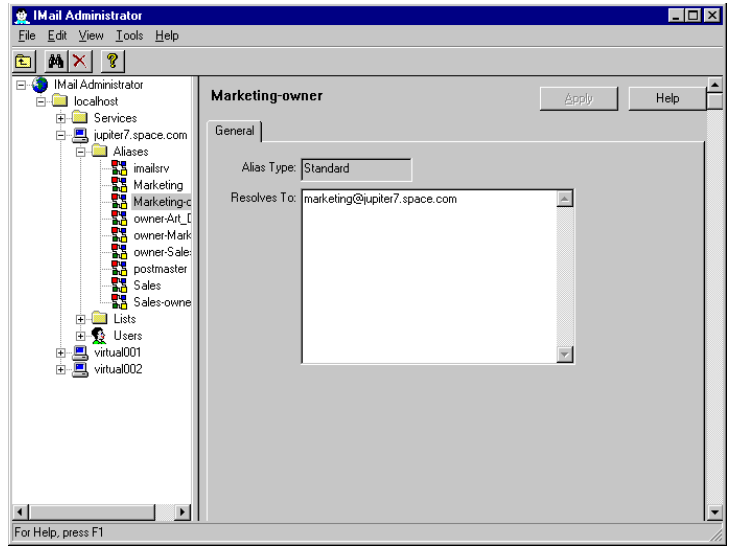
Enter a name for the alias. Alias names are limited to 45 characters and must be created from the character set of A-Z, a-z, 0-9, - (hyphen) and _ (underscore). The name cannot contain spaces and must be unique for this mail host.

If you're adding a standard alias, be sure to enter the complete e-mail address in the form *userid@hostname.com*.

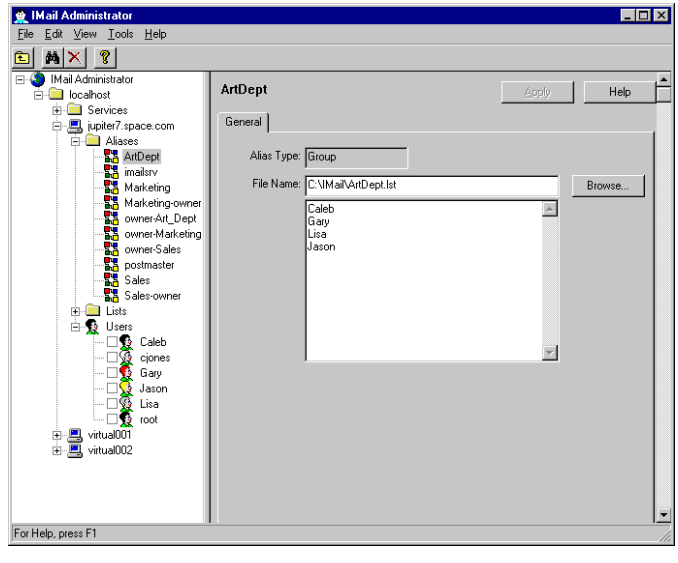
4 Select the type of alias to add. For more information, see "Types of Aliases" on page 76.

5 Click **OK**.

6 If you selected **Standard** alias, you see the following tab. Enter one complete mail address per line (in the form *userid@domain.com*). Note that if you enter more than four addresses, the alias will be converted to a group alias.



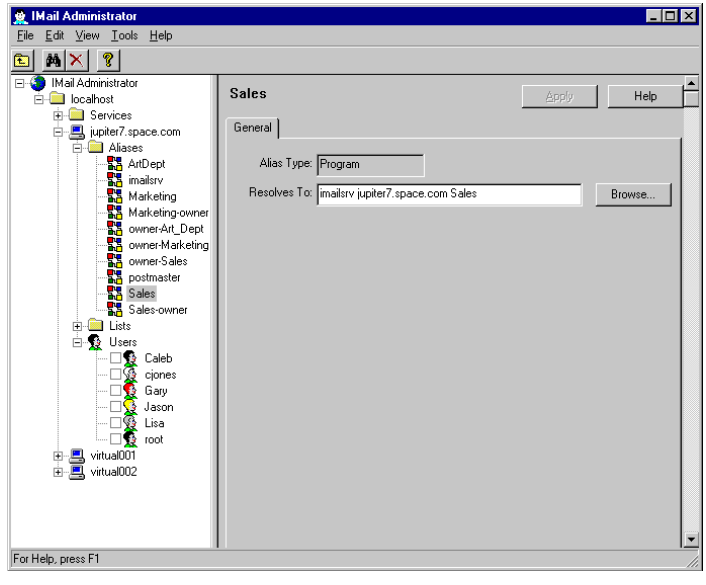
7 If you selected **Group** alias, the following panel appears.



Do one of the following:

- **File Name**. If the addresses for the group already exists in a text file (as described above), enter the file name.
- Enter the e-mail address of each person in the group, one address per line.

8 If you selected **Program** alias, enter the path and name of the executable program, as well as any required command line parameters. When an e-mail is sent to the program alias, the executable program is invoked and the entire contents of the message are passed to it. The program can then do anything it wishes with the file and must delete any *.tmp* files when done.



9 If you selected **Beeper/Pager** alias, see “Chapter 18: Sending Mail to a Pager or Beeper” on page 235.

10 After entering the alias properties, click **Next** and then **Finish**.

Processing Mail to Users That Don’t Exist

To process mail addressed to users that are not registered on the local host, you can create a special alias, *nobody.* If the *nobody* alias exists, all incorrectly-addressed mail is sent wherever you specify.

Note that the use of the “*nobody*” alias prevents messages from bouncing back to the sender.

Chapter 5: Mail Processing Techniques

IMail Server provides administrators with many options for handling incoming mail. By knowing the order in which IMail Server processes incoming mail, you can control the ways that mail is routed. You can further elaborate on mail routing using delivery rules. In addition, the Info Manager lets you set up automatic responses to handle routine inquiries. This chapter covers the following topics:

- Processing order
- Inbound delivery rules for incoming mail that can be applied to a host, a list-server mailing list, or an individual user
- Outbound delivery rules for outgoing mail which can be applied to a host
- The Info Manager for mailing automated responses to inquiries

Processing Order

Incoming mail addressed to a valid local address is processed in the following order.

1 **Alias**. IMail Server checks to see if the addressee matches an alias in the destination domain. An alias is considered to be one of the following: standard alias, group alias, program alias, pager alias, beeper alias, fax alias, or a list-server mailing list name.

   - If there is a match to a program, beeper, pager, or fax alias, IMail Server executes the program or activates the beeper, pager, or fax.
   - If there is a match to a standard or group alias, IMail Server resolves the alias to the appropriate user ID(s), and checks the user ID as described in Step 2.
   - If there is a match to a list-server mailing list, IMail Server processes the mail according to the settings for that list.
   - If there is no match to any alias, IMail Server checks the user ID as described in the next step.

2 **User ID**. IMail Server determines if the user ID is valid for the destination domain. If invalid, the mail is returned to the sender. If valid, IMail Anti-Virus checks for infected messages.

3 **IMail Anti-Virus.** If you have IMail Anti-Virus installed, it checks the message for infected files or code. If infected, the message is either repaired, bounced, redirected, or deleted, according to the settings on the Anti Virus tab. If the message is not infected, or is repaired, the delivery rules for a list-server mailing list are checked as described in the next step.

4 Delivery rules for a list-server mailing list.

If the message matches the rule criteria for the list, delivery follows according to that rule. If not, then the message is sent to the list server. If the message is not addressed to a list, Forwarding is checked.

5 **Forwarding**. IMail Server determines whether an address is present in the **Forward** box on the **General** tab for the account. If so, IMail Server forwards the mail. If not, the mail is delivered to the user ID according to the established delivery rules.

6 **Delivery rules for the mail host**. IMail Server determines if the message matches a rule for the mail host. If so, then delivery follows according to that rule. If not, then rules for the user ID are checked as described in the next step.

7 **Delivery rules for the user ID**. IMail Server determines if the message matches rule criteria for the user ID.

If the message matches rule criteria for a user ID, then delivery follows according to that rule. If not, then the Info Manager is checked as described in the next step.

8 **Info Manager**. IMail Server determines whether the user ID has the Info Manager enabled. If so, the automatic response is sent and the message is delivered to either the forwarding address or (if no forwarding address) to the sub-area or mailbox specified. If the Info Manager is not enabled for this user ID, the vacation setting is checked as described in the next step.

9 **Vacation**. IMail Server determines whether the user ID has a vacation message enabled. If so, the vacation message is sent. If not, the message is delivered to the User ID.

Setting Up Delivery Rules

You can use delivery rules to direct incoming and outgoing mail to particular mailboxes based on the contents of the **To**, **From**, **Sender**, **Subject**, **Header** or **Body** fields of the message. Delivery rules can be applied at three levels:

- Mail host (Inbound and Outbound rules)
- List-server mailing list (Inbound rules)
- Individual users (Inbound rules)

Inbound delivery rules can be used in conjunction with the Info Manager to screen for a particular phrase, and then (if the phrase is found) send an automatic response and forward the mail to someone for follow-up.

Examples

- **An inbound delivery rule for a host.** A school administrator can set up a delivery rule that scans all mail for offensive language and delivers such messages to a special user account that can be reviewed by a faculty member.
- **An outbound delivery rule for a host.** A school administrator can set up an outbound delivery rule that will scan for offensive language or content in mail messages that are being sent out through IMail Server by local users.
- **An inbound delivery rule for a list-server mailing list.** A system administrator can set up a delivery rule for a list-server mailing list to scan the body of all messages addressed to the list for language that indicates that the mail came from a spammer or bulk mailer, and ignore any such messages. For example, the rule can search for one of these text strings:
  - to be removed from any future mailings
  - please respond with the word “remove” in the subject line
  - advertise with bulk e-mail
  - bulk friendly

- **An inbound delivery rule for an individual user.** You could set up a rule for a sporting goods salesman to have all messages with baseball, softball, bat, base, homerun, or cap in the **Subject** be automatically placed in his mailbox named *baseball*.
- **An inbound delivery rule combined with the Info Manager.** You could set up a delivery rule to forward all mail containing the phrase “send info” to a particular mailbox named *Requests* in a user account named *Sales*. Then, you could set up the Info Manager to send out a generic response and also forward the mail to your company's Sales Manager. (For more information about the Info Manager, see “Using the Info Manager” on page 101.)

Rules Processing

IMail Server stores delivery rules in text files named *rules.ima* and *orules.ima*. Inbound rules are stored in the *rules.ima* file. Since inbound rules can be created by mail hosts, users and list-server mailing lists, there can be multiple *rules.ima* files on your IMail Server system. If an inbound delivery rule applies for a mail host, the *rules.ima* file is located in the mail host’s directory. If an inbound delivery rule applies for a user, the *rules.ima* file is located in the user’s directory. If an inbound delivery rule applies for a mailing list, the *rules.ima* file is located in the list’s directory. For information on the order in which rules files are processed, see “Processing Order” on page 81.

Outbound delivery rules are stored in the *orules.ima* file. Since only mail hosts can create outbound rules, the *orules.ima* file is located in the mail host’s directory. You may have multiple *orules.ima* files on your IMail Server system, one for each host.

IMail Server reads the *rules.ima* and the *orules.ima* files during the delivery process. The rule files for the virtual host are evaluated first, and then the rules for users and lists. Any *rules.ima* or *orules.ima* file can be copied to other directories. For example, if you create inbound delivery rules for one host, you can copy the *rules.ima* file to the directories of other hosts to apply the same rules to them.

Delivery rules created by the system administrator for an individual user affect only mail sent to the user’s *Main* mailbox. Users can use IMail Web Messaging to create their own delivery rules by selecting “Change Processing Rules” on the Menu page of Web Messaging.

However, rules created by a system administrator for a domain will take precedence over rules for a particular user, as described in “Processing Order” on page 81.

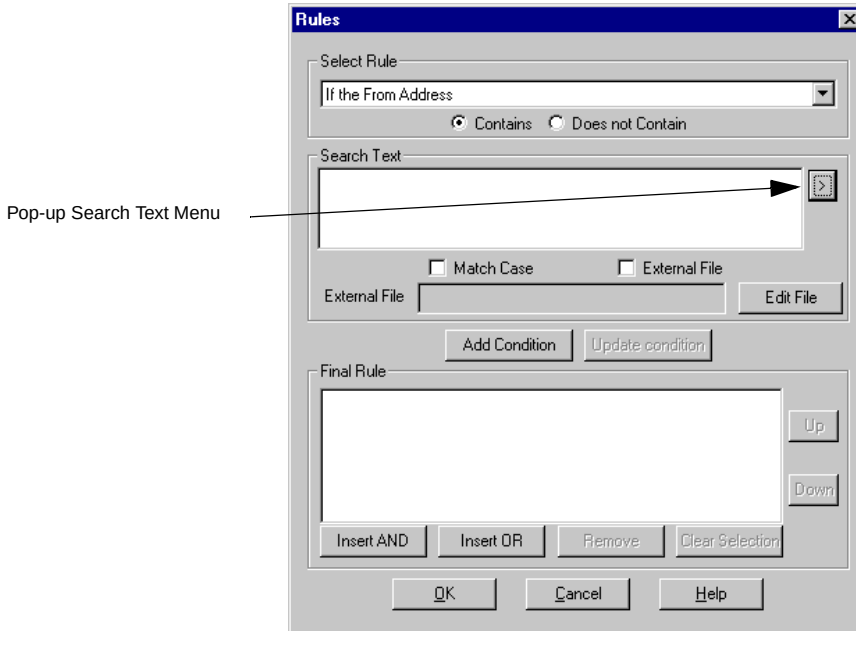
Creating an Inbound Delivery Rule

Inbound delivery rules, are used to sort incoming mail messages for mail hosts, users, and mailing lists. The following procedure describes the creation of an inbound delivery rule for a host. Note that this procedure is the same for mail hosts, users and lists.

1 In the left panel, do one of the following:

- To create a delivery rule for a mail host, select the host.
- To create a delivery rule for a user, expand a host and the “**Users**” folder, and then select a user.
- To create a delivery rule for a list-server mailing list, expand a host and the “**Lists”** folder, and then select a list.

2 In the right panel, click the **Inbound Rules** tab. Click the **Add** button. The **Rules** dialog box is displayed as shown below.



3 From the **Select Rule** list box, select the rule that you want to create (From, To, Subject, Sender, Body Text, Header Text).

4 Select **contains** to have the delivery rule look for messages that contain the search text. Select **does not contain** to look for messages that do not contain the search text

5 To enter search text, either enter the text in the **Search Text** box as described below, or specify an external file that contains the search text you want to use.

Enter the search text by doing one or more of the following:

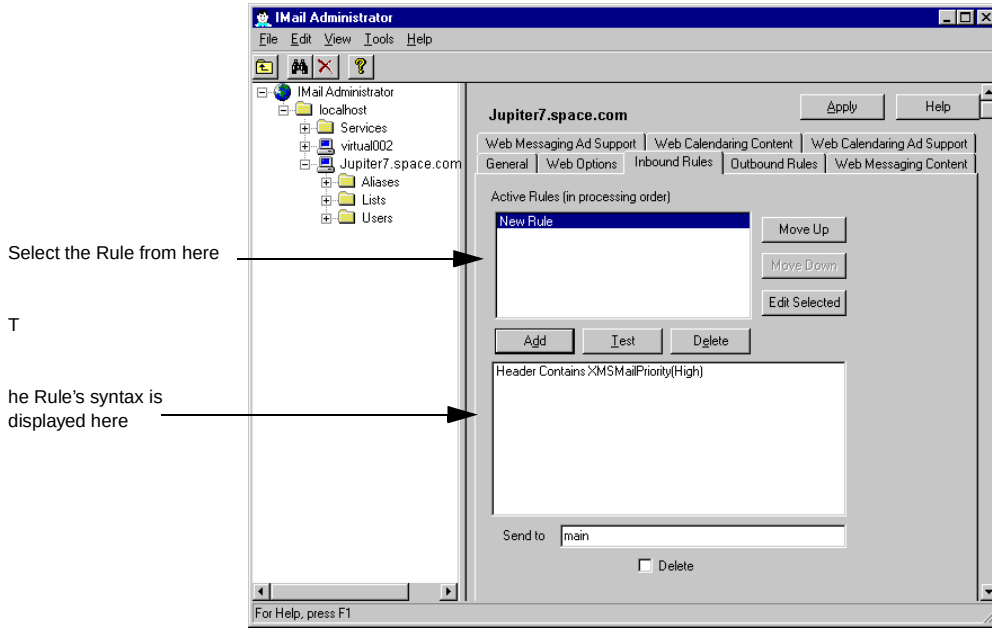
- Enter the literal text that you want to search for. For example, if you want to find the word jazz, type: *jazz.*
- Type search expressions and quantifiers as shown in Text Patterns on page 95.
- Use the popup menu to insert a generic form of a search expression and then edit the inserted expression.
- Paste a portion of a mail message that meets your search criteria. For example, you could copy and paste text such as "XMSMailPriority(High)" from the header of a message; this would search for High priority messages.

6 Select **External File**, if you have placed the search text in an external file. The list box displays the existing external files.

7 Select **Match Case** to search for text that matches the case of the search text. To ignore case, clear **Match Case**.

8 Click **Add Condition**. The condition that you just created is added to the rule and is displayed in the Final Rule textbox. If this is the only condition you want the rule to have, click **OK** and you will return to the Inbound Rules tab (shown below). If you want to add multiple conditions, read “Adding Multiple Conditions to Rules” on page 91.

The **Inbound Rules** tab now looks like this:



A placeholder is placed in the **Active Rules** list just under the selected slot (if any). The rule is temporarily named *New Rule.* The default mailbox is *Main.*

You cannot name delivery rules, because they are identified in the **Active Rules** list only by their sequence in the list. To identify a delivery rule, highlight one of the rules (e.g., *rule1*, *rule2*) and read its contents in the search text box.

9 From the Active Rules text box on the **Inbound Rules** tab, select the rule you just created and in the **Send to** box, enter either an address or a mailbox to which messages meeting the rule criteria will be sent. See below:

- **Enter an Address.** Enter the mail address to which messages meeting the rule criteria will be sent.
- **Enter a Mailbox.** Enter the name of the user's mailbox to which messages meeting the rule criteria will be sent. If you enter a mailbox that doesn't exist, one will be created for this user on the IMail Server system. A POP3 user will see this mailbox only if he logs on to this mailbox using the format userid-newbox.

- **Select Delete.** Select the **Delete** option to discard the message.

Note

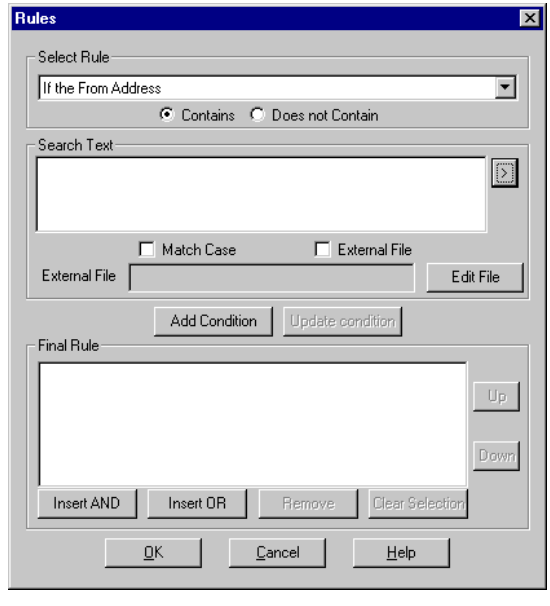
If the text in the **Send to** box contains an @, the text will be treated as an address, otherwise, the text will be treated as a mailbox. By default, if nothing is entered in the **Send to** box, messages meeting the rule criteria will be sent to the user's *Main* mailbox.

When the screen is refreshed, the delivery rule, previously identified as *New Rule*, will appear in the format *Rule#* to identify its sequence in the **Active Rules** list. Any existing delivery rules are renamed to reflect the new sequence.

Creating an Outbound Delivery Rule for a Host

Outbound delivery rules, are used to sort outgoing mail messages that are initiated by local users. Outbound delivery rules can only be created and applied at the Host level. The following procedure describes the creation of an outbound delivery rule.

1 In the left panel, select the host. In the right panel, select the **Outbound Rules** tab, and click **Add**. The **Rules** dialog box is displayed as shown below.



2 From the **Select Rule** list box, select the rule that you want to create (From, To, Subject, Sender, Body Text, Header Text).

3 Select **contains** to have the delivery rule look for messages that contain the search text. Select **does not contain** to look for messages that do not contain the search text.

4 To enter search text, either enter the text into the **Search Text** box as described below, or specify an external file that contains the search text you want to use.

Enter the search text by doing one or more of the following:

- Enter the literal text that you want to search for. For example, if you want to find the word jazz, type: *jazz*.
- Type search expressions and quantifiers as shown in Text Patterns on page 95.
- Use the popup menu to insert a generic form of a search expression and then edit the inserted expression.
- Paste a portion of a mail message that meets your search criteria.

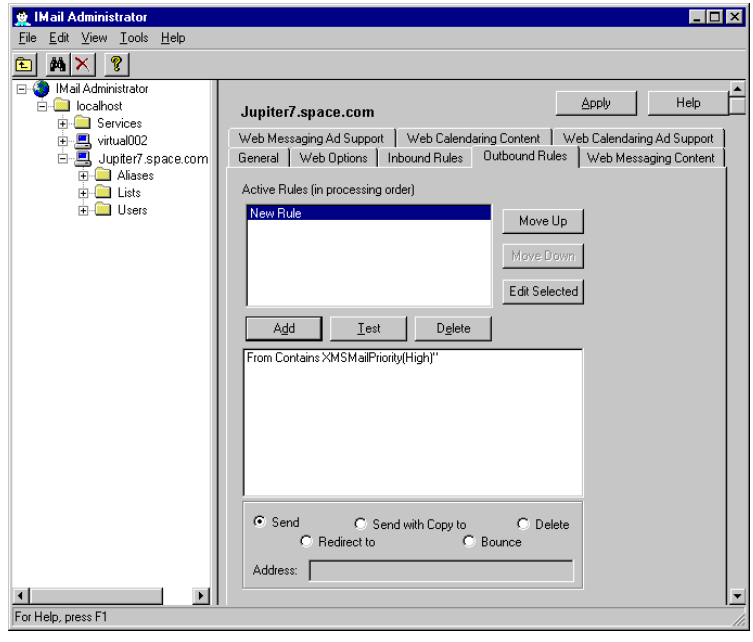
  For example, you could copy and paste text such as "XMSMailPriority(High)" from the header of a message; this would search for High priority messages.

5 Select **External File**, if you have placed the search text in an external file. The list box displays the existing external files.

6 Select **Match Case** to search for text that matches the case of the search text. To ignore case, clear **Match Case**.

7 Click **Add Condition**. The condition that you just created is added to the rule and is displayed in the Final Rule textbox. If this is the only condition you want the rule to have, click **OK** and you will return to the Inbound Rules tab (shown below). If you want to add multiple conditions, read “Adding Multiple Conditions to Rules” on page 91.

The **Outbound Rules** tab now looks like this:



A placeholder is placed in the **Active Rules** list just under the selected slot (if any). The rule is temporarily named *New Rule.*

You cannot name delivery rules, because they are identified in the **Active Rules** list only by their sequence in the list. To identify a delivery rule, highlight one of the rules (e.g., *rule1, rule2*) and read its contents in the search text box.

8 From the Active Rules text box on the **Outbound Rules** tab, select the rule you just created. In the lower section of the Outbound Rules tab, select the action you want to occur when a message is caught by the rule. You can choose only one of the following actions:

- **Send.** Processes the message as normal by sending it to the addressee.
- **Send with Copy to.** Processes the message as normal by sending it to the addressee, and also sends a copy to the address that you entered in the Addresses text box.
- **Delete.** Deletes the message.

- **Redirect to.** Does not send the message to the addressee. Instead, the message is sent to the address that is entered in the Address text box.
- **Bounce.** Bounces the message back to the sender, without delivering it.

Note

If you choose either **Send with Copy to** or **Redirect to**, you must also enter an address in the **Address** text box.

9 Click **Apply** to save your changes.

Adding Multiple Conditions to Rules

Sometimes, a rule with only one condition is adequate to fulfill your requirements. However, there are times when you may want to create more complex rules, in these cases, you may want to use multiple conditions. Multiple conditions can be created for both inbound and outbound rules. By using multiple conditions, you can combine multiple rules into one.

Example: If you want all e-mails from your supervisor containing text about “project updates” to be sent to a specific mailbox in your account, you would set a rule with two conditions: 1) the message must be from your supervisor; and 2) the message must contain the words “project updates” in the subject or message body of the e-mail.

To add a rule with multiple conditions:

1 Follow the steps for creating an inbound rule as described earlier in this chapter. Then, while on the rules dialog, create the first condition for the rule and click **Add Condition**.

2 Click either the **Insert AND** or the **Insert OR** button. Click the **Insert AND** button to state that all the rule conditions must be met in order for the message to be trapped. Click the **Insert OR** button to state that at least one of the conditions must be met in order for the message to be trapped.

3 Create the second condition as you did the first, then click **OK**.

4 Continue adding conditions until you are satisfied with the rule, and then click **OK**.

5 When you return to the Inbound or Outbound Rules tab, do one of the following:

- If you created an inbound rule and are on the Inbound rules tab, enter a mailbox or address that you want the rule to be sent to if it is trapped. For more information, see “Creating an Inbound Delivery Rule” on page 85.
- If you created an outbound rule and are on the Outbound Rules tab, select one of the rule actions listed on this tab. For more information, see “Creating an Outbound Delivery Rule for a Host” on page 88.

6 When you are finished, click **Apply** to save your changes.

Conditions are processed in the order that they appear from top to bottom as boolean expressions. To change the processing order of a condition, select it in the Rules dialog box, and click **Up** or **Down**.

Order of Rules

Delivery rules are processed from the top down until a match is found. Therefore, you should sequence the rules in the order in which you want them processed. To move a delivery rule up or down in the list, select it from the Active Rules text box on the Inbound or Outbound Rules tab, and click the **Move up** or **Move down** buttons. For information on processing order, see “Processing Order” on page 81.

Testing a Delivery Rule

To test a delivery rule,

1 On the **Inbound** or **Outbound Rules** tab, select a rule in the **Active Rules** text box, and click **Test**. Observe that the “Rule Tester” dialog box appears.

2 In the **Test Text** box, enter a message that meets your intended search criteria.

3 Click the **Test** button.

If the delivery rule does what you set it to do, **TRUE** is displayed in the **Test Result** box.

If the delivery rule does not test true, **FALSE** is displayed in the **Test Result** box. Edit the rule and test again.

4 Click **OK** to save the rule.

Note

You cannot edit the rule from the Rule Tester dialog box. To edit the rule, you must return to the **Inbound** or **Outbound Rules** tab, select the rule and click **Edit**.

Rule Syntax

When you create a delivery rule, the rule is entered into a file named either *rules.ima* or *orules.ima* in the following format:

Single condition rule:

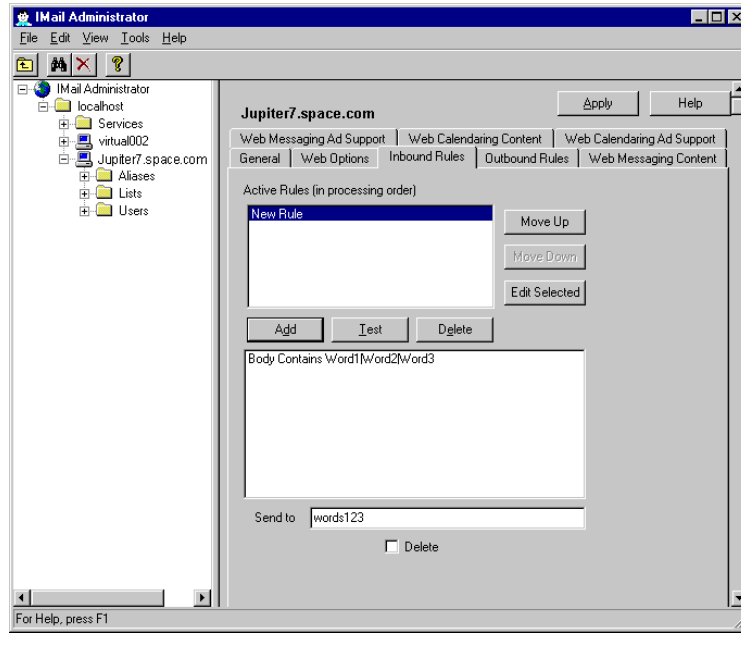
message_area condition search_text quantifier: mailbox_name

Multiple condition rule:

message_area condition search_text quantifier !AND!/ !OR!
message_area condition search_text quantifier: mailbox_name

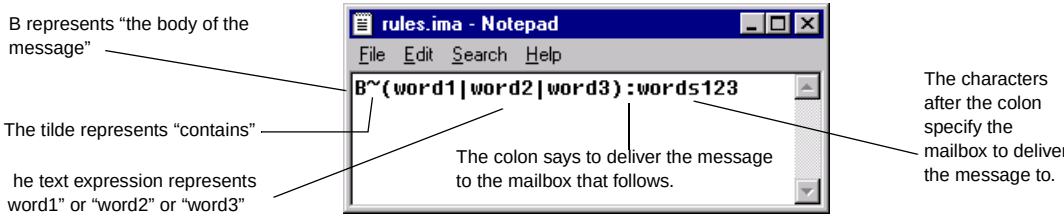
Note that *search_text* can be any combination of literal text and the text patterns on page 95.

For example, a rule with a single condition that looks like this in the **Inbound Rules** dialog box:

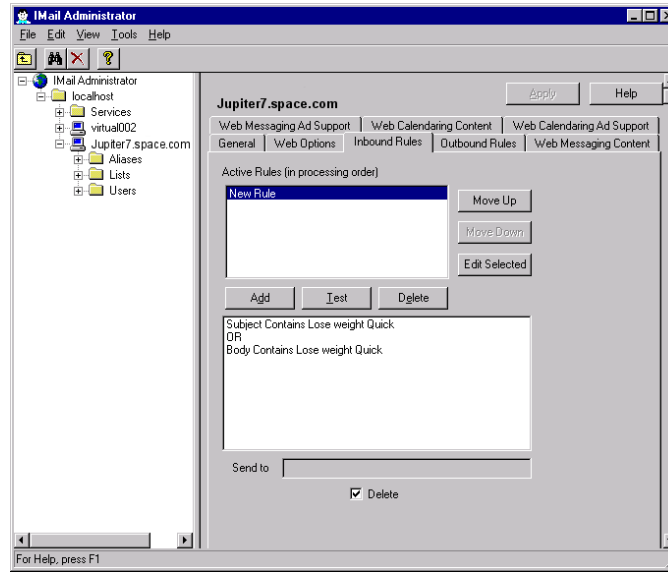


... will search the message body for the words *word1* or *word2* or *word3*; if at least one of the words is found, the message will be delivered to the *words123* mailbox.

The above rule looks like this in the *rules.ima* file:

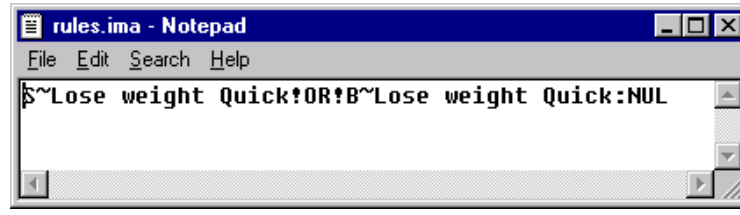


Example 2: A rule with multiple conditions that looks like this in the **Inbound Rules** dialog box:



... will search will search both the subject of the message and the message body for the words Lose Weight Quick. If those three words are found in either location, the message will be deleted.

The above rule looks like this in the *rules.ima* file:



The expressions for each element of a delivery rule are shown in the following tables.

Message Areas

Message Area	Representation
From:	F
Subject:	S
Sender:	N
To:	T
entire header (everything preceding the body)	H
entire body of message	B

Conditions

Condition	Expression
contains	~
does not contain	!~
equals	=
does not equal	!=

Text Patterns

Text Pattern	Expression
Any character	.
Any of the values separated by vertical bars within the parentheses; the vertical bar represents “or”	(this|that|other)
Any word character (a-z, A-Z, 0-9)	\w
Any non-word character	\W
Any digit (0-9)	\d
Any non-digit	\D
Any white space (spaces and/or tabs and/or carriage returns)	\s
Any non-white space	\S

Text Pattern	Expression
Any punctuation character (any character other than \w or \s)	\p
Any non-punctuation character	\P

Quantifiers

Quantifier	Expression
Zero or more	*
One or more	+
Exactly 100	{100}
At least n1, but not more than n2 (where n1 and n2 are numbers)	{n1,n2}

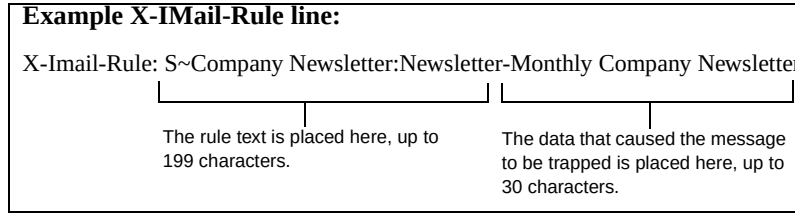
Note

As shown above, the following characters have special meaning in a rule: `{}()|*+,.:\` If you want to use one of these characters in a search string, precede it with a backslash. For example, to search for a plus sign, enter \+ in the search string.

Determining Which Rule Trapped a Message

When a message is trapped by a rule, an X-IMail-Rule line is placed in the message header, to identify which rule caught the message. If multiple rules trap a message, only the last rule will be placed in the X line in the header. The X-IMail-Rule line will also contain up to 30 characters of the message data that caused the message to be trapped. Message data will no be included in the X-IMail-Rule line when a message is trapped by a negative rule (does not contain or does not equal). The maximum length of any X-IMail-Rule line is 250 characters.

If a domain rule traps the message, the X-IMail-Rule line will be added to all local deliveries. If a message is trapped by a user's rule, the X-IMail-Rule line will only be added to deliveries to the user. When a message that is destined for local delivery is trapped by an outbound rule, a line with the rule causing the trap will be written to the Queue file. When this message is delivered, and that line exists in the Queue file, it will be written as an X-IMail-Rule line in the message header. Outbound messages that are not delivered locally, will not have an X-IMail-Rule line in the header.



Note

Because IMail Server inserts the rule and 30 characters of the message in the header, special care should be taken if a trapped message is then forwarded to another recipient. Some e-mail clients will include the header in the forwarded message. If this occurs and you have a rule set up to search the body of the message for the specified text, then the message will be trapped again.

Commonly Used Rule Examples

The following examples explain how to manually write rules in the *rules.ima* and *orules.ima* files.

Example 1: Forwarding Using Rules

A school administrator wants to filter for offensive language and deliver such messages to a specific user account to be reviewed by a faculty member. The administrator should create the following rules:

B~*filtered content in body*:spambox

S~*filtered content in subject*:spambox

H~*filtered content in header*:spambox

F~*filtered content in From address*:spambox

T~*filtered content in To address*:spambox

N‘*filtered content in Sender*:spambox

For example, if you want to catch all mail with the subject “kill dusty” then you would have a rule like this: S`Kill Dusty:spambox.

This would also catch messages with the subject “I want to kill Dusty”, but it would not catch “I am going to kill that guy Dusty”.

The messages are sent to a mailbox called *spambox*. Unfortunately, this would create a file named *spambox.mbx* in the users folder which is accessible by the user.

To prevent the user from having access to the *spambox* mailbox, do the following. Put a forward file in each user's folder. This file must match the name of the mailbox that you used in your rule i.e. *spambox.fwd*. The only thing that should be in the *spambox.fwd* file is the account to which you want the filtered messages to go. If you have an account called filtered@ipswitch.com, the *spambox.fwd* file would look like this: *abuse*.

When the filtered message is in the abuse-spambox, you can log in to the abuse box and see whether the message contained offensive language, or whether it was caught accidentally. If it was caught accidentally, it can be forwarded on to the original recipient.

Note

Do not put the *.fwd* file in the account to which you are sending mail. If you use Windows Notepad to create the *.fwd* file, remember that Windows Notepad adds *.txt* to the filename of any new file created.

Example 2: Deleting messages which contain specific text

If you want to filter for the words "Get Rich Quick" in the subject of a message and delete it without sending it to a mailbox, you would create a rule that looks like this:

S~Get Rich Quick:NULL

H~Get Rich Quick:NULL

Example 3: Filtering messages that have attachments

The rules file would look like this:

B~(name=".vbs"\c|name=".*\shs"\s|name=".*\scr"\s):spambox

B~(begin 6.*\.vbs\s|begin 6.*\.shs\|begin 6.*\.scr\s):spambox

The first rule filters MIME attachments, characterized by the string: name="filename.ext" while the second rule filters unencoded attachments, characterized by the string Begin 6.

These rules include the \s text pattern to search for "any white space" (spaces, tabs or carriage returns) after an attachment extension. Without this pattern, the number of false positives will rise.

Note

This will filter all incoming messages containing attached files with .vbs, .shs and .scr exensions. Filtered messages will be directed to a sub-mailbox, (spambox.mbx) in the user's folder for the user to whom the message was addressed. If the sub-mailbox does not exist, its creation will be determined based on the sub-mailbox settings that are enabled in IMail Administrator on the host's **General** tab.

Example 4: Filtering messages with no subject

You need your rule to say: If the subject does not contain any character, send to the mailbox called test.

In the rules.ima file:

H!~\sSubject:\s*\w*\s:test

This rule will catch messages that have no subject in the header, and messages that have no word characters in the subject.

Note

\s matches any white space character.

Storing Search Text in External Files

If you need to frequently update and disseminate the search text for delivery rules, you can use external text files to store the search text. Then, all you have to do is distribute the text file. The external text file must have a file extension of *.rul*.

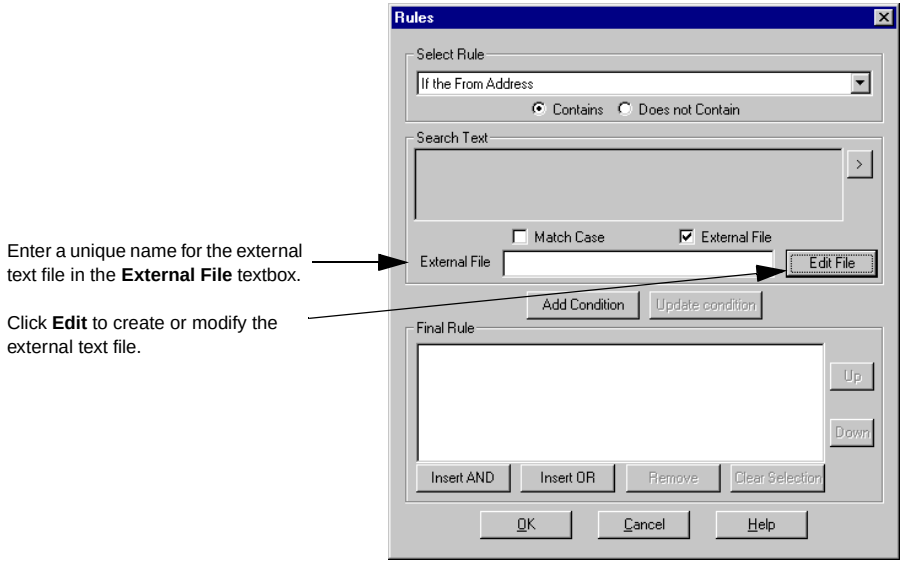
For example, an administrator can use this method to catch mail from known spammers. The administrator might create a text file named *spam.rul*. Each time a new spammer address is discovered, the administrator can add it to the *spam.rul* file. The *rules.ima* or *orules.ima* file can reference the text file named *spam.rul*. The procedure for storing search text in an external file is the same for inbound and outbound rules.

Example: To send spam messages to a mailbox named *spambox*, the *rules.ima* file would contain the line: *h~:spam:spambox*

Note that the *.rul* file name is preceded by a colon. IMail Server reads the *rules.ima* file and looks for the referenced *spam.rul* file at the same location as the *rules.ima* file.

To create a delivery rule that references an external text file:

1 Select the mail host, user, or list that you want to create a rule for. Then click either the **Inbound** or **Outbound Rules** tab (depending on which type of rule you are creating), and click **Add**.



2 In the **Rules** dialog box, select the **External File** option and do one of the following:

- If the external text file already exists, select the file. For example, select `:rulefilename` where *rulefilename* is the name of the *.rul* file you want to reference.
- If the external text file does not exist, enter a new, unique name for the *.rul* file. Do not enter the file extension *rul* as IMail Server will append it to whatever you enter.

3 Click **Edit File** to open and edit the *.rul* file in Windows Notepad (or your default text editor). If the rule file does not exists, it will be automatically created. See the "Rule Syntax" topic in the previous section to create the search text.

4 From **Select Rule**, select the area that you want to search (From, To, Subject, Sender, Body text, or Header text).

5 Select **contains** to have the delivery rule look for messages that contain the search string; select **doesn't contain** to look for messages that do not contain the search string.

6 Select **Match Case** to search for text that matches the case of the search string; to ignore case, clear **Match Case**.

7 Click **OK**. You are returned to the **Inbound** or **Outbound Rules** tab. Select a message action as described in "Creating an Inbound Delivery Rule" on page 85 and "Creating an Outbound Delivery Rule for a Host" on page 88.

8 Click **Apply** to save the rule.

Limitations

Each delivery rule is limited to 5000 characters.

Delivery rules search the first 32,000 bytes of a message. If a message contains fewer than 32,000 text characters plus attachments, the rule will scan the attachment as though it is text. Rarely, when the message text is only a few characters, a delivery rule could find something in an attachment that looks like a match, but isn't.

Using the Info Manager

The Info Manager provides a way to automatically handle routine e-mail inquiries for basic information about your company. For example, you may want to respond to general inquiries with an acknowledgment that the inquiry was received and a promise to follow up.

Using the Info Manager for a Single Automated Response

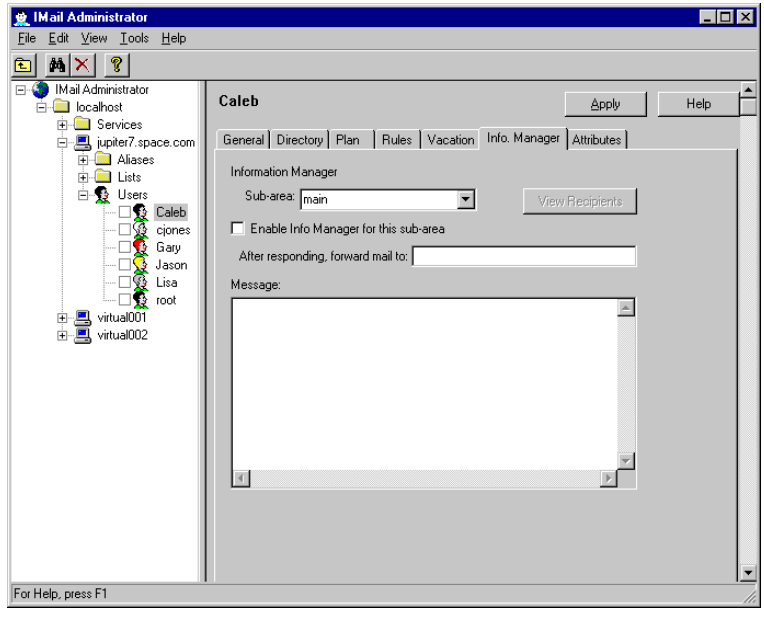
To use the Info Manager, you might set up a special user account whose user ID is *Info*. This mail account does not belong to a particular user, but accepts mail addressed to *Info@yourcompany.com*. When someone sends mail to the *Info* account, they receive a prepared response such as:

> This is an automated response from General Sales. You will be receiving a personal response by e-mail from one of our staff.

To create an automated response for a mail account:

1 If you do not already have a user account set up to be an Info Manager account, create an Info Manager account as follows:

- Expand a host name and select the "**Users**" folder.
- Click **Add User** and enter a name for the special account.
- Click **OK**. The account has a default password of *password*.
- Select the user account you set up to be an Info Manager account, and click the **Info Manager** tab.



2 If you need only one automated response for all inquiries, enter *main* (the *Main* mailbox) as the **Sub-area**. Note that if you enter *Main* as the sub-area, all messages sent to the Info Manager account are saved in the main mailbox (*main.mbx*).

(If you want to have multiple automated responses, see "When to Use a Sub-divided Info Manager Account" below.)

3 Turn on **Enable info manager for this sub-area**.

4 To forward the message after the automatic response is sent, enter a forwarding address in the box labeled **After responding, forward mail to**. If you are absolutely sure you want to discard the message, you can enter NUL in this box. See the note below.

Note

IMail Server must deliver incoming messages somewhere (even if it is NUL) after sending the automatic response. If you don't enter a forwarding address, IMail Server will deliver the message to the **Sub-area** specified in Step 3. If the sub-area is not a mailbox, IMail Server will convert it to a mailbox to deliver the message.

5 In the **Message** box, enter the response to send to mail addressed to this account.

The first line becomes the subject line for the automated response. It must be less than 80 characters long.

6 Click **Apply** to save the message and enable the Info Manager.

When to Use a Sub-divided Info Manager Account

You can sub-divide an Info Manager account into more specific sub-areas that can send more detailed information in response to inquiries. For example, you can have three automated responses as follows:

- one response that lists products, prices, and ordering information
- one response that describes the classes you offer to the public
- one automated response that sends out company news

To divide the Info Manager account into more specialized responses, you create sub-areas of the *Info* account (such as *Sales*, *Classes*, or *News*) from which the sender can obtain more specific information. Then, when someone sends mail to the *Info@ipswitch.com*, IMail Server returns a prepared response that describes the *Info* account sub-areas such as:

> Thank you for contacting Ipswitch. For information about our products, please send e-mail to *Info-sales@ipswitch.com*. For information about our classes, send mail to *Info-classes@ipswitch.com*. For the latest Ipswitch news, send e-mail to *Info-news@ipswitch.com*.

The sender can then send a message to

Info-sales @ your _ company .com and receive back the automated message about products and prices. A sender can also send a message to *Info-classes@your_company.com* and receive back the automated response describing the classes you offer.

Sub-areas and Mailboxes

There is no limit to the number of sub-areas you can use with the Info Manager. Sub-areas take up no disk space as long as a forwarding address is specified. However, IMail Server will convert a sub-area to a mailbox if the forwarding address is left blank. This is because IMail Server must deliver each incoming message somewhere (even if it is to NUL) after sending the automatic response.

Sub-dividing an Info Manager Account

To use a sub-divided Info Manager mail account:

1 If you do not already have a special account for the Info Manager to use, do the following:

- Expand a host name and its "**Users**" folder.
- Click **Add User** and enter a name for the special account.
- Click **OK**. The account is created with a default password of *password*.

2 Make sure the new account is selected in the left panel, then click the **Info Manager** tab. You see the tab shown on page 102.

3 Create a new sub-area or select an existing sub-area to which the response message will apply.

4 Turn on **Enable info manager for this sub-area**.

5 To forward the message after the automatic response is sent, enter a forwarding address in the box labeled **After responding, forward mail to**. If you are absolutely sure you want to discard the message, you can enter NUL in this box. See the note below.

Note

IMail Server *must* deliver the incoming message somewhere (even if it is NUL) after sending the automatic response. If you do not enter a forwarding address, IMail Server will deliver the message to the **Sub-area** you specified in Step 3. If the specified sub-area is not a mailbox, IMail Server will convert it to a mailbox to deliver the message.

---

6 Enter the message to be returned to all senders who send mail to this account and sub-area.

The first line becomes the subject line for the automated response. It must be less than 80 characters long.

7 Click **Apply** to save the message and enable the Info Manager.

Notes about Forwarding

- To forward a copy to a different user ID on the *same* host, you can enter the simple user ID (for example, just *userid* instead of *userid@domain.com)*.
- To forward a copy to a user on a *different mail syste*m, you must enter a complete mail address in the form of: *userid@domain.com*.
- To forward a copy to a particular mailbox of an account on the same host, you can append a mailbox name to the user ID by using a hyphen. For example,

  `dave-music@domain.com`

Disabling the Info Manager

To disable the automated response, but keep the text to be enabled another time, turn off **Enable info manager for this sub-area**.

More About the Info Manager

The automatic response message is saved in a file with an extension of *.inf* in the folder of the special account. If you want to set up the same Info Manager information for multiple accounts, you can copy the *.inf* file from one account's directory to the directories of other accounts.

When a person sends mail to an Info Manager account, the sender's mail address is listed in a file with the extension *.snt* in the account's directory. To view this file, click the **View Recipients** button.

To prevent automatic responses to bulk mailers, Info Manager messages are not returned to the sender if the original message contains the *Precedence: bulk* header. To prevent automatic responses to list-server mailing lists, Info Manager responses are not returned to the sender if the original message contains *imailsrv* in the address.

Note

Do not send mail from an account for which the Info Manager is enabled because the recipient of the message will receive an automated response if they reply.

You can use the Info Manager and delivery rules together. For example, you can use delivery rules to search incoming messages for a particular text string and route such mail to an Info Manager account for which you have set up an automated response. For an example of using the Info Manager and delivery rules together, see “Examples” on page 83.

IMail Server processes the Info Manager after delivery rules, and before vacation processing. For more information on processing sequence, see “Processing Order” on page 81.

Chapter 6: IMail Web Messaging

This chapter describes how to configure and use the Web Messaging server, and how to customize the Web Messaging interface.

Note

Before users can use the Web Messaging e-mail functions, you must start the Web Messaging server, and enable web access for users as described in this chapter.

What is Web Messaging?

Web Messaging lets your e-mail users to send and receive mail using a web browser. Users can log on to Web Messaging from any browser on any machine and perform all of their mail functions — without having to install e-mail client software or a browser plug-in on their local PC or workstation.

Web Messaging works like an IMAP4 mail client – all users' mail is stored on the mail server. When a user creates a mailbox in Web Messaging, it is created on the mail server.

In addition to the messaging capabilities, Web Messaging offers the following:

128 bit Secure Sockets Layer. Web Messaging uses 128 bit SSL when making connections to the IMail Server, thus giving you confidence that your transmissions will remain secure. For more information on Web Messaging security, see **"Web Messaging Security" on page 111**.

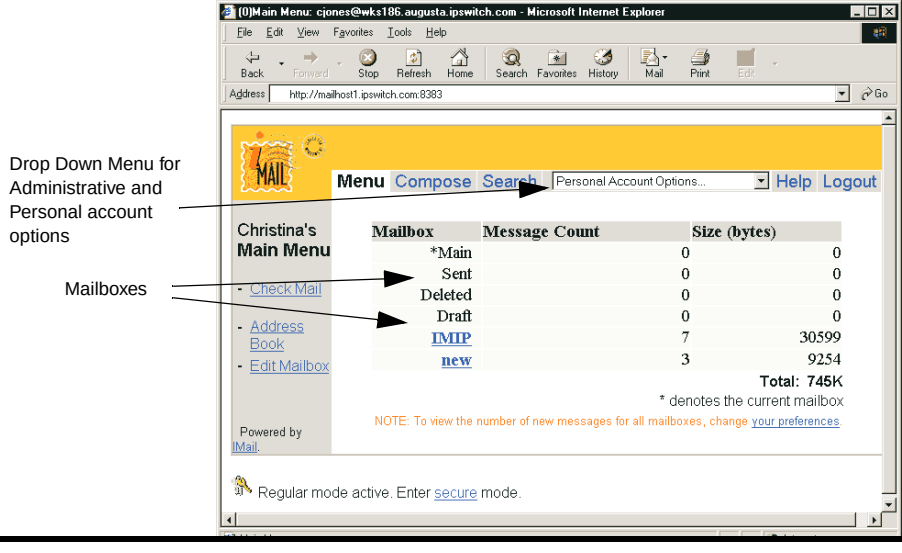
Remote administration for IMail Server. Web Messaging offers an extended menu from which administrators can remotely monitor and manage the mail server, user accounts, aliases, mailing lists, and delivery rules. The menu choices for administration tasks only appear if the user has the required permissions. For information on the administration functions, see "Using Remote Administration Functions" on page 123.

Spell Checking Feature. Web Messaging has a spell checker, that enables users to check for misspelled words before sending mail. The

spell check comes equipped with two different dictionaries to choose from, as well as a user dictionary that is editable to meet the user's spelling needs.

Customizable interface. You can create your own look and feel for the Web Messaging interface by editing the HTML templates and other files used to generate the Web Messaging pages. If you have multiple mail hosts, each mail host can have a different Web Messaging interface. For information on customizing the interface, see "Appendix G. Changing the Look and Feel of Web Messaging" on page 285.

Online ads. Web Messaging also supports the display of advertisements on all Web Messaging pages. This feature is very useful to Internet Service Providers (ISPs) and other mail service providers who would like to sell online advertising space on their mail server. This feature can also be used to display announcements on an intranet. For more information about online ads, see "Displaying Online Advertisements" on page 129.



What Can Users Do with Web Messaging?

Web Messaging provides users with full e-mail functions and the ability to change personal information from a web browser on any system connected to the Internet.

Users can connect to the Web Messaging server and log on to their mail account using their IMail Server user ID and password.

Users can start Web Messaging by entering the web server's address in their browser's address field. This web address consists of the host name of the IMail Server host and a web server port number. The default port number is `8383`. For example, if your IMail Server host is named mailhost1.ipswitch.com, then the Web address will be: `http://imail.ipswitch.com:8383`

For information about setting the port number, see "Web Address for the Web Messaging Server" on page 112.

Users can bookmark the address (save it as a Favorite site) in their web browser.

Once logged on, users can read, send, delete, and reply to e-mail, send and receive attached documents, and print e-mail directly from the browser.

Users can also set mail forwarding, enter a vacation message, organize their mail into folders (mailboxes), maintain an address book, maintain LDAP and finger information, and set delivery rules for incoming mail.

You can give users the ability to change their password. Users can also set preferences to change how the mail summary appears and how mail functions work.

Users now have the ability to follow a link directly to IMail Web Calendaring without logging out of Web Messaging.

Online help is available from the Web Messaging pages.

Notes for the System Administrator:

- Users should be aware that the Web Messaging server connection may time out when the server receives no requests from the user's browser for 12 minutes. After 12 minutes, the session is placed in a rollover queue that holds up to 50 users.
- Because the rollover queue is used, users must click on **Log off** to be sure they have logged off of the Web Messaging session. The Log off function removes the user from the rollover queue and the standard connect tables.

If the server times out while a user is creating a message, the user won't know it until clicking the **Send** button, in which case they are returned to the logon screen and the message is lost. When composing a long message, we recommend that you save frequently. Click the **Save** button on the **Compose** page to save the message in the **Draft** mailbox. You can then re-open the message from the **Draft** mailbox, and continue editing.

- Web Messaging is not a POP3 mail client and will not display mailboxes that a user has created on their POP3 client. Mailboxes created with an IMAP4 client or Web Messaging will appear, as both of these methods create mailboxes on the server.

System Requirements

The Web Messaging server is installed on the host where the IMail Server software is installed.

To access their e-mail via the web, users need a frames-capable browser. Older versions of browsers may not support frames. Web Messaging is designed to support Microsoft Internet Explorer version 4.0 or later, Netscape Navigator version 4.0 or later, and other HTML 4.0 compliant browsers.

Upgrading

If you have an existing version of Web Messaging installed, during the IMail Server installation, you can select one of the following options:

- Install the files for the new version in the directory [*IMail Top Directory*] *\Web*, thus overwriting your old Web Messaging files. If you are using online advertisements, you do not want to overwrite the *ads.txt* file.
- Install the files for the new version in the directory [*IMail Top Directory*]*\Web\new*, so your existing files in [*IMail Top Directory*]*\Web* do not get overwritten.
- Do not install the new version files.

IMail Server uses the files in [*IMail Top Directory*]*\Web* to generate the Web Messaging interface.

If you want to save some existing files (such as an *ads.txt* file for online advertisements, *MailNews.txt* for the News of the Day message

,butontxt.ini or *message.ini*) copy them to a temporary directory, move the new version files from *\new* into *\Web*, and then replace the new versions of selected files with your old version.

If you have customized templates you wish to continue using, refer to the "Upgrading Customized Templates Document" (upgrade6to7.txt) for the proper procedures to upgrade the old templates for use with IMail Server v7.0. This file is located in [IMail Top Directory]\Web\UpgradeHelp.

Web Messaging Security

Web Messaging offers several means of protecting your e-mail communications from being altered in transit or being read by someone other than the intended recipient.

Secure Mode. Enables Secure Sockets Layer connection and encryption. The SSL capabilities offer the most secure method of safeguarding e-mail messages. SSL will increase processing time on your server.

Logon User ID and password. Users must log on with their user ID and password. This provides the basic level of security that protects the user's mail.

Logoff. After reading mail in the browser and then logging off, a user cannot click the browser's **Back** button to return to a mail message. However, clicking in the History list may re-display the message, though the user cannot activate any of the mail functions. As a precaution, users can clear the browser's history if the browser is in a common use area.

When logging on to Web Messaging, users can choose either or both of the following options (on the Logon page):

expire page views. If you are logging on to mail from a public terminal or from someone else's computer, you can select this option to prevent the browser from saving (caching) the pages you view. Note that Microsoft's Internet Explorer can be set to ignore this "expire page views" command, so it is still possible your pages will be saved.

Remember Userid and Password (not recommended if you share this computer). This option will save your User ID and password in a file, so you do not have to enter them each time you log on to Web

Messaging. When you log on, the browser automatically enters your User ID and Password. Note that if you select this option, anyone who has access to the machine could connect to your e-mail through Web Messaging without having to enter your User ID and password. Do not use it on a public terminal.

Setting Up Web Messaging

To set up Web Messaging, you need to:

- Determine the web address for your Web Messaging server.
- Optionally, set up the SSL capability to provide secure communications between the server and users' browsers.
- Configure the Web Messaging server.
- Set user access to Web Messaging.

Web Address for the Web Messaging Server

By default, the Web Messaging server is assigned a web address that consists of the host name of the IMail Server host and a web server port number. The default port number is `8383`. If your mail host had a name of mailhost1.ipswitch.com, then the address will be: `http://imail.ipswitch.com:8383`

Your mail users can start Web Messaging by entering the address in their browser's address field.

If you are not running another web server on the same host, you can set the port number to the normal HTTP (web) server port of `80`. In this case, users do not have to specify the port with the web address. For example, you could enter: `http://imail.ipswitch.com`

Note that some firewalls may block the 8383 port, in which case you need to change the port number. To change the port number, see "Configuring the Web Server" on page 117.

If You Have Multiple Mail Hosts

If you have set up multiple mail hosts on your IMail Server system, the web address is determined by whether the mail host has it's own IP address or uses a virtual IP address. (For information on virtual hosts, see "Chapter 3: Configuration" on page 33.)

If each host has its own IP address, you will have a different web

address for each host. For example, if you have set up the following hosts:

```
mail.marcel.com          156.21.50.78
mail.magnolia.net        156.21.50.80
```

the web address for the respective hosts would be:

```
mail.marcel.com:8383
mail.magnolia.net:8383
```

If a mail host does not have an IP address, then it will have the same web address as the primary mail host. For example, if you have set up the following hosts:

```
mail.marcel.com          156.21.50.78
mail.magnolia.net        <$virtual IP>
```

the web address for both hosts would be:

```
mail.marcel.com:8383
```

The host *mail.magnolia.net* can still have its own set of users, but users on this host must identify the host when they enter their logon user ID. For example, the user *fred* on *mail.magnolia.net* would enter the web address *mail.marcel.com:8383* to open the Logon page, then would enter *fred@mail.magnolia.net* as his user ID.

Using Secure Sockets Layer (SSL)

You can set up the Web Messaging server to use Secure Sockets Layer (SSL) for communications between a browser and the server. SSL encrypts your mail communications so they can be read only by the intended recipients.

SSL is a protocol that uses “certificates” to authenticate the client and server, and uses a public/private key “pair” to encrypt and decrypt communications. All of the major browsers are SSL enabled.

Certificates. Certificates are used to establish the identity of the client (browser) and the server.

You can run SSL for Web Messaging with:

- A self-signed SSL certificate. The server identifies itself to the client, but its certificate has not been issued by one of the third-party Certificate Authorities. Clients who log on to IMail Server using Netscape and Internet Explorer will receive a warning message (“This site is not secured...”). These users can continue

logging on after acknowledging the warning.

- An SSL certificate issued by a Certificate Authority. The certificate verifies to the client that the identity claimed on the certificate is accurate. You can purchase a third-party certificate from Thawte Consulting (www.thawte.com) or Verisign (www.verisign.com).

IMail Server comes with an SSL Utility that generates both an IMail Server self-signed SSL certificate as well as a certificate request you can send to a Certificate Authority.

Public/private key encryption. When a browser connects to the Web Messaging server, the server sends its certificate and public key to the browser. The browser can now use the public key to encrypt communications. Only the web server has the private key, which is used to decrypt communications sent from the browser.

Ciphers. The server and client must agree on the algorithm, called a "cipher," used to encrypt data. You select the cipher when setting up SSL on the server.

For more information on how SSL works, visit:

home.netscape.com/security/techbriefs/ssl.html

Setting Up SSL on the Server

This section outlines the procedure for setting up SSL on the server.

- First, you use the IMail SSL Configuration Utility to set up the SSL certificate and public/private key pair.
- Then, you enable SSL in the IMail Administrator, on the **Web Messaging** Advanced tab.

For detailed information about the SSL options, see the online help in the IMail SSL Configuration Utility and help for the **Web Messaging Server** tab in IMail Administrator.

To enable SSL for the Web Messaging Server, you need to do the following:

1 Set the registry path for the SSL keys.

From the **Start** menu**, select Programs -> IMail -> IMail SSL Configuration Utility**. Select **Registry Path** from the **File** menu. Enter the path: `software\ipswitch\imail\ssl`

2 Generate a certificate and public key. We recommend that you use the self-signed certificate for your server.

   In the **IMail SSL Configuration Utility**, click **Certificate**. For more information, select **Help Topics** from the **Help** menu, then go to the “Getting an SSL Certificate” topic.

3 Configure SSL and select the cipher to use for encryption.

   In the SSL Configuration Utility, click **SSL Configuration**, and then complete the wizard. For information, select **Help Topics** from the **Help** menu, then go to the “Configuring SSL” topic.

4 If you want the server to authenticate clients, configure how it will do it.

   In the SSL Configuration Utility, click **Client Authentication**. For more information, select **Help Topics** from the **Help** menu, then go to the “Dealing with Clients” topic.

   We recommend that you allow any client to connect to your server, thus you would not turn on the **Client Authentication** option.

5 Activate SSL for the Web Messaging server. In the IMail Administrator, select the “**Services**” folder, then select **Web Messaging** and click on the **Advanced** tab to show the SSL options. Turn on **Enable SSL**. See “Configuring the Web Server” on page 117 for information about the SSL options.

Starting an SSL Connection from a Browser

Users can open Web Messaging with an SSL connection as follows:

1 In the browser, enter the address for the Web Messaging server, for example: `mail.domain1.com:8383`. The IMail Web Messaging logon appears.

2 On the Logon page (or on any other Web Messaging page), select **Enter Secure Mode**.

3 The browser usually asks you to confirm that you want to use “secure mode.” Click **OK**. If you used the self-signed certificate, the browser may also display a warning that the certificate is not “trusted.” Click **OK** again to continue.

The browser is now in secure mode. You can click again at the bottom of any Web Messaging page to return to regular mode.

Enabling SSL from within the Web Address

When you enter the web server's address in a browser and use HTTPS (in place of HTTP) in the address, the browser attempts to connect to the server using SSL. For example, the address would look like:

```
https://mail.domain1.com:8383
```

Using a Different Port for SSL

The standard port for SSL is 443. If you use a different port number, this port number must be specified in the web address that Web Messaging users log on to. For example, if you use port 8384 for SSL, and the web server is on port 8383 of mail1.domain.com, the web address would be:

```
mail1.domain.com:8384
```

Users can bookmark the web address (save it as a Favorite), so they do not have to enter it each time they log on.

Troubleshooting SSL

You can check the following if you are having trouble getting SSL to work:

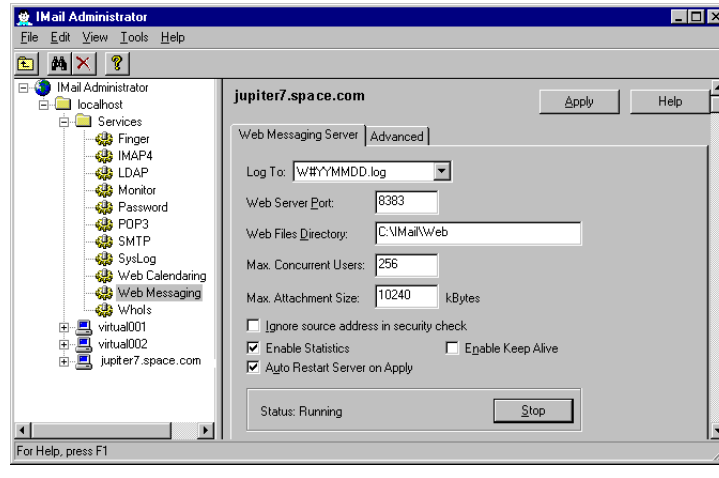
- IWebMsg.ini should have EnableSSL=1 (ForceSSL=1 may or may not be there).
- IWebMsg.ini is in proper windows directory (%WINDOWS% usually \Winnt).
- After changing IWebMsg.ini, stop service and restart it again to have changes recognized by the application.
- Select "Allow Service to interact with Desktop" to see if there is any message from SSL.DLL, like initialization failure because certificate or key file is not found. If SSL.DLL initialization has failed, then Web Messaging will not continue.
- If application is running but SSL is not working, EnableSSL is the only problem.
- SSL2.CGI allows change from secure to non-secure mode. If SSL is disabled, then changeover from secure to non-secure is not allowed; hence SSL2.CGI is not parsed.

- The private key file is protected using a password specified in SSL Configuration Utility. This password is required for decoding the key file while loading the SSL server. This password is stored in the registry and automatically retrieved during the loading process of SSL Server. The registry path for IMail Server is usually SOFTWARE\Ipswitch\imail\ssl. The registry path must be correct; otherwise an error message is generated and the files will not be created.

Configuring the Web Server

The Web Messaging server is installed on the host where the IMail Server software is installed. You can change the default port number and web directory, set SSL options, set other web server options, and start and stop the web server. (Some of these options can also be set in the *iwebmsg.in*i file in the *winnt* folder.)

1 Select the "**Services**" folder in the left panel and click **Web Messaging**. Then click on the **Web Messaging Server** tab.



2 Change any of the web server properties. See the previous sections for more information about the web server port and SSL.

Log to. This is where web server information will be stored. You can choose from:

W#YYMMDD.log	No Log
App Log	Log Server

Web Server Port. This is the port on the local system on which the Web Messaging server operates. If you change the port, the Web Messaging server must be stopped and restarted.

Note

If you use a non-standard port number (anything other than 80), users will need to specify the port in the logon web address. For more information, see "Web Address for the Web Messaging Server" on page 112.

Web Files Directory. This directory contains the files used to create web pages for Web Messaging. If you change this directory, you must stop and restart the web server.

Max Concurrent Users. This is the maximum number of users that can be logged into Web Messaging at the same time.This option must set between 256 and 1024 users.

Note

It is not possible to limit Web Messaging to allow less than 256 concurrent users, and no more than 1024. If a number outside of this range is entered for this option, it will still be displayed, but will not function. In that case even though the setting may display 2, the system is actually allowing 256 concurrent users.

Max Attachment Size. Use this setting to control the maximum size (in kilobytes) allowed for attachments.

Ignore source address in security check. Before displaying a page, the web server checks the IP address that requested the page against the IP address from which the user logged on. If you select this option, the web server does not check the IP address. This can be useful with some firewalls and with service providers that use dynamic IP addresses (such as America Online).

Enable Keep Alive. Turn on this option if you want to create a persistent TCP connection between the Web Messaging server and a browser (if the browser supports it). If the option is turned off, the server closes the TCP connection after each response.

Normally, the connection between a browser and a web server is valid only for a single request/response pair. Turning on **Enable**

Keep Alive can improve performance by reducing overhead per request, but it also means that less resources are available for other processes, such as creating new connections.

Note

If you turn on **Enable Keep Alive** and **Enable Thread Pooling**, the number of simultaneous connections allowed to the server will equal the **Max Work Threads**. Thus, you will be limiting the number of connections allowed.

Enable Statistics. Enables statistical information about the system, to be viewed through Web Messaging.

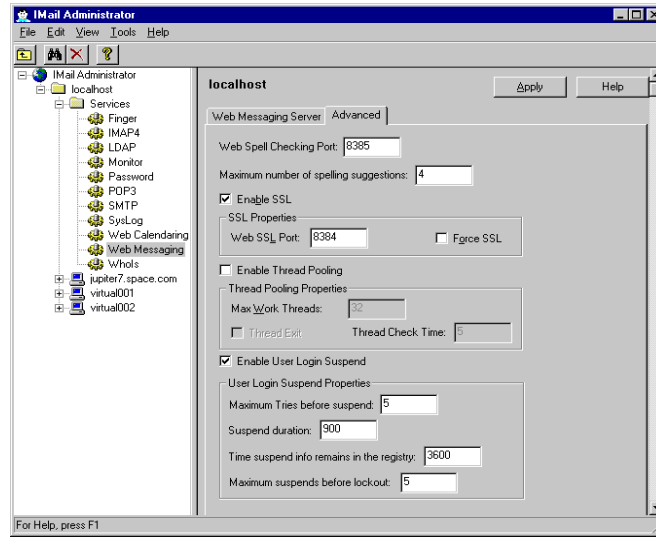
Auto Restart Server on Apply. If this is selected, the web server will be stopped and restarted automatically when you click **Apply** (if you changed anything requiring the server to stop and restart). We recommend that you select this option.

3 Click Apply to save your changes.

4 Click **Stop** to stop the Web Messaging server. The **Stop** button toggles to **Start**. Click **Start** to restart the server.

Advanced Tab

On the Advanced tab, you can set Spell Checking, SSL, thread pooling and user login suspend properties.



1 Optionally, set Spell Checking Options.

Web Spell Checking Port. The port which runs the spell checker's java applet. By default the port is 8385 but is configurable.

Maximum Number of Spelling Suggestions. The maximum number of spelling suggestions that will be given for a misspelled word.

For information about setting up spell check dictionaries, see the Spell Check section on page 109.

2 Optionally, set SSL options. For information about SSL, see "Using Secure Sockets Layer (SSL)" on page 113.

Enable SSL. Turn on this option if you are using the Secure Sockets Layer (SSL) utility to encrypt communications with the Web Messaging client. This sets the Web Messaging server to accept SSL connections in addition to normal connections.

Web SSL Port. The TCP port on which Web Messaging listens for an SSL-based HTTP request. If you used the default **Web Server Port** for Web Messaging (8383), then you can assign any TCP port number here, the default is 8384. The standard SSL port is 443.

Note

If you use a non-standard port number (anything other than 443), users will need to specify the SSL port in the logon web address.

Force SSL. Turn this option on if you want the Web Messaging server to accept only SSL-based HTTP connections; normal HTTP connections are not accepted.

3 Optionally, set **Thread Pooling** options.

Web Messaging can create a thread pool for handling HTTP requests (from the browser) on this TCP port. Using thread pooling reduces the overhead involved in creating and closing threads. However, if all threads in the pool are in use (in other words, your server is seeing heavy use), then an additional HTTP request will be denied. Also, threads reserved for use by Web Messaging are not available to other processes running on your server. You need to determine if thread pooling is appropriate for your Web Messaging server.

Enable Thread Pooling. Turn on this option to create a thread pool for handling HTTP requests from clients. Web Messaging creates up to **Max Work Threads** (default is 64) to process requests. If this option is turned off, Web Messaging creates a thread to handle each request (either persistent or normal) and after handling that request, destroys the thread.

Max Work Threads. Use this setting to constrain the load on your web server. This value sets the maximum number of work threads that can be used simultaneously by Web Messaging. If an HTTP request requires a work thread and the maximum has already been reached, Web Messaging returns a “server not available” message. This option requires that **Enable Thread Pooling** is turned on. The default value is 64.

Thread Exit. Turn on this option if you want Web Messaging to close a thread after the HTTP request is processed completely. Web Messaging will create a replacement for closed threads on next poll time, which is set in **Thread Check Time**. Turn off this option if you want Web Messaging to keep the thread open and available for another request. This option is used only when **Enable Thread Pooling** is turned on.

Thread Check Time. This is the interval (in seconds) used by Web Messaging to check the status of the thread pool. If the current number of work threads is less than **Max Work Threads**, then new threads are created. This option is used only when **Enable Thread Pooling** is turned on. The default value is 10 seconds.

4 Optionally, set suspend user options

Enable User Login Suspend. Turn on this option to activate automatic suspension of user accounts. This occurs only when an account has met the criteria listed by the administrator.

Maximum Number of Tries before Suspend. The maximum number of times a user can attempt to logon before their account is suspended.

Suspend Duration. The amount of time(in seconds), that the account will be suspended.

Time Suspend Info Remains in the Registry. The amount of time that information about suspended accounts is stored.

Maximun Number of Suspends Before Lockout. The maximum number of times a user can attempt to logon before being locked out of the system.

5 Click **Apply** to save your changes.

Setting Access to Web Messaging Functions

Web Messaging provides access to mail functions based on the user permissions granted in the IMail Administrator. Permissions can be assigned for each individual mail account or globally, for all users on a mail host. A user can be granted some or all of the following permissions:

Allow Web Access. Allows this user access to their account via Web Messaging.

Host Administrator. Allows this user to add, modify, or delete users and aliases and set rules on their mail host. **Allow Web Access** must also be selected.

List Administrator. Allows this user to remotely manage IMail Server mailing lists on their mail host. **Allow Web Access** must also be selected.

IMail System Administrator. Lets this user manage all mail hosts, view the spool directory and logs, set rules, and edit the messages displayed when users log on to Web Messaging. If this user also has **Host Administrator** permission, they can manage user accounts and aliases on *all* mail hosts. If this user has **List Administrator** permission, they can manage lists on *all* mail hosts. **Allow Web Access** must also be selected.

To set access to Web Messaging for an individual user mail account:

1 In IMail Administrator, select the mail host, and then select the "**Users**" folder. Select a user ID to see the user's properties in the right panel.

2 Select **Allow Web Access** and then click **Apply** to apply the change.

3 Optionally, click the **Host Administrator**, **List Administrator** or **IMail System Administrator** options to allow this user access to the extended menu options associated with each. Click **Apply** to save any changes.

To set **Allow Web Access** as the default for all *new* users that you create:

1 Select the mail host, and then select the "**Users**" folder.

2 Select **Allow Web Access** and click **Apply** to apply the change.

To set **Allow Web Access** to be the default for all *existing* users:

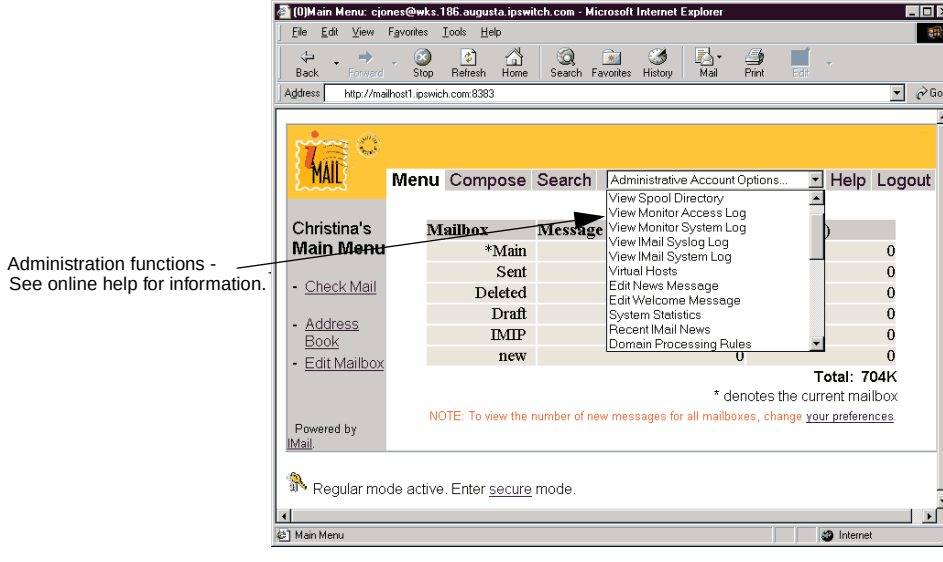
1 Select the mail host, and then select the "**Users**" folder to see the default settings in the right panel.

2 Select **Global User Changes**.

3 Select **Allow Web Access** and then click **Change ALL Accounts** to apply the change.

Using Remote Administration Functions

An extended menu containing remote administration functions is available to you if your mail account has Host Administrator, List Administrator or IMail System Administrator access enabled. See "Setting Access to Web Messaging Functions" for how to grant permissions.



The following sections provide an overview of the remote administration functions. See the Web Messaging online help for more information on these functions.

User Administration

If you have User Administrator permissions, you can add, modify, and delete user mail accounts for your mail host. If you have User Administrator and IMail System Administrator permissions, you can add, modify, and delete user mail accounts for *any* mail host.

Alias Administration

If you have Alias Administrator permissions, you can add, modify, and delete aliases for your mail host. If you have Alias Administrator and IMail System Administrator permissions, you can add, modify, and delete aliases for *any* mail host. See “Chapter 4: User Mail Accounts” on page 59 for a description of the alias properties.

List Administration

If you have List Administrator permissions, you can add, modify, delete and moderate lists for your mail host. If you have List Administrator and IMail System Administrator permissions, you can add, modify, delete and moderate lists for *any* mail host.

Viewing Monitor Logs and the Spool Directory

If you have IMail System Administrator permissions, you can view the following IMail Server log files.

- Monitor Access Log — shows each access attempt to the Web Messaging server and to the IMonitor web server.
- Monitor System Log — shows logons to the mail server and to the IMonitor web server and shows the status of services.
- IMail System Log — shows IMail Server send and receive mail transactions. This shows the contents of *syslog.txt*.
- IMail Syslog Log — records transaction and debug information when enabled in each of the servers (for example, POP3 and SMTP). This shows the contents of *lognnnn.txt*, the System Log Service file.
- Spool directory — shows all IMail Server send and receive mail transactions that are in process. Click **View Spool Directory** to display the spool information.

For more information on the log files and spool directory, see “Appendix E: Spool, Queue, and Log Files.”

Managing Virtual Hosts

If you have IMail System Administrator permissions, you can add, modify, and delete virtual (mail) hosts.

Managing Mailing Lists

If you have List Administrator permissions, you can create, modify, and delete list server mailing lists.

Setting Rules

If you have Host Administrator permissions, you can set rules for the mail host. If you also have IMail System Administrator permissions, you can set rules for *any* mail hosts. Regular users can set rules for their own mail account.

Editing News of the Day and Welcome Message

If you have IMail System Administrator permissions, you can add, delete, or modify the News of the Day and the Welcome message directly from the Web Messaging interface.

Spell Checker

IMail Web Messaging has added a spell check feature, which allows users to check for spelling errors using specific dictionaries. The spell check is a java applet, and comes equipped with two dictionaries to choose from. The administrator can select which dictionaries to install for the primary domain during installation. For procedures to install the dictionaries in other domains, see "Installing Dictionaries for Domains" below.

Note

In order to use Spell Check, the user must have Java Runtime Environment (JRE) 1.1 or 1.2 installed on their computer.

Installing Dictionaries For Domains

During installation, the dictionary files are installed for the primary domain only. In order for users in other domains to use Spell Check, the administrator must copy the dictionaries from the *[IMail Top Directory]* into the user's or host's folder. If during installation, you choose to keep your existing files but save the new ones, then the dictionary files will be located in *[IMail Top Directory]\Web\New\TopDir.*

The user's folder is located at:

[IMail Top Directory]IMail\users\"user's name"

After copying the files into the user's or Host's folder, the dictionaries will be available for use, and will be displayed in the dictionary selection box on the **Compose** page.

Enabling Spell Check

Before a user can take advantage of the spell checker, the administrator must first enable the spell checking option for the User's account. (Spell Checking is enabled by default for all new user accounts when it is enabled for the domain.)

To enable Spell Checking for an individual user:

1 Select **User Administration** from the Web Messaging interface.

2 Select the user account that you want to enable spell check for and click **Modify**.

3 Select **Enable Spell Checking** and click **Save**.

To enable Spell Checking for all new accounts in a domain:

1 Select **User Administration** from the Web Messaging interface.

2 Select the appropriate domain from the **Current Domain** List box.

3 Under Default Attributes for all Users, select **Enable Spell Checking**.

4 Click **Update Attributes** to save your changes.

Spell Check can also be enabled globally for a domain through IMail Administrator on the host's **Web Options** tab.

Note

Users must select the appropriate Java setting with which to run the spell checker. If the wrong java setting is selected, the user will receive an "invalid user error." To select a Java setting, select **Edit My Preferences** from the Web Messaging interface. Then in the spell check applet field, select either 1.1 or 1.2. The default Java Runtime Environment is 1.1.

Accessing Spell Check

The Spell Checker can be accessed through the following Web Messaging pages: draft.html, fwdmsg.html, replymsg1.html, sendmail.html. The user must select at least one dictionary in order to be able to use spell check. Once a message has been entered in the **Body** field, click on the **Spell Check** button, to launch the Spell Checker. You can spell check a message that contain up to 65,000 characters.

Disabling Spell Check

Spell Checking is enabled by default for all new accounts. If however, you do not want users to use the Spell Checker, it can be disabled.

To disable Spell Checker for an individual user:

1 In the Web Messaging interface, select **User Administration** from **Administrative Account Options**.

2 Select the user account that you want to disable spell check for and click **Modify User Account**.

3 Deselect **Enable Spell Checking** and click **Save**.

To disable Spell Checker for all users in a domain:

1 Select **User Administration** from the Web Messaging interface.

2 Select the appropriate domain from the **Current Domain** List box.

3 Under Default Attributes for all Users, deselect **Enable Spell Checking**.

Editing Dictionaries

The Spell Checker contains compressed dictionary files., which have a .clx extension, and cannot be edited.

Each user has a user dictionary that they can customize to fit their needs. This file is called Userdict.tlx and can be edited by completing the following steps.To edit the User Dictionary, select **Edit User Dictionary** from the **Options** menu.This option allows the user to customize the user dictionary, by adding or deleting words.

Note

Additional word lists and dictionaries can be incorporated into the Spell Checker if desired. These files and dictionaries are easily integrated into IMail by copying them into the TopDir directory of a host.

Dictionary Explanations

The dictionary files are word lists that are in a compressed file format and are not editable. The user dictionary is editable.

User Dictionary(UserDict.tlx)- This dictionary is created for the new user. Words can be added to or removed from the user dictionary. Words in user dictionaries may be offered as suggestions for misspelled words.

American English Dictionary (ssceam2.clx). Contains American English words.

American Legal Dictionary (sscela2.clx). Supplements the American English dictionary with words related to jurisprudence, law,criminology, and law enforcement.

American Medical Dictionary (sscema2.clx). Supplements the American English dictionary with words related to anatomy, diseases, health care, generic and trademark drug names, and medical research.

Brazilian Portuguese Dictionary (sscepb2.clx). Contains 119,000 Brazilian Portuguese words.

British English Dictionary (sscebr2.clx). Contains British English words.

British Legal Dictionary (sscelb2.clx). Supplements the British English dictionary with words related to jurisprudence, law, criminology, and law enforcement.

British Medical Dictionary (sscemb2.clx). Supplements the British English dictionary with words related to anatomy, diseases, health care, generic and trademark drug names, and medical research.

Danish Dictionary (ssceda2.clx). Contains 102,000 Danish words.

Dutch Dictionary (scedu2.clx). Contains 178,000 Dutch words, including the" new spelling" (De Nieuwe Spelling).

Finnish Dictionary (sscefi2.clx). Contains 251,000 Finnish words.

French Dictionary (sscefr2.clx). Contains 137,000 French words, including both European and Canadian French.

German Dictionary (sscege2.clx). Contains 295,000 German words, including spelling reform (Die Neue Rechtschreibung).

Italian Dictionary (ssceit2.clx). Contains 283,000 Italian words.

Norwegian Bokmal Dictionary (sscenb2.clx). Contains 95,000 Norwegian words in the Bokmal dialect.

Portuguese Dictionary(sscepo2.clx). Contains 135,000 European Portuguese words.

Spanish Dictionary (sscesp2.clx). Contains 288,000 Spanish words.

Swedish Dictionary (sscesw2.clx). Contains 110,000 Swedish words.

Displaying Online Advertisements

You can set up the Web Messaging interface to display advertising. Ads are displayed at the top of each Web Messaging page and can consist of HTML text and/or graphics, including hyperlinks. Multiple ads are also supported on a time-sharing basis. With Ad Support enabled, Web Messaging cycles through up to 1000 ads, changing the displayed ad every 30 seconds.

To enable ad support:

1 In IMail Administrator, select the mail host, then select the **Web Messaging Ad Support** tab.

2 Turn on **Enable Ad Support**.

To disable ad support, make sure this box is turned off.

To create or edit an online advertisement:

1 On the **Web Messaging Ad Support** tab, click **Add**. Enter the HTML code and text for the ad in the text box and click **Apply**.

The ad can contain up to 512 characters of HTML code. It can display a *.gif* file and can link to a web address (URL). If the ad is larger than the frame size, a scroll bar appears on the right side of the frame. Thus, an ad can be a full web page.

You can enter up to 1000 ads using the interface. The ad displayed on the Web Messaging page will be changed every 30 seconds.

The ads are saved in the *ads.txt* file. If you prefer edit outside IMail Administrator, you can enter and edit ads by opening *ads.txt* in an editor. There is no limit to the number of ads you enter in *ads.txt*.

To create or edit a trailer message:

The trailer (tail) message displays in the frame at the bottom of the screen if you have Ad Support enabled.

Select the mail host and click the **Web Messaging Content** tab. This must be a full HTML page, starting with `<HTML><BODY>` and ending with `</BODY></HTML>`. The trailer message is stored in the *mailtail.html* file.

A nice idea for using the trailer message is to use a Java scrolling text area to print any current news.

In addition to the above procedure, you can also edit *mailtail.html* directly in a text editor. *mailtail.html* is located at *[IMail Top Directory]\Web.*

Customizing Web Messaging

The Web Messaging interface is comprised of web pages that provide access to e-mail functions, personal mail account information, and remote administration functions.

“Appendix G. Changing the Look and Feel of Web Messaging” on page 285 describes how you can create your own look and feel for the Web Messaging interface. If you have multiple mail hosts, each mail host can have a different Web Messaging interface.

Chapter 7: IMail Web Calendaring

This chapter describes how to configure and use **IMail Web Calendaring**. Before users can use Web Calendaring, the administrator must enable **IMail Web Calendaring** access for users as described in this chapter.

What is IMail Web Calendaring?

IMail Web Calendaring allows users to store schedules, set appointments, and send reminder information using a web browser. Users can log on to Web Calendaring and perform their calendar activities using Microsoft Internet Explorer version 4.0 or higher and Netscape version 4.0 or higher.

In addition to the various scheduling capabilities, IMail Web Calendaring offers the following:

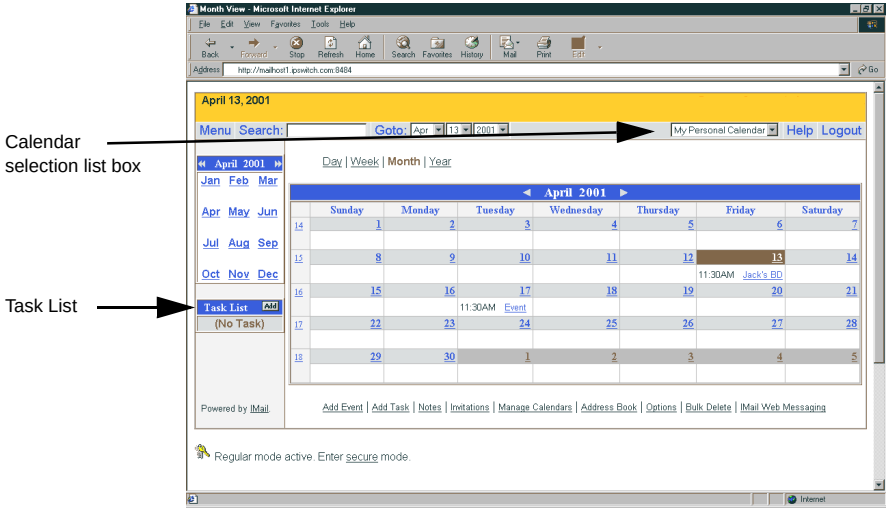
E-mail Reminders for Events. When an event is scheduled, users have the option of receiving an e-mail to remind them of the event. Up to two reminder e-mails can be sent before or after the event.

E-mail Invitations. Not only can users schedule an event, but they can also invite others to the event, all from the same page. If an invitation is sent to another IMail Web Calendaring user, that user can go to the Invitations page in Web Calendaring to either accept the invitation and add it to their calendar, or reject it.

Search Feature. IMail Web Calendaring has a search feature which lets a user look up any entry on a calendar by name, if they are unsure of its date or time. The search results will include Tasks, Notes, and Events.

Customizable interface. You can create your own look and feel for the Web Calendaring interface by editing the HTML templates and other files used to generate the Web Calendaring pages. If you have multiple mail hosts, each mail host can have a different Web Calendaring interface. For information on customizing the interface, see “Appendix H. Changing the Look and Feel of Web Calendaring” on page 303.

Online ads. IMail Web Calendaring also supports the display of advertisements on all Web Calendaring pages. This feature is very useful to Internet Service Providers (ISPs) and other mail service providers who would like to sell online advertising space on their mail server. This feature can also be used to display announcements on an intranet. For more information about online ads, see “Displaying Online Advertisements” on page 143.



What Can Users Do with IMail Web Calendaring?

Web Calendaring provides users with a web interface that gives them the ability to schedule tasks, set appointments, and receive e-mail reminders that contain the date, time, and description of the appointment.

Users can connect to the Web Calendaring server and log on to their mail account using their IMail user ID and password.

Users can access Web Calendaring by entering the web server's address in their browser's address field. This web address consists of the host name of the IMail Server host and a web server port number. The default port number is 8484. For example, if your IMail Server mail host is named host1.ipswitch.com, then the web address is:

http://host1.ipswitch.com:8484

Users can bookmark the address (save it as a Favorite site) in their web browser.

Once logged in, users can schedule appointments and events, record notes, receive e-mail reminders for events and send invitations to others.

Users can also set preferences to change the default settings of the calendar. They can change the opening view, as well as display settings for the calendar.

Users can follow a link directly to IMail Web Messaging without logging out of Web Calendaring.

Online help is available from the Web Calendaring pages.

System Requirements

The Web Calendaring server is installed on the host where the IMail Server software is installed.

To access their calendars, users need a frames-capable browser. Older versions of browsers may not support frames. IMail Web Calendaring is designed to support Microsoft Internet Explorer version 4 or later, Netscape Navigator version 4 or later, and other HTML 3 compliant browsers.

IMail Web Calendaring Security

IMail Web Calendaring offers several means of protecting your communications from being altered in transit or being read by someone other than the intended recipient.

Secure Mode. Enables Secure Sockets Layer encryption. The SSL capabilities offer the most secure method of safeguarding schedule information. SSL will increase processing time on your server.

Logon User ID and password. Users must log on with their user ID and password. This provides the basic level of security that protects the user's calendar.

Logoff. After accessing their calendar from the browser and then logging off, users cannot click the browser's **Back** button to return to a calendar. However, clicking in the History list may re-display the calendar, though the user could not activate any of the calendar

functions. As a precaution, users can clear the browser's history if the browser is in a commonly used area.

When logging on to IMail Web Calendaring, users can choose either or both of the following options (on the Login page):

Expire page views. If you are logging on to your calendar from a public terminal or from someone else's computer, you can select this option to prevent the browser from saving (caching) the pages you view. Note that Microsoft's Internet Explorer can be set to ignore this "expire page views" command, so it is still possible your pages will be saved.

Remember Userid and Password. This option will save your password in a file (called a cookie), so you do not have to enter it each time you log on to Web Calendaring. When you log on, the browser enters the User ID and password. Note that if you select this option, anyone who has access to the machine could connect to your calendar through IMail Web Calendaring without having to enter your User ID and password. Do not use it on a public terminal.

Setting Up IMail Web Calendaring

To set up IMail Web Calendaring, you need to:

- Determine the web address for your Web Calendaring server.
- Optionally, set up the SSL capability to provide secure communications between the server and users' browsers.
- Set user access to Web Calendaring.

Web Address for the IMail Web Calendaring Server

By default, the IMail Web Calendaring server is assigned a web address that consists of the host name of the IMail Server host and a web server port number. The default port number is `8484`. If your mail host had a name of host1.ipswitch.com, then the address will be: `http://host1.ipswitch.com:8484`

Your mail users can start IMail Web Calendaring by entering the address in their browser's address field.

If you are not running another web server on the same host, you can set the port number to the normal HTTP (web) server port of `80`. In this case, users do not have to specify the port with the web address.

For example, you could enter: `http://host1.ipswitch.com`

Note that some firewalls may block the 8484 port, in which case you need to change the port number.

If You Have Multiple Mail Hosts

If you have set up multiple mail hosts on your IMail Server system, the web address is determined by whether the mail host has it's own IP address or uses a virtual IP address. (For information on virtual hosts, see "Chapter 3: Configuration" on page 33.)

If each host has its own IP address, you will have a different web address for each host. For example, if you have set up the following hosts:

`mail.marcel.com`	156.21.50.78
`mail.magnolia.net`	156.21.50.80

the web address for the respective hosts would be:

```
mail.marcel.com:8484
mail.magnolia.net:8484
```

If a mail host does not have an IP address, then it will have the same web address as the primary mail host. For example, if you have set up the following hosts:

`mail.marcel.com`	156.21.50.78
`mail.magnolia.net`	<$virtual IP>

the web address for both hosts would be:

```
mail.marcel.com:8484
```

The host *mail.magnolia.net* can still have its own set of users, but users on this host must identify the host when they enter their logon user ID. For example, the user *fred* on *mail.magnolia.net* would enter the web address *mail.marcel.com:8484* to open the Logon page, then enter *fred@mail.magnolia.net* as his user ID.

Using Secure Sockets Layer (SSL)

You can set up the Web Calendaring server to use Secure Sockets Layer (SSL) for communications between a browser and the server. SSL encrypts your communications so they can be read only by the intended recipient.

SSL is a protocol that uses "certificates" to authenticate the client and server and uses a public/private key "pair" to encrypt and decrypt

communications. All of the major browsers are SSL enabled.

Certificates. Certificates are used to establish the identity of the client (browser) and the server.

You can run SSL for Web Calendaring with:

- A self-signed SSL certificate. The server identifies itself to the client, but its certificate has not been issued by one of the third-party Certificate Authorities. Clients who log on to IMail Web Calendaring using Netscape and Internet Explorer will receive a warning message ("This site is not secured..."). These users can continue logging on after acknowledging the warning.
- An SSL certificate issued by a Certificate Authority. The certificate verifies to the client that the identity claimed on the certificate is accurate. You can purchase a third-party certificate from Thawte consulting (www.thawte.com) or Verisign (www.verisign.com).

IMail Server comes with an SSL Utility that generates both an IMail Server self-signed SSL certificate as well as a certificate request you can send to a Certificate Authority.

Public/private key encryption. When a browser connects to the Web Calendaring server, the server sends its certificate and public key to the browser. The browser can now use the public key to encrypt communications. Only the web server has the private key, which is used to decrypt communications sent from the browser.

Ciphers. The server and client must agree on the algorithm, called a "cipher," used to encrypt data. You select the cipher when setting up SSL on the server.

For more information on how SSL works, visit

home.netscape.com/security/techbriefs/ssl.html.

Setting Up SSL on the Server

This section outlines the procedure for setting up SSL on the server.

- First, you use the IMail SSL Configuration Utility to set up the SSL certificate and public/private key pair.

- Then, you enable SSL in the IMail Administrator. Expand the "**Services**" folder and click on **Web Calendaring**. The **Web Calendaring Server** tab appears.

For detailed information about the SSL options, see the online help in the IMail SSL Configuration Utility and help for the **Web Calendaring Server** tab in IMail Administrator.

To enable SSL for the Web Calendaring Server, you need to do the following:

1 Set the registry path for the SSL keys.

From the **Start** menu**, select Programs -> IMail -> IMail SSL Configuration Utility**. Select **Registry Path** from the **File** menu. Enter the path: `software\ipswitch\imail\ssl`

2 Generate a certificate and public key. We recommend that you use the self-signed certificate for your server.

In the **IMail SSL Configuration Utility**, click **Certificate**. For more information, select **Help Topics** from the **Help** menu, then go to the "Getting an SSL Certificate" topic.

3 Configure SSL and select the cipher to use for encryption.

In the SSL Configuration Utility, click **SSL Configuration**, and then complete the wizard. For information, select **Help Topics** from the **Help** menu, then go to the "Configuring SSL" topic.

4 If you want the server to authenticate clients, configure how it will do it.

In the SSL Configuration Utility, click **Client Authentication**. For more information, select **Help Topics** from the **Help** menu, then go to the "Dealing with Clients" topic.

We recommend that you allow any client to connect to your server, thus you would not turn on the **Client Authentication** option.

5 Activate SSL for the Web Calendaring server. In the IMail Administrator, expand the "**Services**" folder and click on **Web Calendaring**, then select the **Web Calendaring Server** tab to show the SSL options. Turn on **Enable SSL**.

Starting an SSL Connection from a Browser

Users can open Web Calendaring with an SSL connection as follows:

1 In the browser, enter the address for the Web Calendaring server, for example: `mail.domain1.com:8484`. The Web Calendaring Logon appears.

2 On the Logon page (or on any other Web Calendaring page), select **Enter Secure Mode**.

3 The browser usually asks you to confirm that you want to use "secure mode." Click **OK**. If you used the self-signed certificate, the browser may also display a warning that the certificate is not "trusted." Click **OK** again to continue.

The browser is now in secure mode. You can click again at the bottom of any Web Calendaring page to return to regular mode.

Enabling SSL from within the Web Address

When you enter the web server's address in a browser and use HTTPS (in place of HTTP) in the address, the browser attempts to connect to the server using SSL. For example, the address would look like:

```
https://mail.domain1.com:8484
```

Using a Different Port for SSL

The standard port for IMail Web Calendaring SSL is 8485. If you use a different port number, this port number must be specified in the web address that Web Calendaring users log on to. For example, if you use port 8485 for SSL, and the web server is on port 8484 of mail1.domain.com, the web address would be:

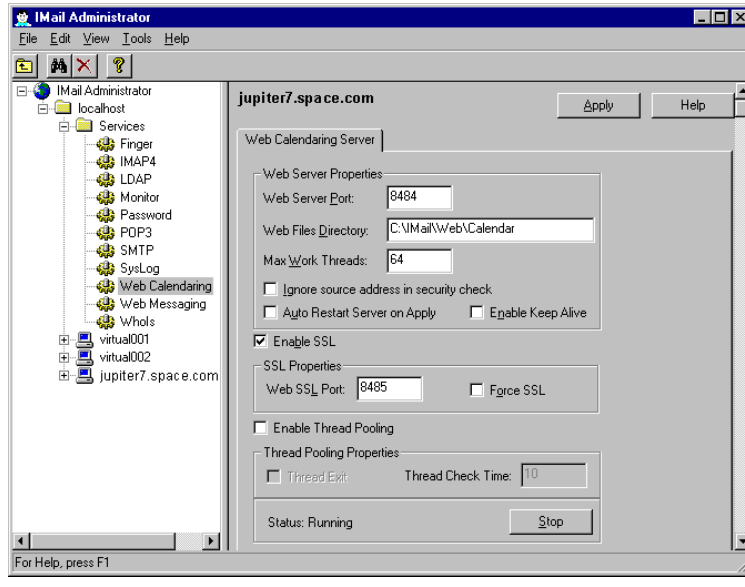
```
http://mail.domain1.com:8484:8585
```

Users can bookmark the web address (save it as a Favorite), so they do not have to enter it each time they log on.

Configuring the Web Calendaring Server

The Web Calendaring server is installed on the host where the IMail Server software is installed. You can change the default port number and web directory, set SSL options, set other web server options, and start and stop the web server. (Some of these options can also be set in the *iwebcal.in*i file in the *winnt* folder.)

1 Select the "**Services**" folder in the left panel and click **Web Calendaring.** The **Web Calendaring Server** tab appears.



2 Change any of the web server properties. See the previous sections for more information about the web server port and SSL.

Web Server Port. This is the port on the local system on which the Web Calendaring server operates. If you change the port, the Web Calendaring server must be stopped and restarted.

Note

If you use a non-standard port number (anything other than 80), users will need to specify the port in the logon web address. For more information, see "Web Address for the IMail Web Calendaring Server" on page 134.

Web Files Directory. This directory contains the files used to create web pages for Web Calendaring. If you change this directory, you must then stop and restart the web server.

Ignore source address in security check. Before displaying a page, the web server checks the IP address that requested the page against the IP address from which the user logged on. If you select this option, the web server does not check the IP address.

This option can be useful with some firewalls and with service providers that use dynamic IP addresses (such as America Online).

Enable Keep Alive. Turn on this option if you want to create a persistent TCP connection between the Web Calendaring server and a browser (if the browser supports it.) If the option is turned off, the server closes the TCP connection after each response.

Normally, the connection between a browser and a web server is valid only for a single request/response pair. Turning on **Enable Keep Alive** can improve performance by reducing overhead per request, but it also means that less resources are available for other processes, such as creating new connections.

Auto Restart Server on Apply. If this is selected, the web server will be stopped and restarted automatically when you click **Apply** (if you changed anything requiring the server to stop and restart). Ipswitch recommends that you select this option.

3 Optionally, set SSL options. For information about SSL, see "Using Secure Sockets Layer (SSL)" on page 113.

Enable SSL. Turn on this option if you are using the Secure Sockets Layer (SSL) utility to encrypt communications with the Web Messaging client. This sets the Web Calendaring server to accept SSL connections in addition to normal connections.

Web SSL Port. The TCP port on which Web Calendaring listens for an SSL-based HTTP request. If you used the default **Web Server Port** for Web Calendaring (8484), then you can assign any TCP port number here, the default is 8485. The standard SSL port is 443.

Note

If you use a non-standard port number (anything other than 443), users will need to specify the SSL port in the logon web address.

Force SSL. Turn this option on if you want the Web Calendaring server to accept only SSL-based HTTP connections; normal HTTP connections are not accepted.

4 Optionally, set **Thread Pooling** options.

Web Calendaring can create a thread pool for handling HTTP requests (from the browser) on this TCP port. Using thread pooling reduces the overhead involved in creating and closing threads. However, if all threads in the pool are in use (in other words, your server is seeing heavy use), then an additional HTTP request will be denied. Also, threads reserved for use by Web Calendaring are not available to other processes running on your server. You need to determine if thread pooling is appropriate for your Web Calendar server.

Enable Thread Pooling. Turn on this option to create a thread pool for handling HTTP requests from clients. Web Calendaring creates 64 work threads to process requests. If this option is turned off, Web Calendaring creates a thread to handle each request (either persistent or normal) and after handling that request, destroys the thread.

Thread Exit. Turn on this option if you want Web Calendaring to close a thread after the HTTP request is processed completely. Web Calendaring will create a replacement for closed threads on next poll time, which is set in **Thread Check Time**. Turn off this option if you want Web Calendaring to keep the thread open and available for another request. This option is used only when **Enable Thread Pooling** is turned on.

Thread Check Time. This is the interval (in seconds) used by Web Calendaring to check the status of the thread pool. This option is used only when **Enable Thread Pooling** is turned on. The default value is 10 seconds.

5 Click the **Stop** button to stop the Web Calendaring server. The Stop button toggles to **Start**. Click **Start** to restart the server.

Setting Access to IMail Web Calendaring

IMail Web Calendaring provides access to calendar functions based on the user permissions granted in the IMail Administrator. Permissions can be assigned for each individual mail account or globally, for all users on a mail host.

Setting access to Web Calendaring for an individual user.

1 From the Web Messaging interface, select **User Administration** from **Administrative Account Options**.

2 Select the User ID from the listbox, and click **Modify User Account**

3 Under User Attributes, select the **Enable IMail Web Calendaring** option.

4 Click **Save** to update your changes.

To apply settings as defaults for all *new* users.

1 From the Web Messaging interface, select **User Administration** from the **Administrative Account Options**.

2 In the User Attributes section, select the checkbox next to the attributes that you want to enable for all new users.

3 Click **Save** to update your changes.

Note

Web Calendaring and Spell checking are enabled by default for all new users

---

Enable SSL, Spell, Check and Web Calendaring for an entire domain.

1 In IMail Administrator, expand the "localhost" folder and select a host. Click on the **Web Options** tab.

2 Enable Spell Checking, SSL, or Web Calendaring, by selecting the check box beside each feature.

3 Click **Apply** to save your changes.

Additionally, IMail Web Calendaring may also be enabled by an administrator from IMail Web Messaging.

Setting user access to Web Calendaring from Web Messaging .

1 From **Administrative Account Options**, select **User Administration.**

2 Under **Default Attributes**, select **Allow Web Access** and **Enable IMail Web Calendaring**.

3 Click **Update Attributes**.

Invitations

Sending E-mail Invitations

When scheduling an event, a user can invite others to the event by sending them an e-mail invitation. Invitations are sent to people whose e-mail addresses are placed in the **Invitee** section of the **Add Event**, or **Add Task** pages.

If the Invitee uses IMail Web Calendaring, they will receive an e-mail invitation, and the invitation will be displayed on the **Invitations** page in IMail Web Calendaring. If the invitee does not use IMail Web Calendaring, they will still receive an e-mail notifying them of the event.

Viewing Invitations

IMail Web Calendaring users not only have the ability to send invitations to others but they can also view all of their invitations on one page and confirm or reject those invitations. All of these functions are performed from the **Invitations** page in IMail Web Calendaring. Clicking on the **Invitations** link displays a list of all invitations that have been sent to you by other users. Clicking on one of the invitation names, displays more information about the event, and allows the recipient to reject or confirm the invitation.

Accepting Invitations

Click on the **Confirm** button to automatically add the event to the calendar. The entry will then appear on the calendar when the user is in **Day** or **Month** view.

Declining Invitations

Click on the **Reject** button to automatically delete the invitation from the **Invitations** page. In this case, the event will not be added to the calendar.

Displaying Online Advertisements

You can set up IMail Web Calendaring to display advertising. Ads are displayed at the top of each calendar page and can consist of HTML text and/or graphics, including hyperlinks. Multiple ads are also supported on a time-sharing basis. With Ad Support enabled, IMail

Web Calendaring cycles through up to 1000 ads, changing the displayed ad every 30 seconds. You can enable ads for each mail host. Thus making it possible to have different ads for different hosts.

To enable ad support:

1 In IMail Administrator, select the mail host, then select the **Web Calendaring Ad Support** tab.

2 Turn on **Enable Ad Support**.

To disable ad support, make sure this box is turned off.

To create or edit an online advertisement:

1 On the **Ad Support** tab, click **Add**. Enter the HTML code and text for the ad in the text box and click **Apply**.

The ad can contain up to 512 characters of HTML code. It can display a *.gif* file and can link to a web address (URL).

If the ad is larger than the frame size, a scroll bar appears on the right side of the frame. Thus, an ad can be a full web page.

You can enter up to 1000 ads using the interface. The ads you entered are saved in the file *ads.txt*. If you prefer to use an editor rather than the IMail Administrator, you can enter and edit ads by opening *ads.txt* in an editor. There is no imposed limit to the number of ads if you enter them manually in the *ads.txt* file.

To create or edit a trailer message:

The trailer (tail) message displays in the frame at the bottom of the screen if you have Ad Support enabled.

Select the mail host and click the **Web Calendaring Content** tab. This must be a full HTML page, starting with `<HTML><BODY>` and ending with `</BODY></HTML>`. The trailer message is stored in the *tail.html* file.

A nice idea for using the trailer message is to use a Java scrolling text area to print any current news.

In addition to the above procedure, you can also edit *tail.html* directly in a text editor. *tail.html* is located at *[IMail Top Directory]\Web\Calendar.*

Customizing IMail Web Calendaring

The IMail Web Calendaring interface is comprised of web pages that provide access to calendar functions.“Appendix H. Changing the Look and Feel of Web Calendaring” on page 303 describes how you can create your own look and feel for the calendar interface.

If you know how to edit HTML code, you can rearrange the components of a page, or change the text next to radio buttons or in hyperlinks, by editing web templates used to generate the web pages.

You can change the button colors and styles, and page background colors and styles by replacing the default graphic files with your own graphic files.

If you have multiple mail hosts, each mail host can have a different calendar interface.

Chapter 8: SMTP Server

The SMTP server sends and receives mail from other Internet hosts using the Simple Mail Transfer Protocol (SMTP). The SMTP server processes incoming and outgoing mail. Outgoing mail is spooled until the SMTP server can confirm it has arrived at its destination. Incoming mail is spooled until users access it using a POP3 or IMAP4 mail client. Spooling allows the transfer from client and server to occur in the background.

You can use settings to secure your SMTP server from unwanted use. See “Chapter 9: Security and Antispamming”for more information.

SMTP RFCs Supported

The SMTP Server supports the following Request for Comments (RFCs):

- RFC 821 and 822 SMTP
- RFC 1869 SMTP Service Extensions
- RFC 1870 SMTP Service Extension for Message Size Declaration
- RFC 1891,1892,1893,1894 SMTP Service Extension for Delivery Status Notifications
- RFC 1985 SMTP Service Extension for Remote Message Queue Starting. Currently, IMail Server provides support for “ETRN host.name” and “ETRN @domain.name.” For more information, see “Using ETRN to Retrieve Mail” on page 54.
- RFC 2222 SMTP Service Extension for Authentication. IMail Server supports PLAIN, LOGIN, and CRAM-MD5.

Basic Information

The SMTP server program will continue to run when you log off the system. This server can run completely hidden or with some feedback.

The SMTP server uses the *smtpd32.exe* program and gets most of its settings from the NT Registry. Therefore, you MUST remove and re-install the SMTP server if you move its location. This is because the full path to the application is stored in the NT Registry.

Logging On

By default, the SMTP service logs on to the System Account and starts automatically. You can view and change SMTP settings using the Services application in the Windows NT/2000 Control Panel.

To view and/or change settings for the SMTP service:

1 In the Control Panel, select the Services application. The Services dialog box appears.

2 Select the **IMail SMTP Server** service and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the account you want to log on to.

If any of your hosts uses the Windows NT User Database option to register and authenticate users, the SMTP service MUST log on to the **System Account**.

If you want to see the icon for the service, in the Services application, select **Allow service to interact with desktop**. If you select this, the SMTP service will run under the current logged on user account. (Refer to the Windows NT documentation for more information.) The SMTP service will continue to run even if you log off. The icon will disappear but will reappear the next time you log on as the same user.

If none of your hosts uses the Windows NT Database, you can select **This Account** and then select the name of the user whose account you want the service to log on to. Make sure the specified user is a Host Administrator.

Note

If one or more of your mail domains is based on an external database, the SMTP service must log on to an account that has access to the external database.

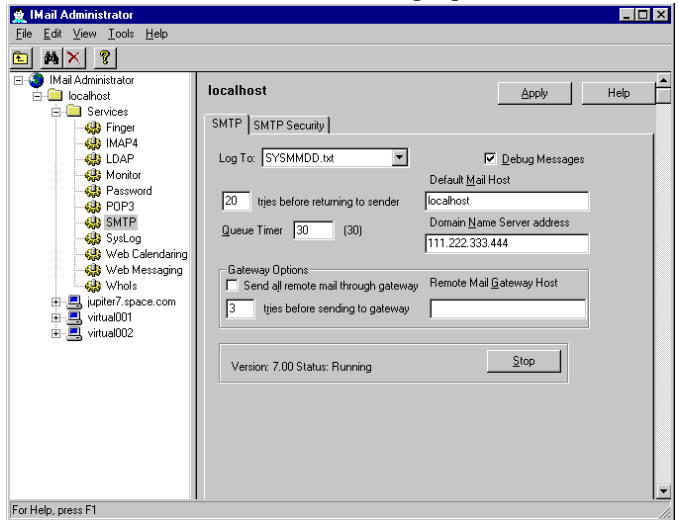
Make sure you send several test messages after installation and look in whichever log file is logging SMTP, and in the *event log*. If the SMTP service cannot create the lock file, the permissions are probably set incorrectly.

Configuring the SMTP Server

To configure the SMTP server:

1 Select the "**Services**" folder in the left panel and click on **SMTP**.

2 Then click on the SMTP tab in the right panel.



3 Enter the options you want to use to configure the SMTP server. (Each option is described below in "SMTP Options".)

4 Click **Apply** to save your changes.

5 After making changes, stop the SMTP service, wait 5-10 seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start Service** button.

6 Click **OK** to exit the dialog box.

SMTP Options

You can use the following options to configure the SMTP server.

Logging Options

In the **Log To** box, select the file that you want to use for logging SMTP events.

- **No Log** disables logging.
- **SYSMMDD.TXT** causes all inbound and outbound mail to be logged in the file: `MAILDIR/spool/sysmmdd.txt`, where *mm* is the month and *dd* is the day the log was written.
- **App Log** causes inbound mail to be logged in the Application Log, which is viewed with the Windows NT Event Viewer.
- **Log Server** (the default setting) causes messages to be sent to the Log Server IP address specified on the **Log Files** tab.

Debug Messages. When turned on, writes debug messages to the log file.

Note

This option is very resource intensive if you debug messages in IMAP4.

Default Mail Host. The name of the host to send mail to if only a user ID is specified in the mail message and that user ID is not found on the local system. Normally this field should be blank. This field can be useful when multiple systems are required to work as one system.

Domain Name Server address. The IP address of the system that provides domain name service for your network. You can enter multiple name servers here, separated by a space. This setting is required in order to send mail externally.

Tries before returning to sender. Defines the number of times that delivery is attempted before giving up and returning the mail to the sender. Each time the **Queue Timer** reaches 0, a delivery attempt is made. Thus, if the **Queue Timer** is set to 30 (minutes) and you want to attempt delivery for up to 3 days, this field should contain 144. The default value of 20 with the default **Queue Timer** value of 30 will cause the message to be returned after about 10 hours.

Queue Timer. How often, in minutes, the SMTP server will check the outbound queue for queued mail. (See also the **Tries before returning to sender** option.)

Server Status. A status message to the left of the **Start/Stop Service** button shows whether or not the service is running.

Start/Stop Service. This button toggles between Start service and Stop service depending on whether the service is running.

Using a Remote Mail Gateway

You can use the Gateway Options to configure your mail server to use a remote mail gateway.

Remote Mail Gateway Host. The name of another host to send mail to for further delivery when that mail cannot be delivered directly to the destination host. This can be used in conjunction with the **Send all remote mail through gateway** option to force delivery of mail through the gateway host. Since IMail Server should be able to reach all hosts directly, this field should typically be left blank.

Send all remote mail through gateway. Causes IMail Server to send all mail to the **Remote Mail Gateway Host**, which will forward it on to the addressee's mail host. If this option is not selected, IMail Server will send mail directly to the addressee's mail host.

Tries before sending to gateway. The number of times that delivery directly to a remote host should be attempted before giving up and delivering to the gateway host. Proper function of this value is dependent on the validity of the **Remote Mail Gateway Host** name and the **Send all remote mail through gateway** option.

Advanced Options

Several Advanced options that were previously available only through the registry, have been added to the IMail Server interface on the SMTP Advanced tab. The default settings on the Advanced tab should be appropriate for most installations. However, if you need to change these settings, be aware that they can change the operation of the server.

Maximum recipients per message. The maximum number of addresses that can receive a single message. The default setting for this option is 0.

Delay between recipients. Sets a delay (in milliseconds) between the delivery of messages to recipients. The default setting for this option is 0.

Port. The port that the SMTP service listens on. The default port number is 25.

Maximum Processes. This is the number of simultaneous SMTP processes that IMail Server spawns. By default this option is set to 30. If you see heavy mail traffic or run several large list server mailing

lists, you may want to increase this number.

Note

If you set this value too high, it can cause your server to malfunction.

Mailbox delimiter. Enter the character that will be used to delimit the mailbox name in a user ID. If nothing is entered here, the default delimiter of - (dash) will be used.

Note

Before changing the mailbox delimiter, you should first check for existing usernames and aliases that contain the new delimiter character. Otherwise, these aliases or usernames will contain delimiters, which will cause their incoming mail to be undeliverable or delivered to another user whose username matches the portion of the address preceding the new delimiter.

Host delimiters. Enter the character or characters that you want to use to delimit the host name. Each character will be seen by IMail Server as equivalent to the @ in e-mail addresses. By default the characters used are: @ % * : $ and &. Any of these can be used between the user ID and the virtual host name in the POP3 or IMAP4 login user ID. To change these characters, enter the string of characters in the Host Delimiters textbox.

Note

The @ character is required by Web Messaging.

Delivery Application. If you wish to replace the delivery application with an external program, enter the full pathname of the file in this textbox.

Hello Message. You can use this box to change the text of the SMTP service welcome message. The text is limited to 400 characters or less. If over 400 characters are entered, the default message is used.

SMTP Security

For information on setting the SMTP Security tab and other security functions see **Chapter 9: Security and Antispamming.**

Chapter 9: Security and Antispamming

This chapter describes how you can secure your mail server against unwanted use. The SMTP server processes all incoming and outgoing messages. Due to the openness of the SMTP (Simple Mail Transport Protocol) and Internet protocols, it is difficult to block unwanted mail and at the same time keep your mail server available to your users and to other Internet mail users. Nonetheless, there are techniques you can use to secure your server.

Most of the security options discussed in this chapter can be found on the **SMTP Security** tab.

See “Chapter 8: SMTP Server” on page 147 for information about configuring the SMTP server.

Background on SMTP Protocol Security

If you are unfamiliar with “spamming” and “spoofing,” the following paragraphs provide some background.

The SMTP standard for Internet messaging allows electronic mail to make its way across a network in “hops” by passing from one computer system to another, repeating this process until the mail arrives at its final destination. This is part of the original design of SMTP and was necessary in the early days of the Internet in order for e-mail to travel between various networks. In the current Internet this is not necessary and mail usually is delivered directly from the sending host to the receiving host. Exceptions to this include application gateways that are used to bridge firewalls.

This inherent design of SMTP allows a host computer that needs to deliver a message to another computer (or even hundreds or thousands of recipients) to make a connection (or multiple connections) to some other SMTP server and ask that server to relay the message(s) on its behalf.

Recently there has been a lot of controversy over unwanted e-mail. Many companies and ISPs have been blocking the receipt of this mail from known sources, as it is possible to deny access to a sending machine by using a firewall or some other method. Once a bulk mailer’s home mail server is known and blocked, senders of bulk

e-mail — taking advantage of SMTP's open design — may attempt to deliver their mail through someone else's computer by asking the other computer to route that mail for them.

Senders of unsolicited e-mail can also use this method to try to hide their real identity by manipulating the headers in the message in a certain way and then sending the message through your system for delivery to its final destination — making it appear as if the message originated from the relaying server. This is known as "spoofing." (IMail Server, however, will always include the IP address of the source in the message headers.)

When a bulk mailer chooses your computer to deliver unsolicited mail to thousands of other people (known as "spamming"), your system immediately becomes busy delivering messages that didn't originate with your users, tying up your valuable system resources.

IMail Server offers several ways to protect your server against such abuse. The following sections describe these security options.

Security Strategies

This section provides an overview of the options you can use to protect your system against "spamming" and "spoofing" and other types of abuse. See the following sections for a description of all the options and the procedures that describe how to implement them.

Mail Relay Options

IMail Server (or *any* SMTP server) accepts mail destined for another host and redelivers it to that host — this is the mail relay function.

A message that originates on a computer other than the IMail Server host and destined for another host must pass through the IMail Server (i.e., IMail Server must relay the message). If your mail users use a POP3 or IMAP mail client to send mail, then IMail Server needs to relay mail for them.

Local mail is processed without requiring relay. That is, a message destined for the IMail Server host or a message originating from the IMail Server host does not use the relay function. Thus, if all of your mail users send and receive mail from the same host that IMail Server is on, or if they all use Web Messaging to access mail, you can select the **No Mail Relay** option.

If you are concerned about bulk mailers using the relay function to send mail through your server, you can restrict the addresses for which IMail Server relays mail by using the following options.

- Use the **Relay mail for** option and specify the IP address or range of addresses that you want to give access to your mail server. You need to include the IP addresses for all of your users, because when they send a mail message, the message is relayed through the SMTP server to its destination.
- Use the **Relay mail for local hosts only** option to limit relay access to mail hosts on your IMail Server and the **Relay mail for local users only** option to limit relay access to users on those hosts.
- When you use one of the "Relay for" options, you may have users who need to send mail from an IP address not listed. You can do this with IMail Server's support for the **SMTP AUTH** command. Make sure the remote user selects the "user authorization" option in their mail client. (Note that this feature will be named differently on different clients.) SMTP AUTH authenticates the user ID and password of a user sending mail. This is handled transparently by the mail server and client.

For information about setting up relay options, see "Setting Mail Relay Options" on page 157.

Validating Incoming Mail

There are a number of ways that you can check the header and body information of incoming mail to try to filter out unwanted messages.

- Enter known spam mail addresses or a domain name (for example, @domain.com) in the **Kill file**.
- Use delivery rules to search incoming mail for specific information in the header or body of a message. For example, you can search a header or body for "$$$ GET RICH QUICK" and if found, route the mail to a particular mailbox for the user. Delivery rules support powerful search expressions. You can combine rules with the Info Manager to route spam mail to an administrator's mailbox so that the user never receives it.

  For information on using delivery rules, see Chapter 4, "User Mail Accounts."

- Select the option to **Disable SMTP "VRFY" command**. The SMTP VRFY command is used to verify a user ID on a host and as such can be used to test for valid user IDs. Disabling the command helps prevent "spoofing" by not allowing someone outside your network to check if a user ID is valid. If you select this option, when IMail Server receives an SMTP VRFY request, it will return the message: `252 Cannot VRFY user`
- Select one of the options that attempts to identify improper use or the mail header:

  Auto deny possible hack attempts
  Refuse NULL <> Senders
  Check valid sender

For information about setting these options, see "Validating Incoming Mail" on page 162.

Access Control Options

If there is a known IP address from which you want to block all mail, use the **Control Access** feature to deny that address access to your server. For information about setting access, see "Setting Access to the SMTP Server" on page 163.

Changing the SMTP Welcome Message

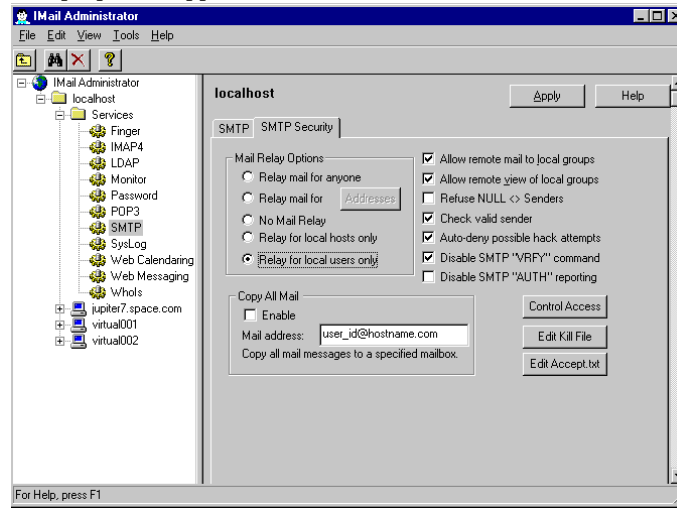
When you log on to SMTP, the service responds with a "welcome message" that identifies the mail server version, vendor and operating system. You can change the welcome message to hide this information. Changing the message may help protect your server from spammer or hacker attacks. For more information see "Advanced Options" on page 151..

Setting SMTP Security Options

You can set who has access to your mail server and control SMTP security in several ways. This section describes how to use the SMTP Security options to prevent unwanted access and unwanted mail. See "Security Strategies" on page 154 in this chapter for information about when to use different security options.

To set any of the options for the SMTP server:

1 Click the **SMTP Security** tab. The SMTP Security properties appear.



2 Select any of the options (described in the following sections) you want to use to set security for the SMTP server.

3 Click **Apply** to save your changes. Click **OK** to save your changes and exit the dialog box.

Note

If you make changes to the IP addresses that can use the SMTP server, you must stop and restart the SMTP service for the changes to take effect.

Setting Mail Relay Options

You can use the **Mail Relay Options** to prevent unauthorized mailings, such as mass promotional mailings (known on the Internet as spam mail) from passing through the IMail Server as a relay or gateway. The **Relay mail for** option lets you configure IMail Server to only accept mail that originates from local users or that is destined for local users. You can define the systems or address blocks that you want to consider local.

Some Considerations When Setting Relay Options

Consider the following issues when using the “Relay for” options.

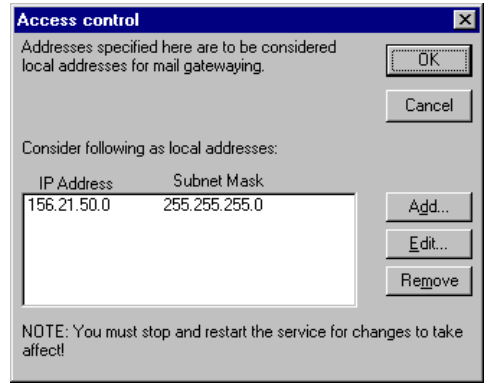
- Note that when one of your mail users sends a mail message, the message is relayed through the IMail Server. So, you must enter the IP addresses or IP address range of all of your mail user’s systems.
- If a user needs to send mail from an unknown IP address, you can have the user select the “user authorization” option in their mail client. When this option is selected, the IMail Server uses the SMTP AUTH command to validate the user’s logon user ID and password.
- If you have IMail Server set up to be a backup server for a remote mail server and you want to restrict relay access to your server, use the **Relay for Addresses** option and specify the address of the host for which IMail Server is a backup server. See “Chapter 3: Configuration” on page 33 and “Appendix B. Backups” on page 257 for more information about setting up a backup server.

Relay mail for anyone. Allows the SMTP server to accept mail destined for other hosts and re-deliver that mail to the proper host (i.e, relay the mail). This is the default setting.

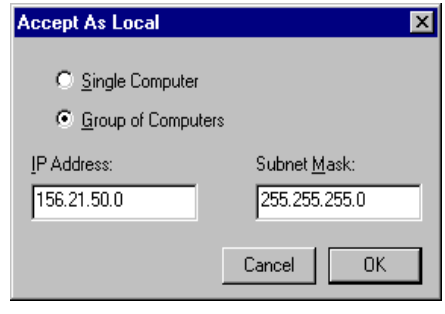
This setting leaves your mail server open to any other SMTP server to use as a mail relay. Some bulk mailers may take advantage of this capability to not only relay mail through your server, but to make it appear as if mail is originating from your server. See “Background on SMTP Protocol Security” on page 153 for more information.

Relay mail for. Allows the SMTP server to accept mail destined for other hosts only if the mail is received from the specified IP addresses (which the mail server will consider to be local addresses).

To specify the valid IP addresses, click the **addresses** button. The “Access Control” dialog box appears.



1 Click the **Add** button. The “Accept as Local” dialog box appears.



2 In the **IP Address** box, enter the IP address of the computer to be considered local to the IMail Server.

To add a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be considered local.

For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This will allow those 254 systems to be considered the same as the local system and they can use the mail server to send mail to the outside world.

3 Click **OK** to add the IP address(es) to the list.

IMail Server will relay mail for all the computers listed.

4 Click **OK** to save the changes. Note that you must stop and restart the service for the changes to take effect.

A “non-local” system that attempts to send mail through the IMail Server system will receive the following message:

```
550 unknown local host %s, not a gateway
```

No Mail Relay. The SMTP server will refuse to accept mail destined for other hosts, unless the user authenticates. If you use this setting, make sure that “Disable SMTP Auth Reporting” is not selected. This will force users to authenticate.

Note

If you are using a client such as Outlook or Eudora, you must select “my server requires authentication”. The wording of this option may vary depending on the client used.

Relay mail for local hosts. Checks the “From” address of incoming mail and determines that it contains a valid IMail Server host name. This must be the name of a host or virtual host, or a valid alias for a host on the IMail Server system. If it is not, the server does not relay the mail. If a host has an alias, you must enter the alias in the *accept.txt* file.

You can use the *accept.txt* file in conjunction with this option to make the IMail Server accept the named remote hosts as “local” hosts.

You cannot use this option if you are using a “store and forward” setup to relay mail for another server.

Relay mail for local users. Checks the “From” address of incoming mail and first determines that it contains a valid IMail Server host name, then checks that host for the user ID. It does not check user aliases; thus, if a user needs to use an alias for their e-mail address, the alias needs to be in *accept.txt*. If the host name or User ID is not valid, the server does not relay mail.

You can use the *accept.txt* file in conjunction with this option to make the IMail Server accept the named remote hosts and users as “local” hosts and users.

You cannot use this option if you are using a “store and forward” setup to relay mail for another server.

Using the accept.txt file. The *accept.txt* file lets you name remote hosts and users that you want the IMail Server to accept as "local" hosts and users. This file can be used with the **Relay for Local Hosts Only** and **Relay for Local Users Only** options.

To create an *accept.txt* file:

1 Using Windows Notepad or another editor, create a file and name it *accept.txt*.

2 Enter one IP address or host name per line. Do not use spaces or punctuation.

For example, to enter hosts:

```
mail1.widget.com
mail5.foo.com
```

For example, to enter users:

```
fred@mail1.widget.com
bob@mail5.foo.com
```

The *accept.txt* file must have an exact match for the respective host or e-mail address. It does not accept wild cards or partial matches.

3 Save the *accept.txt* file in the location: [IMail Top Directory]\accept.txt

Setting Access to Local Mail Groups

You can use the following options to set access to local mail groups (aliases of type Group) on your mail server. (These options do not affect list-server mailing lists, standard aliases, or program aliases.)

Allow remote mail to local groups. When selected, the SMTP server accepts mail addressed to a group that has been defined using the IMail Client application. The SMTP server re-sends the message to users in the group.

Allow remote view of local groups. When selected, the SMTP server allows a remote host to execute an SMTP "EXPN" command to show all users in a group that has been defined using IMail Client.

Note

The settings described above do not affect mail to list-server mailing lists. Aliases of type Group are affected. You must have the "Allow remote mail to local groups" option enabled for a Group alias to work

Validating Incoming Mail

You can use the following options to check that incoming mail was sent from a valid user mail account or to deny access to specified mail addresses. IMail Server will always include the IP address of the source of a message in the message header.

Refuse NULL <> Senders. If enabled, IMail Server refuses to accept mail if there is no address specified in the MAIL FROM line of an incoming message (the null address (<>) is used). Allowing no address in the MAIL FROM line makes it easier for spam mailers to send bulk mail to your users. However, note that RFC 822 requires that mail servers accept mail that has no address in the FROM line.

Note that Microsoft Exchange uses the null address for messages from the postmaster, so selecting this option disables the ability of IMail Server users to receive mail from Exchange postmasters.

Check valid sender. If enabled, IMail Server requires that the user mail address `(user@host)` is specified in the MAIL FROM or REPLY-TO line of an incoming mail message. Note that a null address (< >) in the MAIL FROM line is handled separately by enabling or disabling the **Refuse NULL < > Senders** option.

Auto-deny possible hack attempts. If more than 512 characters are sent during anything but the SMTP DATA command, the remote IP address is temporarily put in the “deny access” (Control Access) file until you stop and restart the service and then disconnects. Sending more than 512 characters in anything but the SMTP DATA command will look like an attempt to “hack” in to your server. You will not see the address in the “deny access” list, but it is reported in the log file.

Disable SMTP ‘VRFY’ command. The SMTP VRFY command is used to verify a user ID on a host — as such it can be used from a remote host to test for valid user IDs. If you select this option, when IMail Server receives an SMTP VRFY request, it returns the message:

```
252 Cannot VRFY user
```

Note

Do not select the **Disable SMTP VRFY command** when using “peer” IMail Servers. A peer server needs to use this command to verify a user that is on the other peer. See “Setting Up “Peer” IMail Servers” on page 51 for more information.

Edit kill file. The kill file lets you specify a mail address or a particular mail host that you do not want to accept mail from. To specify a mail address or host in the kill file, click the **Edit kill file** button.

The file *kill.lst* appears in the Windows Notepad. In the *kill.lst* file, enter one entry per line in either of the following formats:

```
userid@host
@host
```

For example, to deny access from a user mail account, you could enter: `fred@widget.com` To deny access to all users from the mail host widget.com, you can enter: `@widget.com`.

IMail Server checks the incoming message's `MAIL FROM: <user@host>` line. When it receives mail from an address listed in the kill file, IMail Server returns the message:

```
501 unacceptable mail address
```

The *kill.lst* resides in the *IMail* directory and applies to the primary host and all virtual hosts.

Setting Access to the SMTP Server

You can specify an IP address or set of IP addresses that are either granted access to the SMTP server or denied access. Systems that do not have access to the SMTP server system will not be allowed to connect. This is useful when you know the IP address(es) of a mail sender that is unauthorized to use your mail server.

Note that, in most cases, you would not use this option to specify the addresses that you want to grant access, because you don't know every host on the Internet that wants to send mail to your users.

To deny access to a specific computer or group of computers:

1 Click **Control access**. The Access Control dialog box appears.

2 Select the **Granted Access** option.

3 Click the **Add** button. The Deny Access On dialog box is displayed.

4 In the **IP Address** box, enter the IP address of the computer to be denied access to the SMTP server.

To deny access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This denies access to those 254 systems.

5 Click **OK** to add the IP address(es) to the list.

Access will be granted to all computers except those listed.

6 Click **OK** to save the changes. Note that you must stop and restart the service for the changes to take affect.

To grant access to a specific computer or group of computers:

1 Click **Control access**. The Access Control dialog box appears.

2 Select the **Denied Access** option.

3 Click the **Add** button. The Grant Access On dialog box appears.

4 In the **IP Address** box, enter the IP address of the computer to be granted access to the SMTP server.

To grant access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This grants access to those 254 systems.

1 Click **OK** to add the IP address(es) to the list. Access is denied to all computers except those listed.

2 Click **OK** to save the changes. Note that you must stop and restart the service for the changes to take effect.

Copying Inbound and Outbound Mail

On the **SMTP Security** tab, you can set an option to send a copy of every inbound and outbound message to a specified mailbox.

1 In the **Copy All Mail** options, in the **Mail address** box, enter the full e-mail address to send a copy of each message to.

2 Turn on the **Enable** option to enable copying of all mail.

If you want to turn off the **Copy All Mail** feature, make sure the **Enable** option is *turned off*.

3 Click **Apply** to save your changes.

Chapter 10: POP3 Server

The POP3 Server lets any POP3 (Post Office Protocol, Version 3) mail client communicate with IMail Server. Supported POP3 clients include Internet Explorer, Netscape Messenger or Communicator, Eudora, Pegasus, NuPOP, Z-Mail, and UNIX mail.

POP3 clients typically use the "off-line" method of accessing the mail server: the mail client periodically connects to the server, downloads the messages to the client computer, and then disconnects from the server. Thus, mail messages are stored only temporarily on the server computer; they are automatically deleted from the server computer when downloaded to the client computer. This method is best suited to users who always read their mail from the same client computer.

In the "online" access methods, an open connection is maintained between the client and the server. Messages are left on the mail server computer and users can read mail on the server without downloading. This allows users to access mail from mail clients on different computers, for example, from a laptop on the road.

As a Windows NT service, the POP3 service can run completely hidden or with some feedback. The POP3 server will continue to run when you log off the Windows NT computer.

See RFC 1939 for a description of the POP3 protocol.

IMail Server also offers mail client access via the IMAP4 (Internet Message Access Protocol Version 4). The IMAP4 server provides both "online" and "off-line" methods of access. For more information on the IMAP4 server, see "Chapter 11: IMAP4 Server" on page 177.

Logging On

By default, the POP3 service logs on to the System Account. You can view and change the way the service logs on:

1 In the Control Panel, start the **Services** applet.

2 Select the **IMail POP3 Server** service and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.

Allow Service to Interact with Desktop. Select this to provide a desktop icon that can be used by whoever is logged in when the service is started. For more information, see your Windows NT documentation.

This Account. Select this only if *none* of your hosts uses the Windows NT database; then enter the name of the appropriate user account; make sure the user is a Host Administrator.

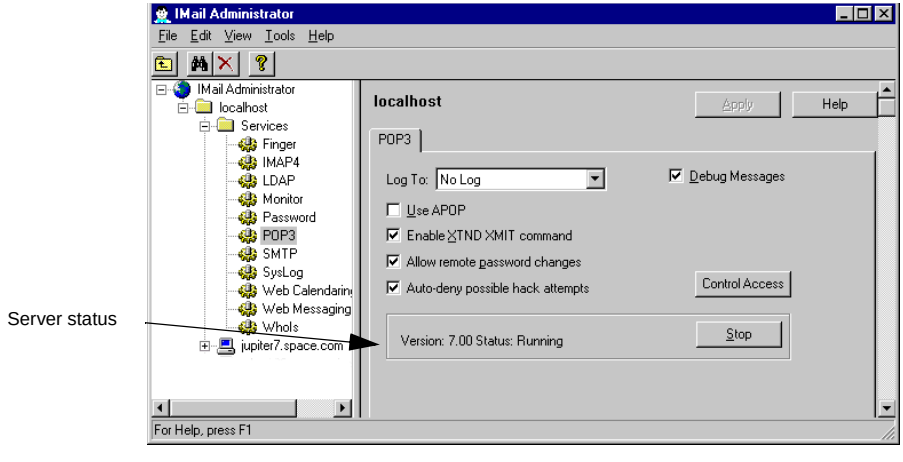
If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Configuring the POP3 Server

To configure the POP3 server:

1 In IMail Administrator, select "**localhost**" in the left panel.

2 Select the "**Services**" folder and click on **POP3**. The POP3 tab appears .



Server status

3 Enter the options you want to use to configure the POP3 server.

Each option is described below.

4 Click **Apply** to save your changes.

5 After making changes, stop the service, wait 5-10 seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

Logging Options

In the **Log To** box, select the way you want to log POP3 events:

- **sysMMDD.TXT**. This sends event information to a file of this name where *MM* is the month and *DD* is the day the log was written. This file is stored in the *Spool* directory.
- **No Log**. Select this to turn off the logging of events.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer.)
- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab.

Other Options

Debug Messages. When selected, debug messages are written to the log file. This option is very resource intensive if you debug messages in IMAP4.

APOP. Turn this on for secure user authorization (password encryption). For more information, see RFC 1939.

Note

APOP only works using the IMail Server database; **APOP** does not work with an NT database.

Enable XTND XMIT command. When selected, the server accepts outbound mail sent via XTND XMIT. (Clients such as WinQVT/Net require this functionality.)

Allow remote password changes. Certain older mail clients have the ability to use the POP3 protocol to change passwords remotely. This check box is provided for system administrators whose end-users may be using those older applications. (These applications include older version of Eudora)

Auto-deny possible hack attempts. When selected, if more than 512 characters are sent during anything but the SMTP DATA command, the remote IP address is temporarily put in the “deny access” (Control Access) file until you stop and restart the service and then

disconnects. Sending more than 512 characters in a command other than the SMTP DATA command would look like an attempt to “hack” into your server. You will not see the address in the “deny access” list, but it is reported in the log file.

Server Status. A status message shows whether or not the service is running.

Start/Stop Service. This button toggles between **Start** and **Stop** depending on whether the service is running.

Advanced Options

When logging on to POP3, the service returns a welcome message that identifies the mail server version, vendor and operating system. Changing the message may help protect your server from spammer or hacker attacks. Previously, this setting was available only through the registry, but now you can edit it directly from IMail Administrator. You can use the POP3 Advanced tab to change the service welcome message, if for example, you wanted to hide the mail server version and vendor information.

To change the Welcome Message for POP3:

Enter the text you want to be displayed in the POP3 service welcome message. The text is limited to 400 characters. If over 400 characters are entered, the default message is used. When APOP is enabled, if the message plus the timestamp exceed 400 characters, the message will be truncated.

Setting Access to the POP3 Server

You can specify an IP address or set of IP addresses that are either granted access to the POP3 server or denied access. Computers that do not have access to the POP3 server computer will not be allowed to create a connection.

To deny access to a specific computer or group of computers:

1 Click the **Control access** button. The “Access Control” dialog box appears.

2 Select the **Granted Access** option.

3 Click the **Add** button. The “Deny Access On” dialog box is displayed.

4 In the **IP Address box**, enter the IP address of the computer to be denied access to the POP3 server.

   To deny access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This will deny access to those 254 computers.

5 Click **OK** to add the IP address(es) to the list.

   Access will be granted to all computers except those listed.

6 Click **Apply** to save the changes. Note that you must stop and restart the service for the changes to take affect.

To grant access to a specific computer or group of computers:

1 Click the **Control access** button. The “Access Control” dialog box appears.

2 Select the **Denied Access** option.

3 Click the **Add** button. The “Grant Access On” dialog box appears.

4 In the **IP Address** box, enter the IP address of the computer to be granted access to the POP3 server.

   To grant access to a group of computers, select the **Group of Computers** option. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be granted access. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This grants access to those 254 computers.

5 Click **OK** to add the IP address(es) to the list.

   Access will be denied to all computers except those listed.

6 Click **Apply** to save the changes. Note that you must stop and restart the service for the changes to take effect.

.

Chapter 12: LDAP Server

LDAP uses a client/server architecture to publish user information (called “attributes”) on the server and provide access to that information from LDAP-enabled clients.

By creating a standard way for applications to request and manage directory information, LDAP (or Lightweight Directory Access Protocol) has become another popular feature for standards-based mail servers. LDAP is simplified subset of the much more elaborate X.500 Directory Access Protocol.

As a Windows NT service, the LDAP service can run completely hidden or with some feedback. The LDAP server continues to run when you log off the Windows NT system.

For more information about LDAP, see the Internet Requests for Comments (RFCs) that describe the protocol. The IMail Server implementation of LDAP is based on RFC-2251.

The IMail Server LDAP Implementation

IMail Server provides an LDAP interface to the IMail user database. The IMail user database is extended to include standard LDAP attributes (such as name, address, organization name, phone number) and any other attributes that a site defines. The user database is flat; it does not support a tree hierarchy of users.

Each user with an account on the IMail Server system has an LDAP entry. When a user is added to the IMail user database, an LDAP entry is defined with the following attributes:

ObjectClass	The type of entry. The value would be “Person.”
CN CommonName	The full name of the user.
Mail	The IMail Server e-mail address for the user. This is constructed from the user ID and the host name.
UID	The IMail Server user ID.

Using an LDAP-enabled client, the user can add, delete, and modify information in his/her own LDAP entry. A user cannot modify another user's entry. The following table describes several additional attributes that the user can add (by using an LDAP client that supports the Modify function):

SurName	The surname, or last name, of the user.
Organization	The company that the user works for.
OrgUnit	The department within the company that the user works for.
Street	The street address of the user.
City	The city in which the user is located.
ST	The state or province in which the user is located.
Postal	The ZIP or postal code of the user.
C	The country name of the user.
Telephone	The telephone number of the user.

These are the most common attributes used in the LDAP entry. Other attributes can be defined by the system administrator or the user.

The system administrator can add and delete users, add LDAP attributes, and modify LDAP attribute values using:

- IMail Administrator — For more information, see "Chapter 4: User Mail Accounts" on page 59.
- A web browser. For more information, see "Chapter 6: IMail Web Messaging" on page 107 and "Using the Web Administration Capability" on page 210.

Note

You can also use an LDAP-enabled client to add and modify LDAP attributes (but not to add and delete users). Refer to the documentation for your client for information on accessing and using an LDAP directory.

Full LDAP Directory Support

IMail Server supports LDAP version 3, which provides the following capabilities:

- Allows users of LDAP-enabled clients such as Netscape Communicator to:
  - Locate LDAP directory information that may include name, phone number, e-mail address, organization, department, and address.
  - List all users on a host.
  - Search for users who meet certain criteria.
  - Modify their own user information in the LDAP directory.
- Host Administrators and System Administrators can use an LDAP-enabled client to add, delete, and modify user accounts, including any LDAP directory information.
- You can monitor the LDAP server and receive notification when it goes down. For more information, see “Chapter 16: The Monitor Server” on page 195.

Supplying LDAP Information for Unregistered Users

You cannot add users to the LDAP database unless they have mail accounts. If you want to provide LDAP information about users whom you don’t want to use e-mail, you must create accounts for them and select **Account Access Disabled** in their User Properties.

Accessing LDAP Information from Microsoft Mail Clients

If a user has Outlook Express as a mail client, and has difficulty accessing LDAP information from the IMail LDAP server, the user can change a setting in Outlook Express to remedy the situation.

If the user does not have an entry for the IMail LDAP server, the user will need to create one as follows:

1 In Outlook Express, select **Accounts** --> **Directory Service** --> **Add** --> **Directory Service** from the **Tools** menu.

2 In the Internet directory (LDAP) server box, enter the name or IP address of the IMail Server system, then fill in the other panels.

3 Click **Finish** when done.

Once the user has created an LDAP entry as described above, the user must edit the LDAP properties:

1 In Outlook Express, select **Accounts** -> **Directory Service**.

2 Select the LDAP account.

3 Select **Properties**, then click the **Advanced** tab.

4 In the **Search Base** text box, enter:

```
objectclass=Person.
```

5 Click **Apply**, then **OK**, then **Close**.

Populating the LDAP Database

If you add a large number of users at one time, you may want to populate the LDAP database afterward. For more information, see "Populating the LDAP Database (ldaper.exe)" on page 268.

Logging On

By default, the LDAP service logs on to the System Account. You can view and change LDAP settings using the **Services** applet in the Windows NT/2000 Control Panel.

To view and/or change settings for the LDAP service:

1 In the Control Panel, start the **Services** applet.

2 Select **IMail LDAP Server** and click **Startup**.

3 Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.

Allow Service to Interact with Desktop. This displays a desktop icon for use by users who are logged in upon service start up. For more information, see the Windows NT/2000 documentation.

This Account. Select this only if *none* of your hosts uses the Windows NT database; then enter the name of the appropriate user account; make sure the user is a Host Administrator.

Note

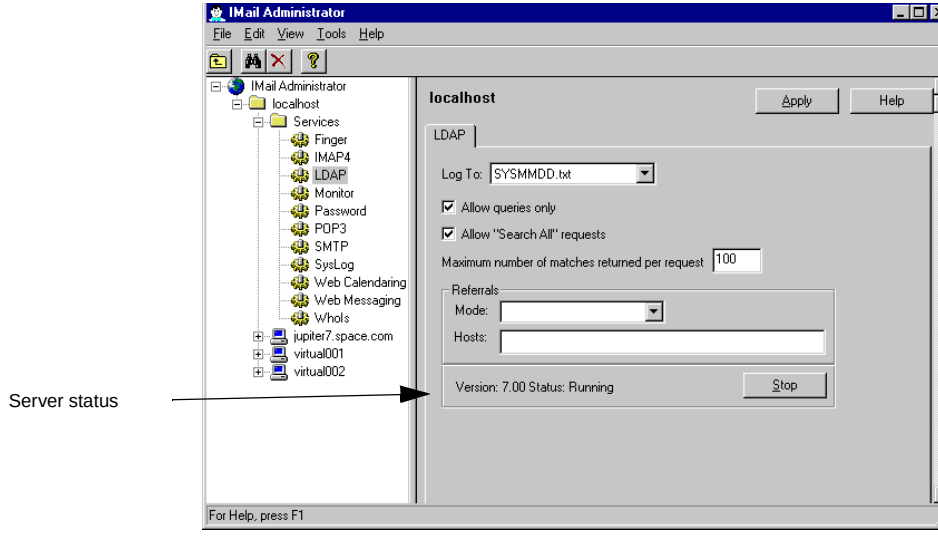
If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Configuring the LDAP Server

To configure the LDAP server:

1 In IMail Administrator, select "**localhost**" in the left panel.

2 Select the "**Services**" folder, and click on **LDAP**. The LDAP tab appears.



3 Enter the options you want to use to configure the LDAP server.

Each option is described at the end of this procedure.

4 Click **Apply** to save your changes.

5 After making changes, stop the service, wait 5-10 seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

Logging Options

In the **Log To** box, select the way you want to log LDAP events:

- **sysMMDD.TXT**. This sends event information to a file of this name where *mm* is the month and *dd* is the day the log was written. This file is stored in the *Spool* directory.
- **No Log**. Select this to turn off the logging of events.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer.)
- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab, and to the Spool directory.

Allow queries only. When enabled, an LDAP client can query the server for LDAP information and read the results, but cannot enter or modify LDAP information.

Allow "Search All" requests. You can disable this to force LDAP clients to be more selective in their search criteria.

Maximum number of matches returned per request. Set this to a low number to limit the server load generated by LDAP requests.

Referrals. Set up a referral to another LDAP database. This feature lets the LDAP server notify an LDAP client where to look for additional information (on another LDAP server). To set up a referral, set the following options:

Mode. This determines what a query from an LDAP client will return:

- **Send data only** returns data from the IMail LDAP server only and does not do a referral.
- **Send referral only** returns the host name (entered in Hosts) of another LDAP server.
- **Send both** returns data from the IMail LDAP server and a referral to another LDAP server (entered in Hosts).

Hosts. Enter the host name of the remote LDAP server. You can enter multiple host names, separated by a comma.

Server Status. A status message to the left of the **Start/Stop** button shows the version number, and whether or not the service is running.

Start/Stop Service. This button toggles between **Start** and **Stop** depending on whether or not the service is running.

Chapter 11: IMAP4 Server

With more and more users finding they need access to their mail from multiple computers, IMAP4 (Internet Message Access Protocol, Version 4) is rapidly becoming a mandatory feature for Internet-standards-based mail servers.

By incorporating IMAP4, IMail Server provides mail users with the added flexibility of being able to access and manipulate their mail folders — anytime, anywhere. Now, whether in the office, at home, or on the road, mail users can refer to messages in all of their folders regardless of when or where they were originally read or saved. This translates to increased efficiency for those working from a "virtual office."

The IMail Server IMAP4 Implementation

The IMAP4 Server lets any IMAP4 mail client communicate with IMail Server. Supported IMAP4 clients include Netscape Communicator and Internet Explorer 4.0 and above. Many mail client vendors are adding IMAP4 support.

As a Windows NT service, the IMAP4 service can run completely hidden or with some feedback. The IMAP4 server continues to run when you log off the Windows NT system.

IMAP4 Server Support

IMAP4 handles mail access only, and relies on SMTP for sending and receiving mail over the Internet. The IMAP4 server allows an IMAP4 client to do the following:

- Access remote mailboxes as if they were local
- Read mail from more than one computer because mail is stored on the server system
- Access mail offline or online. Offline/online access behavior is determined by the mail client that is used.

  Offline access means that the mail client connects to the IMAP4 server, downloads the message headers, then disconnects.

- If the user reads a message that has *not* been previously downloaded, the mail client re-establishes the connection and downloads the message.
- If the user chooses to read a message that *has* previously been downloaded, the mail client shows a local copy.

Online operation is the same as offline, except that an open connection is maintained between the client and the server.

The mail client may support switching between IMAP4 and POP3 methods, both of which are supported by IMail Server.

Full IMAP4 Client Support

The IMAP4 client can access remote message stores (on the mail server) as if they were local. Users can:

- View message headers before downloading
- Select a message or part of a message for downloading
- Leave messages on the server for archiving and sharing
- Send and receive MIME-based attachments
- Manipulate remote mailboxes other than the MAIN (or INBOX) mailbox

Mailbox Management

When a user creates a mailbox using an IMAP4 client, the mailbox is created on the IMail Server system. Because the IMail server will permanently store IMAP4 users' mail, you will want to configure the server with appropriate disk space and you will want to manage the disk space by monitoring mailbox disk usage. As a general rule, a user should have four times the amount of free disk space as their entire users directory takes up.

With IMAP4 user accounts, the system administrator can:

- View, delete, or rename the mailbox directories;
- Set maximum mailbox size and maximum number of messages for each user or globally
- Delete old messages by specifying a date or number of days for which messages older than the date will be deleted.

For information on maintaining user mailboxes, see "Working with User Mail Accounts" on page 60.

Administrators can also set an option that determines whether users must subscribe to a private mailbox before they can read it. For more information, see “Configuring the IMAP4 Server” on page 180.

Public Mailboxes

The IMAP4 server provides a means of creating a *public* mailbox in which you can post messages for reading by IMAP4 clients. To create a public mailbox, create a user ID named *public*. Any mailboxes in the *public* directory will be available for reading by IMAP4 clients.

Administrators can use the *public* user ID to post messages. Users other than *public* can only read the public mailboxes. Administrators can set an option that determines whether users must subscribe to a *public* mailbox before they can read it.

Public mailboxes are read-only by design, and only the user *public* can administer the public mailboxes. Messages received for this account and its sub-mailboxes are treated as normal, but users other than *public* who access these mailboxes through IMAP4 have read-only permissions. If a user tries to mark a message in a public folder as read, he will be notified that the mailbox is read-only.

Logging On

By default, the IMAP4 service logs on to the System Account. You can view and change IMAP4 settings by using the **Services** applet in the Control Panel.

To view and/or change settings for the IMAP4 service:

1 In the Control Panel, double-click the **Services** applet.

2 Select **IMail IMAP4 Server** and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.

Allow Service to Interact with Desktop. Select this to provide a desktop icon that can be used by whoever is logged in when the service is started. See your Windows NT for more information.

This Account. Select this only if *none* of your hosts uses the Windows NT database; then enter the name of the appropriate user account; make sure the user is a Host Administrator.

Note

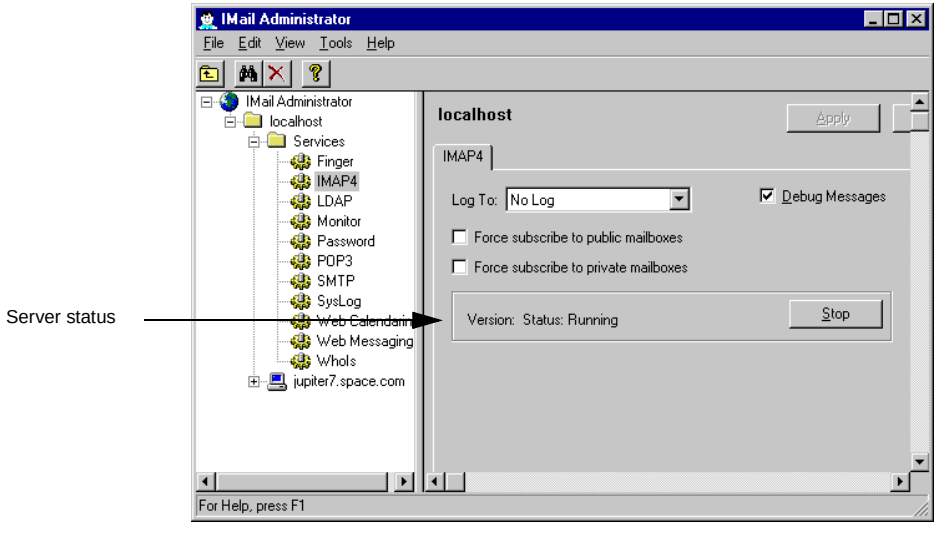
If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Configuring the IMAP4 Server

To configure the IMAP4 server:

1 In IMail Administrator, select "**localhost**" in the left panel.

2 Select the "**Services**" folder and click on **IMAP4**. The IMAP4 tab appears.



3 Enter the options you want to use to configure the IMAP4 server.

Each option is described at the end of this procedure.

4 Click **Apply** to save your changes.

5 After making changes, stop the service, wait five to ten seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

Logging Options

In the **Log To** box, select the way you want to log IMAP4 events:

- **sysMMDD.TXT**. This sends event information to a file of this name where *mm* is the month and *dd* is the day the log was written. This file is stored in the *Spool* directory.
- **No Log**. Select this to turn off the logging of events.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer.)
- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab.

Debug Messages. Turn this on to write debug messages to the log file.

Force subscribe to public mailboxes. Turn this on to require that the IMAP4 client is subscribed to use a public mailbox. If the user is not a subscriber, he is refused access. Note that subscribing to a mailbox is a protocol command; there is no way for a user to subscribe to a mailbox unless the client application provides this capability.

Force subscribe to private mailboxes. Turn this on to require that the IMAP4 client is subscribed to use a private mailbox. If the user is not a subscriber, he is refused access. Note that subscribing to a mailbox is a protocol command; there is no way for a user to subscribe to a mailbox unless the client application provides this capability.

Server Status. A status message to the left of the **Start/Stop** button shows the version number, and whether or not the service is running.

Start/Stop Service. This button toggles between **Start** and **Stop** depending on whether or not the service is running.

Advanced Options

When logging on to IMAP4, the service returns a welcome message that identifies the mail server version, vendor and operating system. Changing the message may help protect your server from spammer or hacker attacks. Previously, this setting was available only through the registry, but now you can edit it directly from IMail Administrator. You can use the IMAP Advanced tab to change the service welcome message, if for example, you wanted to hide the mail server version and vendor information.

To change the Welcome Message for IMAP 4:

Enter the text you want to be displayed in the IMAP4 service welcome message. The text is limited to 400 characters. If over 400 characters are entered, the default message is used. When APOP is enabled, if the message plus the timestamp exceed 400 characters, the message will be truncated.

Chapter 13: Whois Server

The Whois server lets a Whois client look up information about IMail Server users. Whois information can include the user's full name, mailing address, telephone number, and a network mailbox. When the Whois server receives a lookup request about a particular user, it will send the information about the user that it finds in the IMail database.

As a Windows NT service, the Whois service can run completely hidden or with some feedback. The Whois server continues to run when you log off the Windows NT system.

Logging On

By default, the Whois service logs on to the System Account.

To view and/or change settings for the Whois service:

1 In the Control Panel, start the **Services** applet.

2 Select **IMail WHOIS Server** and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.

Allow Service to Interact with Desktop. Select this to provide a desktop icon that can be used by whoever is logged in when the service is started. For more information, see your Windows NT documentation.

This Account. Select this only if *none* of your hosts uses the Windows NT database; then enter the name of the appropriate user account; make sure the user is a Host Administrator.

Note

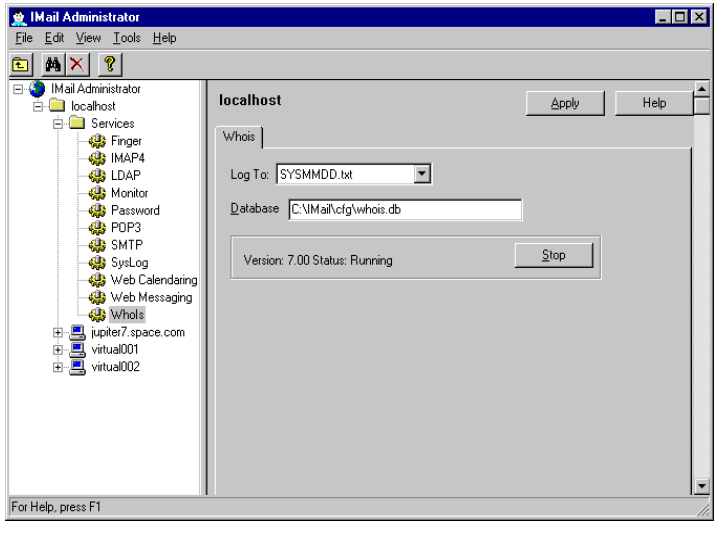
If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Configuring the Whois Server

To configure the Whois server:

1 In IMail Administrator, select "**localhost**" in the left panel.

2 Select the "**Services**" folder and then click **Whois**. The Whois tab appears.



3 Enter the options you want to use to configure the Whois server.

Each option is described at the end of this procedure.

4 Click **Apply** to save your changes.

5 After making changes, stop the service, wait 5-10 seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

Logging Options

In the **Log To** box, select the way you want to log Whois events:

- **sysMMDD.TXT**. This sends event information to a file of this name where *mm* is the month and *dd* is the day the log was written. This file is stored in the *Spool* directory.
- **No Log**. Select this to turn off the logging of events.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer.)

- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab.

Database. The full path name of the Whois database file.

Server Status. A status message to the left of the **Start/Stop** button shows the version number of the Whois server and whether or not the service is running.

Start/Stop Service. This button toggles between **Start** and **Stop** depending on whether or not the service is running.

Chapter 14: Finger Server

In response to Finger requests from other hosts, the Finger server returns the full name of the specified user, his or her complete e-mail address, and the contents of the Plan file (if one exists). For more information on the Finger protocol, see “Setting Up a Finger Plan” on page 69.

If an alias is specified in a Finger request from another host, the Finger server returns the expansion of that alias.

In response to Finger requests that do not specify a user, the Finger server reports that it will not display the current logged in user. To do otherwise is considered by many to be a security breach.

As a Windows NT service, the Finger service can run completely hidden or with some feedback. The Finger server continues to run when you log off the Windows NT system.

Logging On

By default, the Finger service logs on to the System Account. You can view and change Finger settings by using the **Services** applet in the Control Panel.

To view and/or change settings for the Finger service:

1 In the Control Panel, select the **Services** applet.

2 Select **IMail FINGER Server** and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.

Allow Service to Interact with Desktop. Select this to provide a desktop icon that can be used by whoever is logged in when the service is started. For more information, see your Windows NT documentation.

This Account. Select this only if *none* of your hosts uses the Windows NT database; then enter the name of the appropriate user account; make sure the user is a Host Administrator.

Note

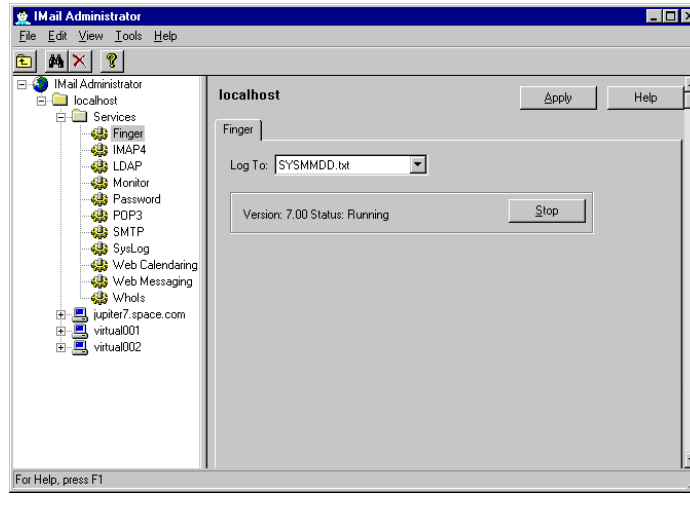
If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Configuring the Finger Server

To configure the Finger server:

1 In IMail Administrator, select the "**Services**" folder in the left panel.

2 Click **Finger**. The Finger tab appears.



3 Enter the options you want to use to configure the Finger server.

Each option is described at the end of this procedure.

4 Click **Apply** to save your changes.

5 After making changes, stop the service, wait 5-10 seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

Logging Options

In the **Log To** box, select the way you want to log Finger events:

sysMMDD.TXT. This sends event information to a file of this name where *mm* is the month and *dd* is the day the log was written. This file is stored in the *Spool* directory.

- **No Log**. Select this to turn off the logging of events.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer).
- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab.

Server Status. A status message to the left of the **Start/Stop** button shows the version number, and whether or not the service is running.

Start/Stop Service. This button toggles between **Start** and **Stop** depending on whether or not the service is running.

Chapter 15: Password Server

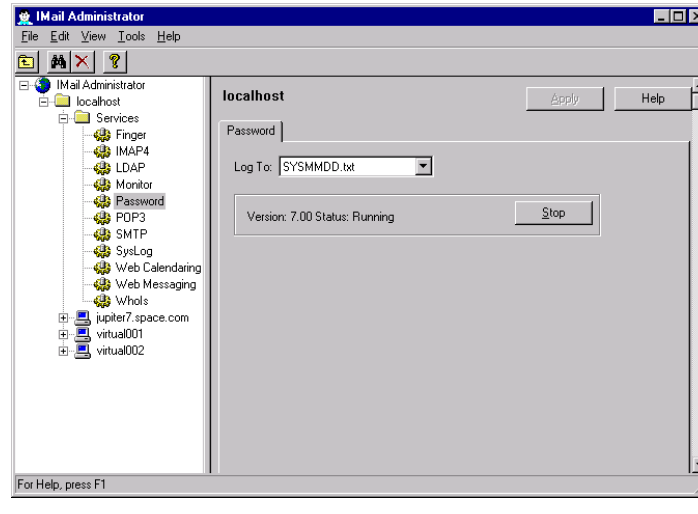
The Password server allows older POP3 mail clients to change their IMail Server password without logging in to the NT server.

These older mail clients have the ability to use the POP3 protocol to change passwords remotely. These clients include older versions of Eudora. As a Windows NT service, the Password service can run completely hidden or with some feedback. The Password server continues to run when you log off the Windows NT system. IMail Server does not require the Password server to be running for normal operations.

Configuring the Password Server

To configure the Password server:

1 In IMail Administrator, select the "**Services**" folder in the left panel, then click **Password**. The Password tab appears.



2 Enter the options you want to use to configure the Password server. Each option is described at the end of this procedure.

3 Click **Apply** to save your changes.

4 After making changes, stop the service, wait 5-10 seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

Logging Options

In the **Log To** box, select the way you want to log Password events:

- **sysMMDD.TXT**. This sends event information to a file of this name where *mm* is the month and *dd* is the day the log was written. This file is stored in the *Spool* directory.
- **No Log**. Select this to turn off the logging of events.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer.)
- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab.

Server Status. A status message to the left of the **Start/Stop** button shows whether or not the service is running.

Start/Stop Service. This button toggles between **Start** and **Stop** depending on whether or not the service is running.

Logging On

By default, the Password service logs on to the System Account. You can view and change Password settings by using the **Services** applet in the Control Panel.

To view and/or change settings for the Password service:

1 In the Control Panel, double-click the **Services** applet.

2 Select **IMail PWD Server** and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.
Allow Service to Interact with Desktop. Select this to provide a desktop icon that can be used by whoever is logged in when the service is started. For more information, see your Windows NT documentation.

This Account. Select this only if *none* of your hosts uses the Windows NT database; then enter the name of the appropriate user account; make sure the user is a Host Administrator.

If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Note

In order to login to the Password Server using an IP-less virtual host, you must use the format of user@domain.com (ensuring the domain they are logging into.

Chapter 16: The Monitor Server

The Monitor server allows you to monitor the status of IMail Server and other services. In addition, the Monitor server provides a means for you to perform system administration tasks using a web browser.

The Monitor server lets you:

- Monitor IMail services (SMTP, POP3, IMAP4, LDAP, PServ, Whois, Finger, and Syslog, Web Calendaring and Web Messaging) as well as disk space on the IMail Server primary system.
- Have the monitor program send e-mail, a pager message, or a beeper message when a service is down.
- Monitor other services such as DNS, NNTP, WWW, FTP, and Telnet on either the local or a remote system.
- Monitor the default gateway on the local system or on a remote system.

When you view service status from a web browser, services displayed in green are up and running; services displayed in red are down.

You can access the Monitor functions either from IMail Administrator or from any web browser (if the Web Administration function of the Monitor server is configured and running) connected to Port 8181 of the IMail Server system.

As a Windows NT service, the Monitor service can run completely hidden or with some feedback. The server will continue to run when you log off the Windows NT system.

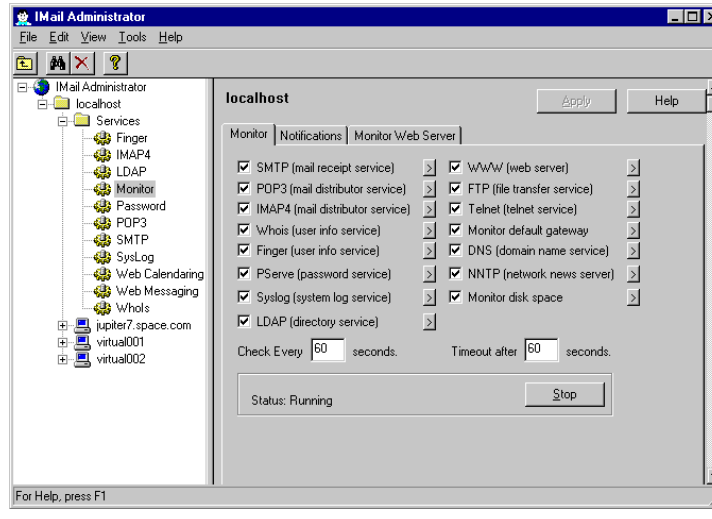
The Monitor server gets its settings from the Windows NT registry and two *.ini* files found in the *winnt* directory: *Monitor.ini* and *ipnotify.ini*. These *.ini* files are used to maintain compatibility with Ipswitch's WhatsUp network monitoring tool, which may be installed on your system. This is so that any notifications you have defined in either IMail Server or WhatsUp automatically show up in the list of notifications in the other application.

Configuring the Monitor Server

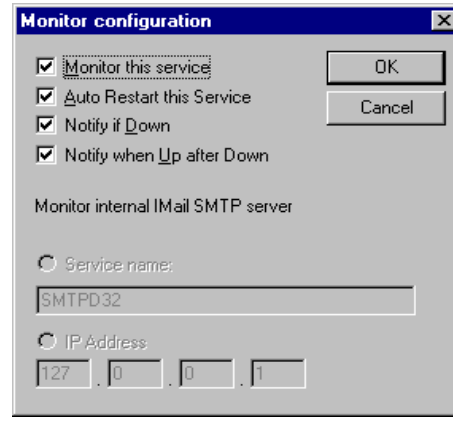
After making changes, stop the service, wait five to ten seconds and restart the service. Any changes that you make are saved automatically as soon as you press the **Stop/Start** button.

To configure the Monitor server:

1 Select the "**Services**" folder, then click **Monitor**. Click the **Monitor** tab. The Monitor settings appear.



2 Select the services that you want to monitor. For each service that you select, you can click the associated arrow button to access configuration options. For example, if you click the arrow button for the SMTP service, the following dialog box appears



Make sure the **Monitor this service** option is selected. If you want the service to automatically restart after going down, select the **Auto Restart this Service** option.

You do not need to set the service name and IP address for the services that are part of IMail Server. These services are SMTP, POP3, IMAP4, Whois, Finger, LDAP, System Logger, and Password.

For services that are *not* part of the IMail Server system (such as DNS), you can enter a service name if the service is local, or an IP address if the service is on a remote system.

3 If you have defined and enabled e-mail, pager, and/or beeper notifications, select **Notify if Down** and the **Notify when Up after Down** as desired. For information on setting up notifications, see “Working with Notifications” on page 199. For information on enabling notifications, see “Enabling Notifications” on page 207.

4 Click **OK** to exit the “Monitor Configuration” dialog box and return to the **Monitor** tab.

5 (Optional) Select **Monitor default gateway**, click the arrow to display configuration options, select the options you want to use, and click **OK**.

6 (Optional) Select **Monitor disk space**, then click the arrow to display the “Monitor Configuration” dialog box, enter the desired options and click **OK**.

7 In the **Check Every** nn **seconds** box, specify how often the monitor program should poll the services.

8 In the **Timeout after** box, enter the number of seconds to wait for a response.Logging On

By default, the Monitor service logs on to the System Account.

Note

We recommend that you keep the default setting so the Monitor service logs on to the System Account. If you use an account other than the System Account, all functions may not work properly.

Changing Monitor Settings in the Control Panel

You can view and change Monitor settings by using the **Services** applet in the Control Panel.

To view and/or change settings for the Monitor service:

1 In the Control Panel, start the **Services** applet.

2 Select the **IMail Monitor Server** service and click **Startup**.

3 (Optional) Select the desired **Startup Type**.

4 Under **Log On As**, select the appropriate account:

System Account. Select this if any one of your mail hosts uses the Windows NT database to register and authenticate users.

Allow Service to Interact with Desktop. Turn this on to provide a desktop icon that can be used by whoever is logged in when the service is started. Using the desktop icon to view the Monitor application window, you can view debug information or a TCP log for the Monitor service: simply select **Debug info** or **TCP Log** from the **View** menu. (The debug log shows the "returns" from the services you are running. The TCP log shows the actual conversation between IMail server and the service.)

For more information, see your Windows NT documentation.

This Account. Select this only if *none* of your hosts uses the Windows NT database, then enter the name of the appropriate user account; make sure the user is a Host Administrator.

Note

If one or more of your hosts is based on an external database, the **Log On As** account must be an account that has access to the external database.

Click the **Quiet** button to turn off a sound alarm triggered by a monitored service going down, or coming back up after being down.

Working with Notifications

When a service doesn't respond to polling, the Monitor server can send notification via a beeper, a pager message, or an e-mail in addition to the visual (red, green) status and the optional sound alarm.

Setting up notification for services involves three processes:

1 You first need to *define* the notification actions that you will want to use, such as activating a network administrator's beeper or sending e-mail to an individual.

2 Make the notification available to IMail Server by adding it to the **Notifications** tab.

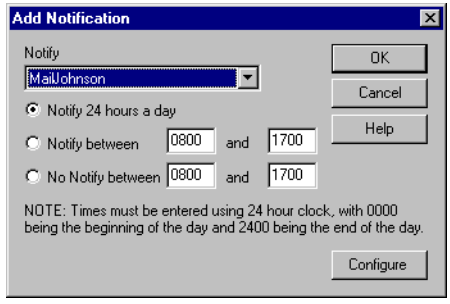
3 Then, you can *enable* notification actions for services, which is just a matter of turning on one or more notifications on the **Notifications** tab. For information on enabling notification actions for a service, see "Enabling Notifications" on page 207.

Defining Any Type of Notification

To define any type of notification, do the following:

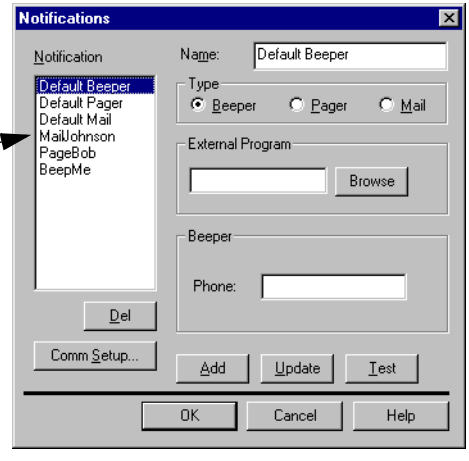
1 In IMail Administrator, expand the "**Services**" folder in the left panel and click **Monitor**. Then click the **Notifications** tab.

2 Click **Add** to view the "Add Notification" dialog box.



3 Ignore the settings in this box for now, and click **Configure** to view the Notifications dialog box.

Notifications that appear in this list are defined in the ipnotify.ini file (located in the *winnt* directory.)



The following sections describe how to set up each type of notifications.

Defining Beeper Notifications

You can define a notification to activate a beeper when the service does not respond to polling.

To define a new beeper notification:

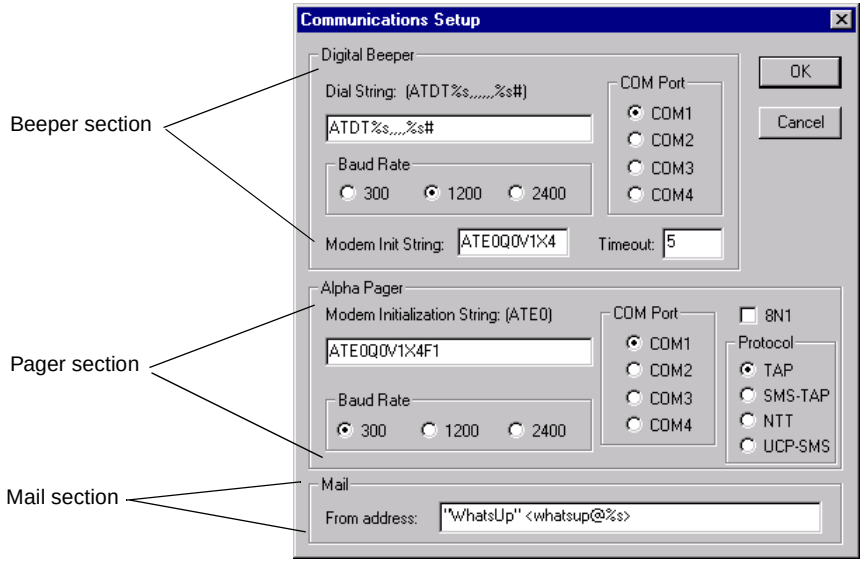
1 In the **Name** text box, delete what's there and enter a unique name to identify the notification, for example "BeepBob."

2 Under **Type**, select **Beeper**.

To use an external program to connect to the beeper, see "Using an External Beeper Program" on page 202.

3 In the **Phone** text box, enter the phone number to dial.

4 Click **Comm Setup**. The "Communications Setup" dialog box appears. You need to fill in the **Digital Beeper** section in the top half of the dialog box.



5 The default **Dial String** is: `ATDT%S,,,,%S#`
The first `%S` is replaced by the phone number and the second `%S` is replaced by the beeper code. Most modems and beepers support the use of '#' to terminate the message and '*' to print out a dash. You may find a need to increase the number of commas in the dial string if it dials the code too soon or decrease the number of commas if it waits too long.

6 Under **Baud Rate**, select the speed (bits per second) at which the serial port will communicate with the modem.

7 Select the **Com Port** to which your modem is attached.

8 The **Timeout** value (in seconds) determines how long the system waits after sending the last character before it hangs up the phone if a transition is not recognized.

When you have entered the information, click **OK** and then click the **Add** button in the Notifications dialog box to add the new beeper notification to the **Notifications** list on the left side of the dialog box. To test the beeper notification, select its name in the list, and click **Test**.

Using an External Beeper Program

You can also use an external program of your own to handle beeper notification. The presence of an external program name in the **External Program** text box enables the external program.

The following information is made available to the external program via the command line.

arg 1: either DN or UP
arg 2: the phone number entered in the Notification options
arg 3: the beeper code as specified in the Notification options
arg 4: the IP address of the host

External program example arguments:

0: beeper.exe 1: DN 2: 8694297 3: 3333 4: 127.0.0.1
0: beeper.exe 1: DN 2: 8694297 3: 2222 4: 127.0.0.1
0: beeper.exe 1: UP 2: 8694297 3: 2222 4: 127.0.0.1

The external program is executed with SW_SHOWMINNOACTIVE.

The external beeper program will not be activated if someone silenced the alarm before the system check is reached.

The UP message will only be sent if the packets lost is greater than system checks when the service comes back up.

Defining Pager Notifications

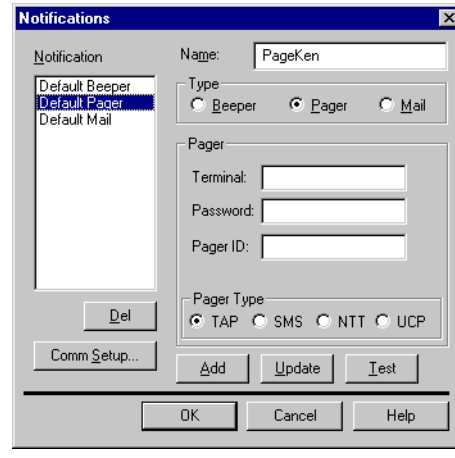
You can define pager notification to send a message to a pager when a service does not respond to polling. The notification message sent to the pager is predefined. It is a simple message, such as: `SMTP down`, `SMTP up`. IMail Server supports Motorola PageNet and other TAP (Telocator Alphanumeric Protocol) pagers.

To define a pager notification action:

1 If you are not in the Notifications dialog box shown at the top of page 200, complete the procedure, “Defining Any Type of Notification” on page 199.

2 In the **Name** text box, enter a unique name to identify the notification, for example “PageKen.”

3 Under **Type**, select **Pager**. The dialog box shows the pager options.



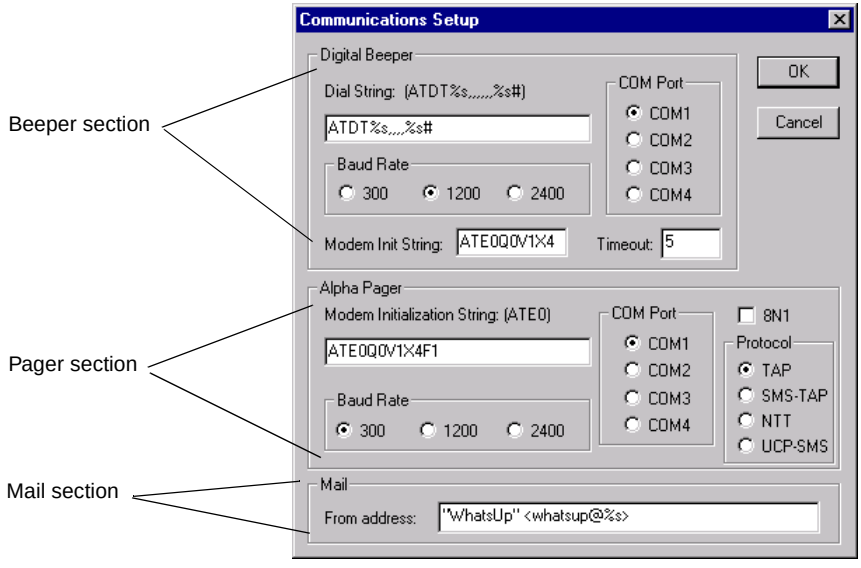
4 In the **Terminal** box, enter the phone number to dial.

5 Enter the pager **Password**, if required.

6 Enter the **Pager ID** number.

7 Select the **Pager Type**.

8 Click **Comm Setup**. You will complete the information for the middle of this dialog box, under the words **Alpha Pager**



The default **Modem Initialization String** is ATE0. What is expected in this string are the modem commands for "Command Echo Off" (E0), "Result Codes On" (Q0), "Verbal Results" (V1), "Result Codes Displayed" (X4), and "Local Echo OFF" (F1). The recommended string to use is: `ATE0Q0V1X4F1.`

9 Select the **Baud Rate** (bits per second) at which the serial port will communicate with the modem.

10 Select the **COM Port** to which your modem is attached.

11 Select the **8N1** check box to send 8 data bits at a time, no parity, one stop bit. Leave it unselected to send 7 data bits, even parity, one stop bit.

12 Under **Protocol**, select the appropriate value; this is determined by the paging service provider you use. TAP is typical for U.S. paging systems. SMS-TAP is typical for U.S. SMS paging systems. NTT is used primarily for Japanese paging systems, and UCP-SMS is typical of European SMS paging systems.

13 When you have entered the information, click **OK** to return to the Notifications dialog box.

14 Click the **Add** button in the Notifications dialog box to add the new pager notification to the list of Notifications on the left side of the dialog box. To test the new pager notification, select its name in the list, and click **Test**.

Defining E-mail Notifications

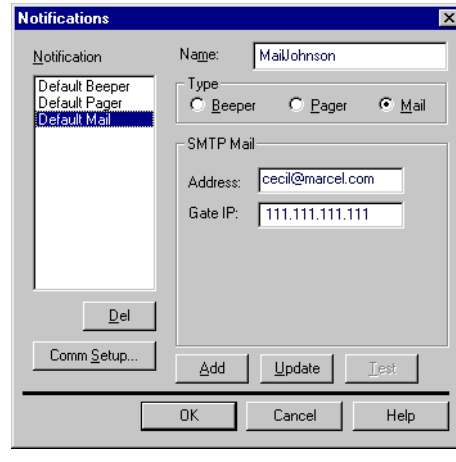
You can define an e-mail notification to send a predefined message to an e-mail address when a service does not respond to polling. The message is a simple one, such as: `SMTP down`, `SMTP up`.

To define an e-mail notification action:

1 If you are not in the Notifications dialog box shown at the top of page 200, complete the procedure, “Defining Any Type of Notification” on page 199.

2 In the **Name** text box, enter a unique name to identify the notification, for example “MailJohnson.”

3 Under **Type**, select **Mail**. The dialog box shows the e-mail options.



4 Enter an e-mail **Address** that is accepted by the Gate IP. (This can be a simple name.) The Address should not contain brackets, braces, quotes, or parentheses.

5 Enter the **Gate IP** address of a host running SMTP.

6 If you need to change the **From** address, click **Comm Setup**. You see the Communications Setup dialog box shown on page 201. You will complete just the information under the word **Mail** at the very bottom of this dialog box.

7 The **From** Address defines the sender of an e-mail notification as: `<Monitor@%s>`, where `%s` is the local host name. In most cases, you will not need to change this address. If you do change the address, be sure to keep the angle brackets (< >) in place.

8 When you have entered the information, click **OK** to return to the Notifications dialog box.

9 Click the **Add** button in the Notifications dialog box to add the new e-mail notification to the list of Notifications on the left side of the dialog box. To test the new notification, select its name in the list, and click **Test**.

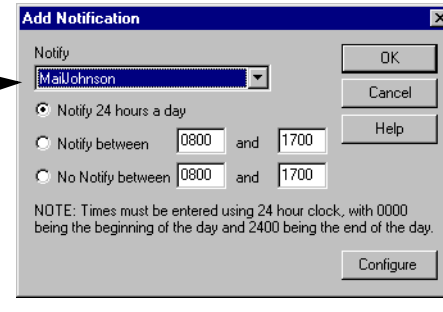
Putting a Notification on the Notifications Tab

In IMail Server, a notification is not activated for IMail Server until it appears on the **Notifications** tab. To activate a defined notification for use in IMail Server:

1 If you are not already on the **Notifications** tab, select the "**Services**" folder in the left panel, and then click **Monitor**. Then click the **Notifications** tab.

2 Click **New**. The "Add Notification" dialog box appears. All notifications that have been defined are available from the **Notify** drop-down list.

This list shows all defined notifications. Click the drop-down arrow to view the entire list.



3 Select the notification you want to add to the **Notifications** tab from the drop-down list.

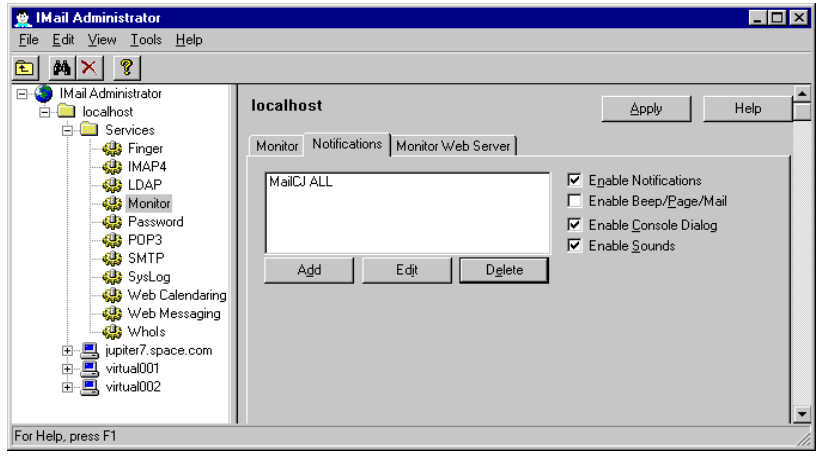
4 Select whether to receive the notification 24 hours a day or between certain hours.

5 Click the **OK** button. The notification appears in the **Monitor Notifications** list box on the **Notifications** tab and can now be enabled.

Enabling Notifications

Once you have defined a notification and put it on the **Notifications** tab, as described in the previous sections, you must *enable* it.

1 Select the **Notifications** tab. The list box shows all the notifications you have activated for use in IMail Server.



To edit an enabled notification, select it and click **Modify**.

2 Select **Enable Notifications** to enable console and sound notifications.

3 Select **Enable Beeper/Pager/Mail** to use any of the beeper, pager, or e-mail notifications in the list box.

4 (Optional) Select **Enable Console Dialog** to display the notification in a message box on the IMail Server system.

Note

In order for the **Enable Console Dialog** option to function, the **Allow Service to Interact with Desktop** option must be enabled in your computer's Service Control Manager. For more information, see "Changing Monitor Settings in the Control Panel" on page 198.

5 (Optional) Select **Enable Sounds** option to play a *.wav* file when a monitored service goes up or down. (Your system must have a sound card installed.)

6 Click **Apply** to save your changes.

You are now ready to enable and disable notifications on a per service basis.

1 Click the **Monitor** tab and make sure the services you want to monitor are selected.

2 To get a notification about a monitored service, click the arrow button to the right of the service name. Select either **Notify if Down**, **Notify when Up after Down**, or both, then click **OK**.

3 On the **Monitor** tab, click **Apply** to save your changes.

Disabling Notifications

You can disable a notification as follows:

1 Select the **Notifications** tab. The list box shows all the notifications you have activated for use in IMail Server.

2 To disable a notification (but not delete its definition), select it and click **Delete**.

Configuring the Web Administration Capability

The Monitor server can enable a Web Administration function that lets you view the status of monitored services, modify IMail Server user registration data, and view log data.

To configure Web Administration through the Monitor server:

1 Click the **Monitor Web Server** tab. The Web Access properties appear.

2 Turn on **Enable Web Administration through Monitor**.

3 Enter the **Port** number for Web Administration. The default is 8181.

4 Enter the **Title** that you want to appear on the web page when accessed from a web browser.

5 In the **Web Dir** box, enter the directory where you can place additional files to be served by the Web Administration function.

6 When **Hide User List Button** is selected, the Web Administration capability will not display a list of users in the host administrator functions.

7 Click the **Control Access** button to specify an IP address or set of IP addresses that are either granted access to the web server or denied access. Systems that do not have access to the web server system will not be allowed to create a connection.

8 Click **Apply** to apply the settings. The Monitor server must be stopped and restarted for changes to take affect.

Setting Access to Web Administration

You can specify an IP address or set of IP addresses that are either granted or denied access. Systems that do not have access to the Monitor server will not be allowed to create a connection.

To deny access to a specific computer or group of computers:

1 Click **Control Access**. The Access Control properties appear.

2 Select **Granted Access**.

3 Click **Add**. The “Deny Access On” dialog box appears.

4 In the **IP Address** box, enter the IP address of the computer to be denied access to Web Administration.

To deny access to a group of computers, select **Group of Computers**. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This will deny access to those 254 systems.

5 Click **OK** to add the IP address(es) to the list. Access will be granted to all computers except those listed.

6 Click **OK** to save the changes. Note that you must stop and restart the monitor service for the changes to take affect.

To grant access to a specific computer or group of computers:

1 Click **Control access**. The “Access Control” dialog box appear.

2 Turn on **Denied Access**.

3 Click **Add**. The “Grant Access On” dialog box appears.

4 In the **IP Address** box, enter the IP address of the computer to be granted access to the Web Administration through the Monitor server.

   To grant access to a group of computers, select **Group of Computers**. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be granted access. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This will grant access to those 254 systems.

5 Click **OK** to add the IP address(es) to the list. Access will be denied to all computers except those listed.

6 Click **Apply** to save the changes. Note that you must stop and restart the monitor service for the changes to take effect.

Using the Web Administration Capability

You can access the Monitor server from any web browser if the Web Administration capability is enabled as described in “Configuring the Web Administration Capability” on page 208.

What you see when you access the Monitor server from a web browser is determined by the User Properties for the user ID you log on with.

For example, in order to log on to the Web Administration capability of the Monitor server, your **Allow Web Access** option must be selected. Furthermore, once logged on, only System Administrators will see the System Administration menu, and only Host Administrators will see the Host Administration menu.

List Administrators will not be able to administer lists by logging on to the Web Administration capability of the Monitor server. In order for list administrators to administer lists on the web, they must use Web Messaging.

To access the Web Administration capability of the Monitor server from a web browser:

1 Start a web browser and open the URL address for the Web Administration server. The address is:

`http://your_imail_server_system:8181`

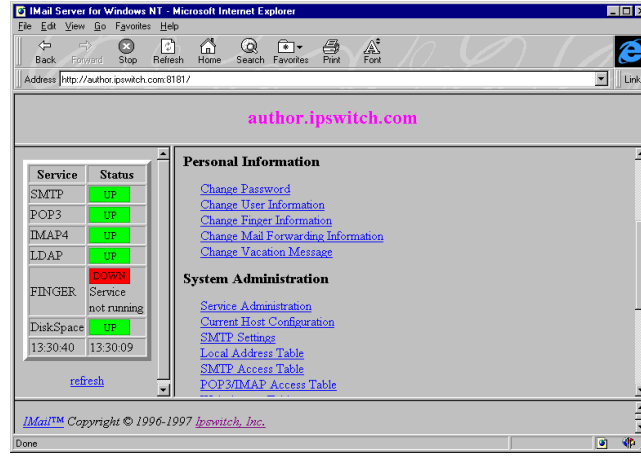
where *your_imail_server_system* is the host name of the IMail Server and 8181 is the port number for the web function.

2 Enter your IMail user ID and password.

Note

The IMail user ID and password use base 64 encoding for sending this information via the HTTP protocol.

The following screen shows an example of the web page display. In addition to providing access to the user mail accounts, the web page can display the status of services monitored by the Monitor server.



In the left panel, the Monitor shows the status of monitored services. Services in green are running; services in red are stopped.

The right panel shows the menu of administration functions. All users will see the functions under **Personal Information**. System administrators will also see **System Administration** functions. Host administrators will also see **Host Administration** functions. List Administrators will also see **List Administration** options.

Personal Account Options

All users have access to the personal information items:

- Change Password — allows user to change password.
- Change User Information — allows user to change the information that is published by the LDAP server.
- Change Finger Information — allows user to change the information in the *plan* file; this information is provided in response to a Finger request.
- Change Mail Forwarding Information — allows user to set a forwarding e-mail address to which all mail is sent.
- Change Vacation Message — allows user to enter a message that will be sent once to each person who sends mail to the user. The presence of a message activates this feature. Therefore, if the window is empty, the vacation message feature is disabled.

System Administration

System Administrators will see these menu items:

- Service Administration — allows the administrator to stop and start IMail services and configure service monitoring.
- Current Host Configuration — allows the administrator to view and modify the host configuration.
- SMTP Settings — allows the administrator to change settings for the SMTP server. For a description of each setting, see “Chapter 8: SMTP Server” on page 147.
- Local Address Table — allows the administrator to modify the Local Address table. For more information on mail relay capabilities, see “Chapter 8: SMTP Server” on page 147.
- SMTP Access Table — allows the administrator to modify the SMTP access table. For more information on SMTP access, see “Chapter 8: SMTP Server” on page 147.
- POP3/IMAP4 Access Table — allows the administrator to modify the POP3/IMAP4 access table. For more information, see “Chapter 10: POP3 Server” on page 165 and “Chapter 11: IMAP4 Server” on page 177.

- Web Access Table — allows the administrator to modify the web access table; this specifies the IP addresses that the Monitor server Web Administration feature allows to connect.
- View Monitor Database — displays all service monitoring events.
- View Spool Directory — displays the message queue and provides access to log files.
- Edit Welcome Message — allows the administrator to enter up to 1000 characters of plain text and/or raw HTML code. The message is displayed in the main logon screen above the logon form. The message persists across reboots.
- Recent IMail News — displays the web page where Ipswitch reports information on new releases, bug fixes, and workarounds.
- View Monitor Access Log — displays each access attempt to the IMail Web Messaging server and to the Monitor server.
- View Monitor System Log — displays logons to the IMail Server and to the Monitor server and shows the status of services.
- View IMail System Log — displays IMail Server send and receive mail transactions (the contents of *syslog.txt*).
- View IMail Syslog Log — displays the contents of *lognnnn.txt*, the System Log Service file. This file records transaction and debug information when enabled for any IMail services.

Host Administration

- Host Administrators will see a **User Administration** menu item. It lets host administrators add, modify, and delete users and aliases.
- List Administrators will see a **List Administration** menu item. This allows user to maintain specific list server mailing lists.

For more information on creating and maintaining users and aliases, see “Chapter 4: User Mail Accounts” on page 59.

Chapter 17: List-Server Mailing Lists

The IMail list server lets you set up automated mailing lists on the IMail Server. These automated lists are known as “list-server mailing lists;” they differ dramatically from a simple group alias (which is just a name for a list of users).

A list-server mailing list can receive mail and re-send the mail to all the users on the mailing list. List-server mailing lists are used widely on the Internet to share information about a topic.

You access the IMail list server using IMail Administrator.

Features

The IMail list server provides the following features:

- Lists can be completely “open” -- allowing postings by anyone on the Internet.
- Lists can also be “public,” meaning that anyone can get on the list by subscribing to it. Users can subscribe to, or unsubscribe from, a list simply by sending the appropriate message to the list server.
- Lists can be *unmoderated* (any message sent to the list is immediately posted to all users on the list) or *moderated* (all messages are viewed by the moderator before being posted to the list).
- Postings to the list can be further controlled by use of a password or by use of a “posters list” (a list of people authorized to post to that list).
- Lists can also be private. A private list does not accept a *Subscribe* command; only the list administrator can add people to the list.
- Messages to a list-server mailing list can be accumulated and periodically mailed out as a *digest*.
- The list administrator can enter an identifying text string to appear on the **Subject** line of all messages (or a digest) posted to the list.

- The list administrator can enter header or trailer text (containing information such as the *Subscribe* and *Unsubscribe* instructions) to appear with all messages (or a digest) posted to the list.

Types of List-Server Mailing Lists

Mail that is received by a list-server mailing list and re-sent to the list subscribers is "posted." Those who can post to a particular list are determined by the *type* of list. There are three types of basic lists. (The list type is set on the **Security** tab of the list properties.)

- Open lists (to which anyone can post a message; the poster need not even subscribe to the list)
- Subscriber lists (to which only subscribers can post)
- Moderated lists (to which only the list owner can post)

Using Passwords and Posters Lists

The posting of messages to each type of list can be further restricted by enabling one or both of the following:

- A password requirement (See "Using a Password" on page 218.)
- A posters list

If a password or posters list is enabled, anyone not using the password and/or listed in the posters list will have their mail returned. The list owner (or moderator) is also notified of the attempt to post.

Note

If there are only a few individuals who you want to post to the list, you can simply give those few the appropriate password. However, if there are more than a few individuals who are to be allowed to post to the list, it may be more efficient to use a "posters" list.

Open Lists (Anyone Can Post)

The characteristics of an open list are the following:

- Anyone can post to the list by sending a message to an address in the form of *listname@domain.com* if **Use Password** and **Enable Posters List** are turned off.
- If **Use Password** is turned on, only those with the password can post. (See "Using a Password" on page 218.)

- If **Enable Posters List** is turned on, only those in the posters list can post.
- If both **Use Password** and **Enable Posters List** are turned on, the poster must use the password and be in the poster list.

Subscriber Lists

The characteristics of a subscriber list are the following:

- The list is made up of subscribers. An individual becomes a subscriber by sending a message addressed to the IMail list server (imailsrv*@domain.com* where *domain.com* represents the mail host); in the body of the message, the intended subscriber enters the subscribe command and the list name. For more information, see “Requesting Information and Subscribing” on page 218.
- Subscribers can post by addressing a mail in the form of *listname@domain.com* if **Use Password** and **Enable Posters List** are turned off.
- If **Use Password** is turned on, only subscribers with the password can post. (See “Using a Password” on page 218.)
- If **Enable Posters List** is turned on, only subscribers in the posters list can post.
- If both **Use Password** and **Enable Posters List** are turned on, the subscriber must use the password and be in the poster list in order to post.

Moderated Lists

The characteristics of a moderated list are the following:

- The moderator can post by sending a message to an address in the form of *listname@domain.com* if **Use Password** and **Enable Posters List** are turned off.
- If **Use Password** is turned on, the moderator must enter a password in order to post to the list. This prevents others from “impersonating” the moderator by using the moderator's mailing address. (See “Using a Password” on page 218.)

- If **Enable Posters List** is turned on, the moderator receives only mail from those in the posters list.
- If both **Use Password** and **Enable Posters List** are turned on, the moderator receives only mail from those in the posters list, and the moderator must enter a password in order to post to the list.

Posting to a List

A user attempts to post a message to a list by addressing the message to the name of the list-server mailing list. For example, to send a message to the "beer" list on domain.com, the user would enter:

```
To: beer@domain.com
Subject: India Pale Ale

... body of message ...
```

Using a Password

To use a password, the first characters on the **Subject** line must be the password enclosed by two colons and brackets:

```
To: beer@domain.com
Subject: [:password:]India Pale Ale

... body of message ...
```

Note

Passwords are case-sensitive.

Requesting Information and Subscribing

In order for a user to get information about lists on a particular host, or to subscribe to lists on a particular host, the user must send a request addressed to `imailsrv`*@domain.com* (where *domain.com* is the name of the host). This e-mail address is a built-in IMail alias that lets users:

- Get general help about the list-server for a particular mail host
- Get specific help about a particular list
- Get a list of all the lists available on a particular mail host
- Get a list of all the subscribers to a particular list

- Subscribe to a subscriber list
- Unsubscribe from a subscriber list

Format of Requests

Requests addressed to `imailsrv`*@domain.com* must contain a list-server command and (when appropriate) a list name in the body of the message. The following commands may appear in the body of the message:

- Help
- Help *listname*
- List
- List *listname*
- Subscribe *listname your_name*
- Unsubscribe *listname your_name*

Commands for Requesting Information

The following examples assume there is a list named *beer* on a mail host named *domain.com*. The commands for requesting information are the following:

- **To get general help from the list server:**

```
TO: imailsrv@domain.com
Subject:

help
```

- **To display the names of all of the lists on the IMail server:**

```
TO: imailsrv@domain.com
Subject:

list
```

- **To get a list of users subscribed to a specific list:**

```
TO: imailsrv@domain.com
Subject:

list beer
```

- **To get help for a specific list:**

```
TO: imailsrv@domain.com
Subject:

help beer
```

Commands for Subscribing and Unsubscribing

The following examples assume there is a list named *beer* on a mail host named *domain.com*. The commands for subscribing and unsubscribing are the following:

- **To subscribe to the list:**

```
TO: imailsrv@domain.com
Subject:

Subscribe beer Fred Farkle
```

- **To unsubscribe from the list:**

```
TO: imailsrv@domain.com
Subject:

Unsubscribe beer Fred Farkle
```

Commands for the Use of Subscribers

The following examples assume there is a list named *beer* on a mail host named *domain.com*. Once a user is already subscribed to a list, he can use the following commands:

- **To receive a digest of messages sent to the list,** enter a command in the form of **set mode digest** *listname.* For example,

```
TO: imailsrv@domain.com
Subject:

set mode digest beer
```

- **To cancel digest mode and receive messages as they are sent to the list**, enter a command in the form of **set mode standard** *listname.* For example,

```
TO: imailsrv@domain.com
Subject:

set mode standard beer
```

Commands for the Use of the List Owner (or Moderator)

The following example assumes there is a list named *beer* on a mail host named *domain.com*. Only the list owner (or moderator) can use the following:

- **To unsubscribe a user from the list:**

```
TO: imailsrv@domain.com
Subject:

Unsubscribe beer userid@domain.com
```

How the List Server Works

When you create a mail host, the program alias *imailsrv* is created automatically and defined as *imailsrv.exe domain*. Therefore, messages addressed to imailsrv*@domain.com* are processed by the IMail list server application, *imailsrv.exe*.

Note

Upgraders: In earlier versions of IMail Server, the list server application and its alias were named *listserv*, but they were changed due to a trademark conflict. If you have used the *listserv* alias, you do not have to change anything because IMail Server allows the old *listserv* alias to work properly. However, all aliases now return *imailsrv* in place of *listserv.* If you set up a new list, use the *imailsrv* alias.

The list server directory is the directory *lists* created under your main *imail* directory. Each list is created as a separate directory under that directory and there is an alias created for each list.

Creating a List-Server Mailing List

To create a list (assuming that **Use Wizards** on the **Tools** menu is turned off):

1 In the left panel, expand the mail host folder and then select the "**Lists**" folder.

2 Click the **Add List** button. The "Add New List" dialog box appears.

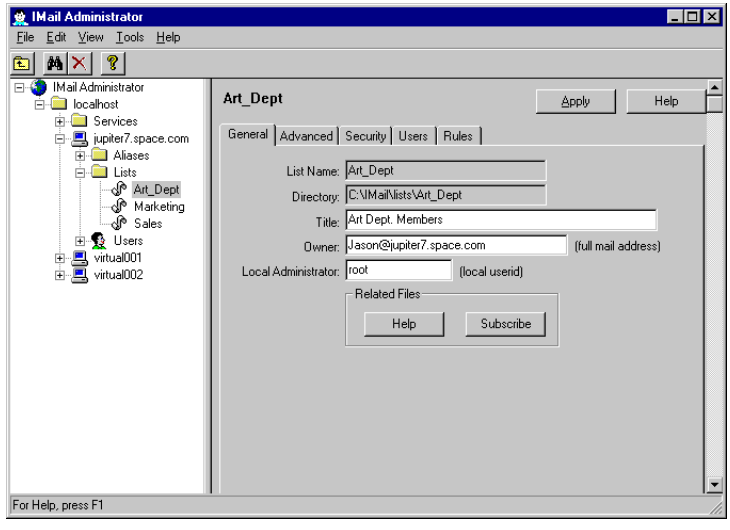
3 Enter a name for the list-server mailing list. This is the name used to send mail to the list. For example, if you enter the name *Parrotlist*, users will send mail to the list by specifying the "To" address as follows: `Parrotlist@domain.com`.

The name must be from 3 to 23 characters in length, with no spaces between characters.

Note

Do not use the name *imailsrv* for a list-server mailing list; this name is reserved.

4 Click **OK**. The **General** tab appears. The **List Name** and **Directory** are displayed but cannot be edited.



5 Complete the entries.

Title. Enter a descriptive title to help the list owner and/or administrator identify the list. The title must be from 3 to 23 characters in length; spaces are allowed.

Owner. This is the full e-mail address of the mail account that receives all messages (such as *Subscribe* requests, *Unsubscribe* requests, and error messages) to the list. It is also the account from which all messages are sent:

- To the list
- To anyone who requests information about the list
- In response to invalid attempts to post to the list

The list owner and list administrator are usually the same person, but a “dummy” user account can be set up for the list owner to hide the identity of the list administrator. On a moderated list, the list owner is also known as the “moderator.”

Local administrator. This is a user ID on the current mail host who can administer the list using Web Messaging. This person can modify list properties, add and delete users, and edit all related files.

Note

List-server mailing lists can also be administered by any user on the local mail host who is a **List Administrator** as specified on the **General** tab of the user properties.

Related Files. You can edit related files by clicking the appropriate button:

- **Help**. The Help file (HELP.TXT) displays a prepared message (limited to 1000 characters) that the list sends in reply to a `Help` *listname* request.
- **Subscribe**. The Subscribe file (SUBSCRIB.TXT) contains a prepared message (limited to 1000 characters) that the server sends in reply to successful completion of a `Subscribe` *listname* request.
- **Addresses**. The Addresses file (USERS.LST) is the list of e-mail addresses that is used to address mail to this list. This file is updated automatically when someone subscribes or unsubscribes. It is a text file with one address per line ending in a carriage return/line feed.

  This file can be edited using a text editor to add or delete addresses that receive mail from this list. However, the Users file (USERS.TXT) should also be similarly edited if you want people who use the *list listname* command to see an updated list of subscribers. Note that any invalid addresses in this file (if, for example, you make a typing error while editing this file) will be ignored when a message is sent to the list.
- **Users.** The purpose of this file, USERS.TXT, is to provide a list of subscribers to anyone who sends a *list listname* command to the list-server mailing list. (The list administrator can disable the *list* command.) This file is a list of user names and e-mail addresses that is updated automatically when someone subscribes or unsubscribes. This is not the list that is used to actually send mail to the list.

If you use a text editor to add or delete addresses from the Addresses file (USERS.LST), you should also edit this file (USERS.TXT) the same way (if you want people who use the *list listname* command to see an updated list of subscribers.

6 Click **Apply** to save your changes.

7 From a different system, send a test mail message to `imailsrv@`*domain*. In the body of the message, place the lines:

```
subscribe listname your_full_name
help
help listname
list
list listname
```

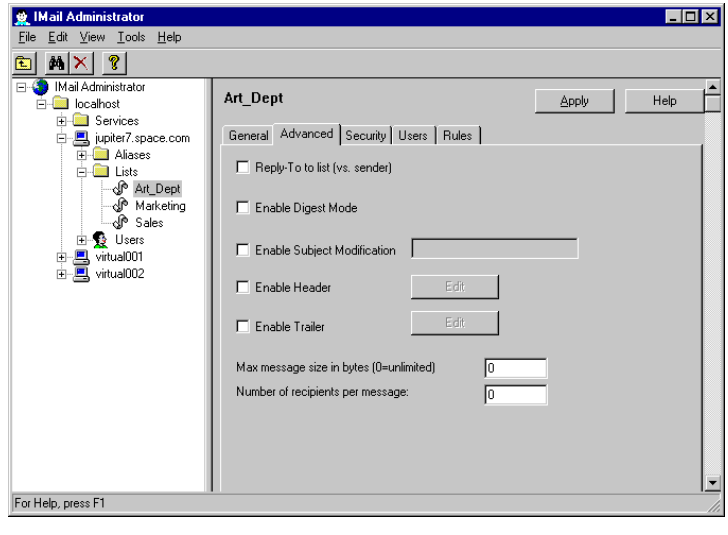
You should get five messages back from the system.

For a description of the commands accepted by the list server, see "Requesting Information and Subscribing" on page 218.

Setting Advanced Options

You can use the **Advanced** tab to further define the operation of a list-server mailing list. To do this:

1 Click the **Advanced** tab. The Advanced options appear.



2 Select the options you want to use.

Reply-To list (vs. sender). Turn on **Reply-To list (vs. sender)** to have replies from a subscriber go to the *list*. Turn this off to have replies from a subscriber go to the *sender* of the original message.

Enable Digest Mode. Turn this on to allow users to group the messages sent to the list into a digest, which is then sent as a single message. You can schedule the digest to be sent periodically or when the accumulated messages exceed a particular size. When list users receive a digest, it contains all messages sent since the last digest.

When you select **Enable Digest Mode**, the **Digest** and **Digest Scheduling** tabs appear. You need to define how the digest will operate by setting the options on these tabs. For more information, see “Setting Up Digest Mode” on page 228.

Enable Subject Modification. When selected, displays the text string (entered in the Edit box) at the beginning of the subject line of every message sent to the list.
For example, if you enter [Bird-info] as the defined text string, the subject line of messages will appear as follows:

```
Subject: re:[Bird-info] How do you receive mail?
```

The default string is the name of the list-server mailing list.

Enable Header/Enable Trailer. When selected, displays text information (entered in the **Edit** function) at the beginning or end of every message sent to the list. To enter the header information, select the **Enable Header** option, click **Edit**, and then enter the text information. This information is entered in the *header.txt* file. To enter the trailer info, select the **Enable Trailer** option, click **Edit**, and then enter the text information. This information is entered in the *trailer.txt* file.

For example, you can enter the *Subscribe/Unsubscribe* information for the list and have it appear at the beginning or end of every message.

Max message size in bytes (0 = unlimited). The maximum size (in bytes) of a message that can be sent to the list. Enter 0 if you want the size to be unlimited.

Number of recipients per message. You must calculate this number; it determines the number of recipients each SMTP process will send to.

Divide the expected number of subscribers by 25, and enter the result. We recommend that no more than 25 processes be used by a list.

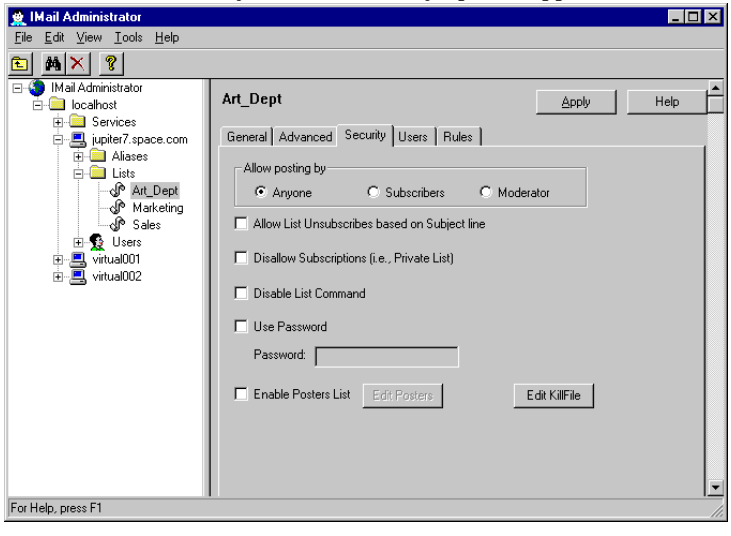
For information on how to change the default number of SMTP processes for IMail Server, see “Advanced Options” on page 151.

3 Click **OK** to save your changes.

Setting Security

You can use the **Security** tab to determine whether you want the list-server mailing list to be moderated or unmoderated, and to set access to the list.

1 Click the **Security** tab. The Security options appear.



2 Select the options you want to use.

Allow posting by. Determines who can post mail to the list.

- **Anyone** lets anyone on the Internet post mail.
- **Subscribers** lets only the subscribers post mail.

- **Moderator** lets only the list owner post mail. Select **Moderator** when you want the list owner to review all messages before they are posted to the list.

Allow List Unsubscribes based on Subject line. When a user wants to unsubscribe from the list, most list servers expect the *Unsubscribe* command to be specified in the body of mail message. If you want the list to also accept an *Unsubscribe* command specified in the Subject line of the message, select this option.

When selected, the list will accept the following commands in the **Subject** line to unsubscribe: *unsubscribe*, *remove*, *signoff*.

Note

It is recommended that you enable this command, but do not advertise that the list server supports it, because these messages are sent to the list address and will go out to the list if the command is misspelled.

Disallow Subscriptions. Rejects a *Subscribe* request, and users can only be added in one of the following ways:

- By using IMail Administrator to edit the User's file
- By the list administrator through Web Messaging
- By the list administrator through the Web Remote Administration utility

Note that *Unsubscribe* requests cannot be disabled.

Disable List Command. A user can obtain a list of the users subscribed to a list-server mailing list by addressing a message to the list server (for example, *imailsrv@domain.com*) and entering the `List` *listname* command in the body of the message. If you do not want users to receive a list of the subscribers to your list, select this option. (Note, however, that list owners can always access this command.)

Use Password. Turn this on to require a password for posting to the list. See "Using a Password" on page 218.

Enable Posters List. Enable this to specify who can post by listing their e-mail addresses in a file. Click **Edit Posters** to edit the list.

Edit Kill File. The kill file lets you specify a mail address or a particular mail host that you do not want to accept mail from. To specify a mail address or host in the kill file, click the Edit kill file button. The file *kill.lst* appears in the Windows Notepad. In the *kill.lst* file, enter one entry per line in either of the following formats:

```
userid@host
@host
```

For example, to deny access from a user mail account, you could enter: *fred@widget.com* . To deny access to all users from the mail host widget.com, you can enter: *@widget.com*.

The list server checks the incoming message's `MAIL FROM: <user@host>` line. The list server denies access to any mail address listed in the kill file.

The *kill.lst* file resides in the *IMail\lists\listname* directory (where *listname* is the directory for the particular list) and applies only to the specified list.

3 Click **Apply** to save your changes.

Setting Up Digest Mode

Lists that receive a large volume of messages can be set up in digest mode. This gives subscribers the option of periodically receiving a digest rather than being interrupted every few minutes with a new message from a list.

The list server stores all messages sent to the list in a digest mailbox. The accumulated messages are then sent to digest subscribers as a single message.

You schedule the digest to be sent at a particular time (for example daily or weekly) or when the size of the digest reaches a specified number of bytes. When list users receive a digest, it will contain all the messages sent to the list since the last digest was sent.

The digest is written to a special mailbox that you define. List users can choose between receiving a digest and receiving all messages as they are sent. To receive the digest, list users must send mail to the list server (*imailsrv@domain*) and enter the following command in the body of the message: set mode digest *listname*

Where *listname* is the name of the list-server mailing list. A confirmation message will be sent to the user. To cancel digest mode, users can enter the following command in the body of the message:

```
set mode standard listname
```

where *listname* is the name of the list-server mailing list.

To set up digest mode for a list-server mailing list:

To set up digest mode, do the following:

1 On the **Advanced** tab, select **Enable Digest Mode**.

When **Enable Digest Mode** is selected, the **Digest** and **Digest Schedule** tabs appear.

2 Click the **Digest** tab. The options appear.

3 **Digest Mailbox.** Enter the name of the mailbox where postings get stored before the digest mailing is sent out.

Copies of all postings are sent to:

`list_administrator-`*`mailboxname`*`@domain.com`

After a posting is sent to the digest list, the Digest Mailbox is emptied and a copy is saved to a file named in the format:

`digestmail``boxMMDD.mbx`

where *digestmailbox* is the name of the Digest Mailbox, MM is the month, and DD is the day of the posting.

The list administrator can view the mailbox by using either Web Messaging or the Remote Administration utility. He or she can delete or add messages before the posting is sent, and can also view posted digests in the *digestmailboxMMDD.mbx* file described above.

4 **Subject Line for Digest Postings.** Enter the text that you want to appear as the **Subject** line on digest postings.

5 **Include Headers/Trailers When Posting to Digest Mailbox.** When selected, the messages posted in the digest include the header and or trailer messages. We recommend disabling this option as it will make the digest larger and the digest has its own header and trailer.

6 **Strip Non-Text Attachments before Posting.** When selected, strips attachments such as images and zipped files.

7 **Enable Message Separators.** Lets you enter lines or characters to automatically separate messages in the digest posting. When you select this option, the **Edit** button is selected. Click **Edit** and then enter the lines or characters you want to use as a separator.

8 **Enable Digest Header/Enable Digest Trailer.** When selected, displays text at the beginning or end of every digest posting. To enter header or trailer text, select **Enable Digest Header/Trailer**, click **Edit**, and then enter the text. (This text is entered in the *digest_header.txt* and/or *digest_trailer.txt* file.)

   For example, you can enter the subscribe/unsubscribe information for the digest and have it appear at the beginning or end of every digest.

9 **Digest Subscribers.** Click this button to edit the list of users (*digest.lst*) subscribed to the digest.

10 Click **Apply** to save your changes.

11 Set the scheduling method (and date/time, if necessary) to determine how often and when the digest will be posted.

Digest Scheduling

If you have completed the previous procedure, you can now schedule the digest:

1 Click the **Digest Scheduling** tab. The scheduling options appear.

2 From the **Periodicity** drop-down list, select how often you want to post the digest.

- **Daily**. If you want to post the digest daily, select this and set the date and time to post the digest.
- **Weekly**. If you want to post the digest weekly, select this and set the date and time to post the digest.
- **Bi-Weekly**. If you want to post the digest every two weeks, select this and set the date and time to post the digest.
- **Monthly**. If you want to post the digest monthly, select this and set the date and time to post the digest.
- **User-defined**. If you want to post the digest every nn days, select this and enter the number of days. This affects both how often the digest is posted and how it is rescheduled for the next posting.

- **Size-Exceeds**. To specify a size that causes the digest to be published, select this and enter the number of kilobytes. This affects both how often the digest is posted and how it is rescheduled for the next posting.
- **Manual**. If you want the digest to be posted only when you click the **Process/Send Now** button, select this.

3 The **Last Processing Date/Time** shows the date and time of the last digest posting.

4 **Next Processing Date/Time**. If the next digest has been scheduled, the next date and time is shown. If date and time are blank, then enter the desired next processing date and time and these values will be updated after the next digest is posted.

5 Click **Process/Send Now** at any time to post the digest now and reschedule according to the selected periodicity.

6 Click **Apply** to save your settings.

Adding and Removing Subscribers and Unknown Users

Using IMail Administrator (not Web Messaging or the Web Remote Administration Utility), a list administrator can create special aliases that:

- Subscribe the sender of a mail message to a list
- Remove the sender of a mail message from a list
- Remove unknown users from a list

Once these aliases are created, mail can be forwarded to one of these aliases to accomplish the desired task.

Setting Up an Alias to Remove an Unknown User

If you get “unknown user” or “unknown host” messages about supposed subscribers to a list, you can create an alias to remove such users from a list.

To set up a special alias for removing unknown users or hosts:

1 In IMail Administrator, expand a mail host folder and select the **“Aliases”** folder.

2 Click the **Add Alias** button. In the “New Alias” dialog box:

- Enter an alias name, for example: *Parrots_del*
- Select the **Program** alias type.
- Click **OK**.

3 On the **General** tab, in the **Resolves To** box, enter the alias properties using the following format:

```
imailsrv -ruhost domain listname
```

For example, suppose you create a program alias *Unknown_del* that resolves to:

```
imailsrv -ruhost exoticbirds.com Parrotlist
```

You can then forward a message about an unknown user or unknown host to *Parrots_del@exoticbirds.com*; the user specified in the **Reply-To** header (or the **From** header if **Reply-To** is not found) of the forwarded message is removed from *Parrotlist*. (The body of the message is ignored.)

Note

The message must be forwarded unmodified (with the headers unchanged), otherwise the forwarder will add himself to the list. Confirmations of the addition of the newly-subscribed user to the list are sent to both the list owner (or moderator) and the newly-subscribed user.

Setting Up an Alias to Delete a User by Forwarding

To set up a special alias for deleting a user by forwarding a message:

1 In IMail Administrator, expand a mail host folder and select the **Aliases** folder.

2 Click the **Add Alias** button. In the “New Alias” dialog box:

- Enter an alias name, for example: Parrot_del
- Select the **Program** alias type.
- Click **O**K.

3 On the **General** tab, in the **Resolves To** box, enter the alias properties using the following format:

```
imailsrv -remove domain listname
```

For example, suppose you create a program alias *Parrot_del* that resolves to:

```
imailsrv -remove exoticbirds.com Parrotlist
```

You can then forward a message from anyone to *Parrots_del@exoticbirds.co*m; the user specified in the **Reply-To** header (or the **From** header if **Reply-To** is not found) of the forwarded message is removed from *Parrotlis*t. (The body of the message is ignored.).

Note

The message must be forwarded unmodified (with the headers unchanged), otherwise the forwarder will remove herself from the list. A message is sent to the list owner (or moderator) to verify the removal of the user. When adding a user, a verification message is also sent to the subscriber.

Chapter 18: Sending Mail to a Pager or Beeper

In IMail Server, you use an alias to forward mail to a pager, or to notify you by beeper that mail has arrived.

To forward mail to a pager, you can create an alias named something like “PageFred” and define a pager ID and phone number for the alias. Users can then address mail to the alias “PageFred” and the IMail Server routes the message to the specified pager. After the alias is set up, anyone can send a message to a pager by entering the specified alias in the “To:” field of the message. The pager will receive up to the number of characters specified in the **Maximum Size** box (200 characters is both the default and the maximum).

To send a notification to a beeper that mail has arrived, you can create an alias named something like “BeepFred” and define a pager ID and phone number for the alias. After the alias is set up, when anyone sends a mail message to “BeepFred,” the predefined beeper code is sent to the beeper, alerting the recipient that they have received a new mail message.

Adding a Beeper or Pager Alias

To create a new alias for a beeper or pager:

1 Expand a mail host and then select the “**Aliases**” folder.

2 Click the **Add Alias** button.

3 Enter a name for the Beeper or Pager alias.

4 Click **Beeper/Pager**.

5 Click **OK**.

6 The “Pager Definition” dialog box appears.

7 Select the alias type: **Pager** or **Beeper**.

If you selected **Pager**, follow the steps under “Defining a Pager Alias” below. If you selected **Beeper**, follow the steps under “Defining a Beeper Alias” below.

Defining a Pager Alias

Fill in the dialog box as follows:

1 Enter the **Phone** number to dial.

2 Enter the **Password**, if required.

3 Enter the **Pager ID** (pager identification number).

4 The pager will receive up to the number of characters specified in the **Maximum Size** box (200 characters is the maximum as well as the default).

5 Select the **Parity**. The TAP protocol requires the 7E1 setting, but select 8N1 if that's what your pager uses.

6 Select the **Protocol**.

7 Select the **COM Port** (the port to which your modem is attached).

8 Select the **Baud Rate** (the speed measured in bits per second) at which the serial port will communicate with the modem).

9 Click **OK**.

Defining a Beeper Alias

Fill in the dialog box as follows:

1 Enter the **Phone Number** to dial.

2 Enter the **Numeric** code, if required.

3 Select the **COM Port** (the port to which your modem is attached).

4 Select the **Baud Rate** (the speed measured in bits per second) at which the serial port will communicate with the modem).

5 Click **OK**.

To modify an alias for a beeper or pager, select the beeper or pager alias in the list and make any necessary changes.

To delete an alias for a beeper or pager, select the beeper or pager alias in the list, right click and select **Delete**.

Sending a Message to a Pager/Beeper

You can use a pager or beeper alias as a forwarding address for a user ID. (You will enter the beeper or pager alias name in the **Forward** box on the **General** tab of the user properties.) Then, when the user ID receives mail, the pager or beeper is activated.

"Forwarding" a Message to a Pager

After a pager alias is set up, anyone can send a message to the pager by entering the specified alias in the To: field of an e-mail message. The pager will receive up to the **Maximum Size** (number of characters) of the mail message.

To have IMail Server automatically forward a user's mail to a pager:

1 Set up a pager alias as described in "Adding a Beeper or Pager Alias" on page 235.

2 Expand the mail host and "**Users**" folder, and then select the user whose mail you want to forward to a pager.

3 On the user's **General** tab, enter the pager alias as a complete mail address (in the form *userid@domain.com*) in the **Forward** text box.

   (Optional) To leave a copy of each message in the user's mailbox *and* forward a copy to a pager, precede the address with a period and comma (.,) using the format:

   ```
   .,userid@host.domain
   ```

Note

If you forward to a pager, be sure you don't have the pager alias set up to send a copy of the message to the user's account, or else the message will get into a loop between the user account and the pager.

Sending a Message to a Beeper When Mail Arrives

If a user sends a mail message to an alias defined for a beeper, the predefined beeper code is sent to the beeper, alerting the recipient that they have received a new mail message.

To automatically beep a user when an e-mail arrives for that user:

1 Set up a beeper alias as described in “Adding a Beeper or Pager Alias” on page 235.

2 Then, on the user’s **General** tab, enter the beeper alias as a complete mail address (in the form *beeper_alias@domain.com*) in the **Forward** text box. Precede the address with a period and comma (.,) using the format:

```
.,userid@host.domain
```

Note

You *must* enter the period and comma in order to leave a copy of each message in the user’s mailbox. Otherwise, the user will just get the beeper notice that mail has arrived, but he won’t get the mail.

Chapter 19: IMail Administrator Remote Connection Capability

IMail Server's remote administration feature, allows administrators to connect to another IMail 7 server to perform maintenance. With this feature an administrator is able to connect directly to a remote IMail Administrator console, enabling them to perform all of the same functions that are available on their local machine.

Requirements for Connection

In order to use the IMail Administrator remote connection feature, the following conditions must be met:

- Both the local and remote machines MUST be running IMail Server Version 7.0.
- The remote machine MUST have the Password server running and set to the correct port.
- The User must be enabled as an IMail System Administrator.

Password Server Setup

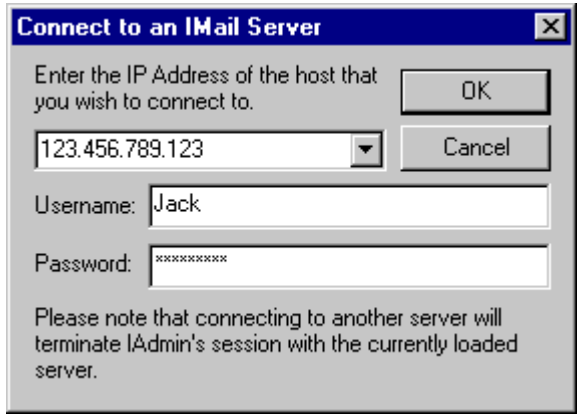
In order to connect to a remote server, the Password server must be running on the remote machine. The Password server will bind to port 8399 (along with 106) to listen for remote connections.

Connecting to a Remote Server

To connect to a remote server complete the following steps:

1 First ensure that the password server is running on the remote IMail server.

2 From IMail Administrator's **File** menu, select **Connect**. The remote connection dialog appears.



3 Enter the IP Address of the host that you wish to connect to. This must be the IP Address of the remote host, not the computer name.

4 IMail Server stores the IP Addresses that you enter, so that on subsequent connections, you can select an address from the drop down list box.

5 Enter your IMail Sever Username and password, and click **OK**.

The IMail Administrator interface for your local server will be closed and replaced by the interface for the remote server. Note that you cannot have two IMail Administrator sessions open at the same time. Therefore, be aware that connecting to a remote server will terminate IMail Administrator's session with the currently loaded server. However, if you do connect to another server, you can always connect back later.

Connecting Back to the Local Machine

To connect back to your local server, complete the following steps:

1 From IMail Administrator's **File** menu, select **Connect**.

2 Enter the IP Address of your local machine. You must enter the IP Address, not 127.0.0.1 or "localhost".

3 Enter your IMail Server Username and password, and click **OK**.

The IMail Administrator interface for the remote server will close and be replaced by the interface for your local server.

Chapter 20: Mail to Fax

You can purchase the Mail to Fax option as a separate add-on capability to IMail Server.

The Mail to Fax application lets you set up mail accounts that can receive mail from a mail client and forward it to a fax machine. For example, you can create an alias named “FaxHome” and define a phone number for the alias. Users can then address mail to “FaxHome” and the IMail Server will route the message to the specified fax.

The Mail to Fax option also supports “dynamic dialing,” which lets users enter a fax phone number when they create the mail message.

Installing IMail Fax Support

To install IMail Fax Support:

1 Log on as System Administrator or to an account that has System Administrator privileges.

2 Insert the IMail Fax Support diskette in a diskette drive.

3 Select **Run** from the **File** or **Start** menu, and then enter the diskette path followed by *install.exe*. For example:

```
a:install.exe
```

The IMail Fax Support installation wizard appears.

4 Click **Next** to display the installation options.

5 Select **Install** for a new installation or **Upgrade** if you are upgrading a previous installation.

6 Click **Next**. The setup program installs the IMail Fax Support files and creates an icon for the IMail Fax Support program in the IMail directory.

7 Click **Finish** to exit the installation program.

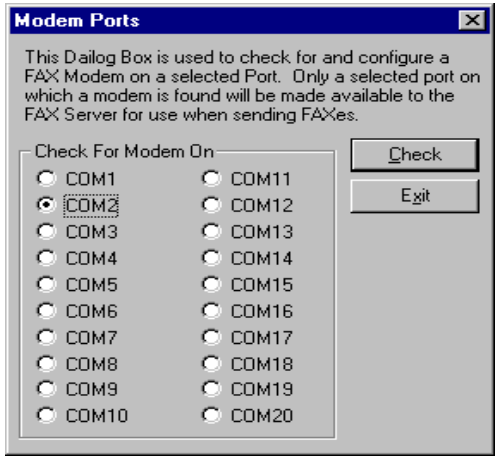
8 Connect a fax modem on the IMail Server system.

Before your IMail Server can send a mail message to a fax, you need to connect and turn on a fax modem for the IMail Server system.

Setting the Modem Port

The first time you start up IMail Fax Support, it displays a dialog that prompts you to select the modem port to which your fax modem is attached. You can also access this dialog box at any time to change the port by selecting **Ports** from the **Settings** menu.

1 In the IMail directory, double-click the IMail Fax Support icon. The Fax Server window appears and displays the Modem Ports dialog box.



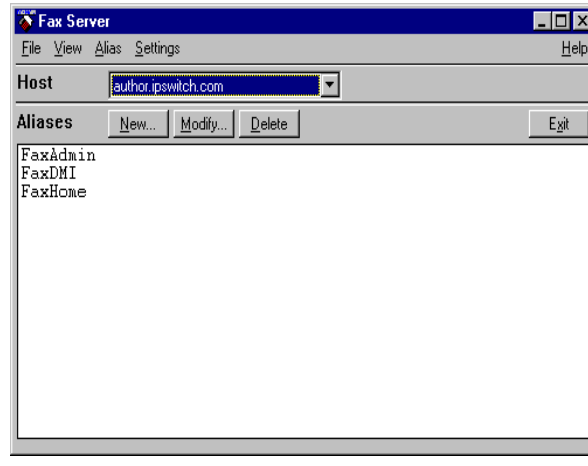
2 Select the port to which your fax modem is attached, and then click the **Check** button.

The IMail Fax Support program checks to make sure a fax modem is available on the port. If a fax modem is not connected for your IMail Server system, IMail Server cannot send mail to a fax machine.

Adding a “Mail to Fax” Alias

To add an alias for a fax:

1 In the IMail Server folder, click the IMail Fax Support icon. The Fax Server window appears.

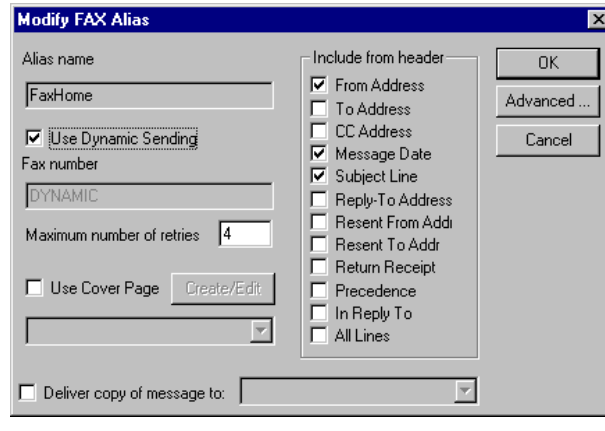


2 If you have multiple e-mail domains, select the virtual host to which you want to add the alias.

3 Click the **New** button. The New dialog box appears.

4 Enter the alias that you want users to send mail to (for fax transmission) and click **OK**.

The Modify FAX Alias dialog box appears.



5 Enter the following Mail to Fax information:

Alias name. This is the alias name you entered in the New Alias dialog box.

Fax number. Enter the phone number of the fax machine to dial when this alias receives mail.

Use Dynamic Sending. You use this option to make the alias a dynamic dialing alias. The **Advanced** button is used to set access to the dynamic dialing alias. For more information, see “Setting Up and Using Dynamic Dialing Aliases” on page 246.

This option is only available for the primary host. You cannot create dynamic dialing aliases on a virtual host.

Maximum number of retries. Enter the maximum number of times to retry sending the fax message when a send error (such as number busy, line error, no dial tone) is received. When maximum is reached, IMail Server stops resending and notifies the sender of the failure.

Use Cover Page. Select this option and enter or select the file name of the fax cover page that you want to send with all messages sent to the fax alias. You can click the **Create/Edit** button to use the Cover Page Editor to create or modify a fax cover page. For more information, see “Creating and Modifying Fax Cover Pages” on page 245.

Deliver copy of message to. If you want to send an e-mail copy of the fax message, check this option and enter an e-mail address. You can select local users from the drop-down list.

Include from header. Check the mail message header items that you want to include in the fax message.

6 Click **OK** to add the alias to the list.

To modify an alias for a Mail to Fax, select the alias in the list, and then click the **Modify** button.

To delete an alias for a Mail to Fax, select the alias in the list, and then click the **Delete** button.

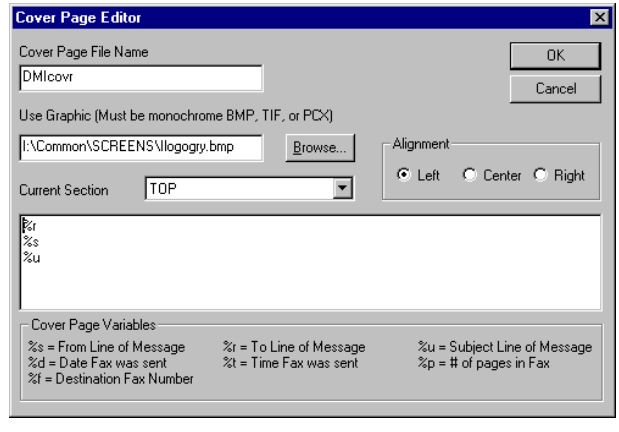
Creating and Modifying Fax Cover Pages

The Cover Page Editor provides an interface for creating and editing fax cover pages. When you define a fax alias, you can specify a cover page to be attached at the beginning of any message sent to that fax alias.

The cover page is converted to a *tif* image file before being sent to a fax machine.

To create or modify a cover page:

1 Create a new alias or modify an existing alias. The Modify Fax Alias dialog box appears.



2 Check the **Use Cover Page** option, and then click **Create/Edit**. The Cover Page Editor screen appears.

3 In the **Cover Page File Name** box, enter a name for the cover page. The file extension *.cpg* will be appended to the name you enter.

4 Optionally, in the **Use Graphic** box, enter the name of a file to be used as a background graphic on the cover page. Click **Browse** to search your system for a file.

The graphics file will be positioned in the lower left corner of the cover page. The graphic is placed in the background so that any cover page text prints over the graphic.

The graphic file must be a monochrome (black and white) *.bmp*, *.tif*, or *.pcx* file. The maximum size for the background graphic is 1728 by 1600 pixels (200 dpi vertical resolution).

5 Select the Current Section from the drop-down list, and enter the information you want to appear in that section in the edit window.

The Fax Cover Page is divided into five sections: *Top*, *Upper Middle*, *Middle*, *Lower Middle*, *Bottom*. You can enter up to five lines per section. Within a section, you can enter text or any of the cover page variables listed below the edit window.

For example, if you want the To, From, and Subject lines of the message sent to the fax alias to appear at the top of the page, select the *Top* section, and then enter the following variables in the edit window:

```
%r
%s
%u
```

Use the **Alignment** options (*Left*, *Center*, *Right*) to set how the information in the Current Section is aligned. (Note that these options do not affect the background graphic.)

6 Click **OK**. The cover page file name appears next to the **Use Cover Page** option.

Setting Up and Using Dynamic Dialing Aliases

If the host for which you are creating a Mail to Fax alias is the primary host, you can use the dynamic dialing alias option to set up an alias and let users enter the fax dial-up number when they create a mail message.

Note

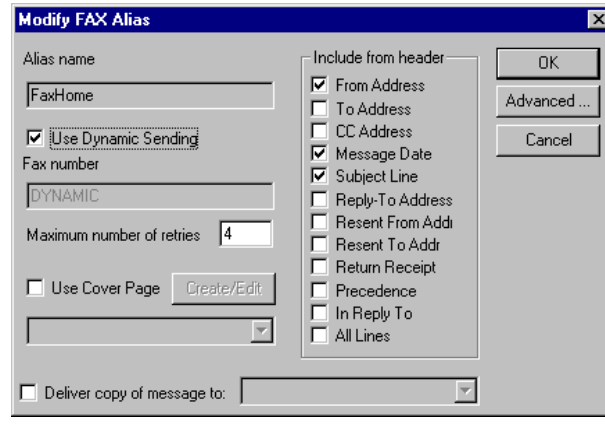
You cannot set up a dynamic dialing alias for a virtual host. Dynamic dialing can be used only on the primary host.

After you set up dynamic dialing aliases, users can create a mail message and enter the fax phone number in the subject line or in the first line of the body of the message to send mail to a particular fax.

To set up a dynamic dialing alias:

1 Create a new alias, or if you want to modify an existing alias to make it a dynamic dialing alias, select it and click **Modify**.

The "Modify Fax Alias" dialog box appears.



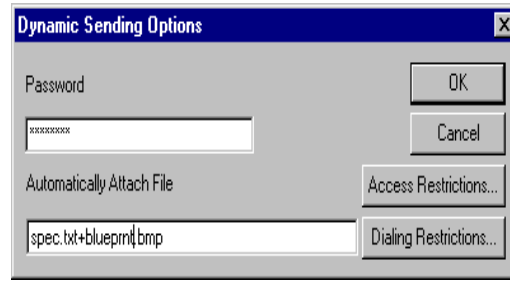
2 Check the **Use Dynamic Sending** option.

When this option is selected, users must specify a fax number in either the subject line or the first line of the body of the message using the following syntax:

`FAXNUM=`*`telephone_number`*

where FAXNUM is all capitals and there are no spaces between FAXNUM and the last digit of the specified telephone number.

3 Optionally, click the **Advanced** button and set up the fax properties to be used for this dynamic dialing alias. The Dynamic Sending Options dialog box appears.



Password. Enter a password here to restrict access to the dynamic dialing alias. Users must supply this password on the same line as the FAXNUM entry, using the following syntax:

```
PASSWD=password
```

where PASSWD is in all capitals and there are no spaces between the work PASSWD and the end of the specified password. (Spaces are used as field delimiters here).

Files to be attached. Enter the file names for any files that you want to send with every fax that is sent to this alias. You must enter the full path file name and separate multiple file names with a plus sign (+) character. No spaces are allowed in this text box.

You can use only files with the following extensions: *.bmp, .pcx, .dcx, .tif, .txt, .tmp, .fmf* and *.fmp*. Files with *.bmp, .pcx, .dcx, .tif* extensions must be monochrome graphics. Files with *.txt, .tmp* extensions must be ASCII text files. Files with *.fmf* and *.fmp* extensions are files that are already in fax format.

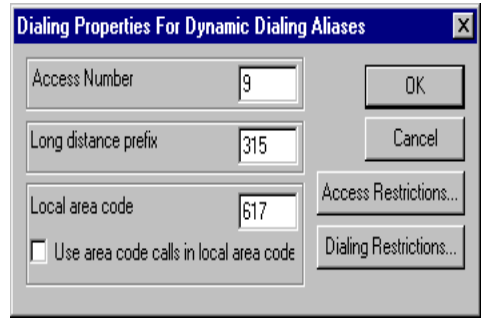
Files with extensions other than those described above will cause the entire fax to fail and an error message will be returned to the sender. If you have set this alias up to send an e-mail copy of the fax to a user mail account, the attached files will not be sent with the mail message.

You can set up **Access Restrictions** and **Dialing Restrictions** for this alias by clicking on either button. For more information, see “Setting Access and Dialing Restrictions” on page 249.

4 Click **OK** to save your changes.

Setting Global Properties for All Dynamic Aliases

There are some properties you can set up as the host default for all dynamic aliases. To display these properties, select **Dynamic Dialing** from the **Settings** menu. The “Dialing Properties for Dynamic Dialing Aliases” dialog box appears.



You can set the following global properties:

Access Number. If you have to dial an access number to get an outside line before dialing the fax number, enter it here. This number will be dialed before any number received dynamically is dialed. Note that the **Access Number** applies only to dynamic dialing aliases, you must still specify an access number within the fax phone number for non-dynamic aliases.

Long distance prefix. Enter a prefix to match against a dynamic dialing number to determine if the call is long distance or not. Dialing numbers that match any of the prefixes specified here will be denied.

Local area code. Enter a prefix to match against a dynamic dialing number to determine if the call is within the local area code. If **Use area code calls in local area code** is not selected, then area codes matching the local area code are removed from the dynamic dialing number before it is dialed. If the option is selected, then the dynamic dialing number is left intact.

Setting Access and Dialing Restrictions

You can set up access and dialing restrictions to be used as the default for all dynamic dialing aliases, or you can set restrictions on a per alias basis. Any properties set up for a particular dynamic dialing alias will override the global defaults.

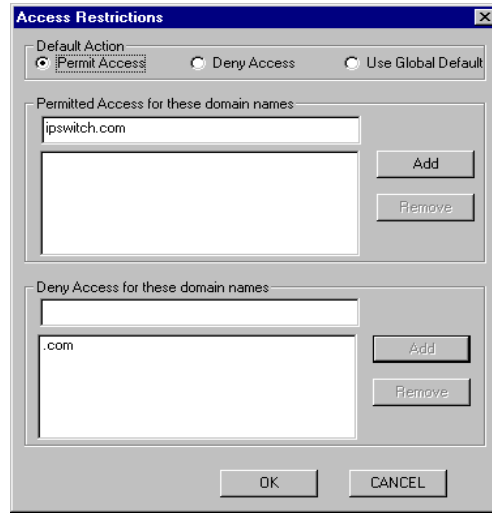
To set up restrictions for all dynamic dialing aliases, select **Dynamic Dialing** from the **Settings** menu. The Alias Properties dialog box appears. In this dialog box, you can select **Access Restrictions** and **Dialing Restrictions**.

To set up restrictions for a specific dynamic dialing alias, select the alias and click the **Modify** button. In the “Modify Fax Alias” dialog box, click the **Advanced** button. The “Dynamic Sending Options” dialog box appears. In this dialog box, you can select **Access Restrictions** and **Dialing Restrictions**.

Access Restrictions let you restrict access to dynamic aliases by setting the domain names that the alias will accept messages from or deny messages from. For example, you can enter “com” in the **Deny Access for these domain names** list to deny messages from senders in any *.com* domain, and enter *ipswitch.com* to the **Permitted Access to these domain names** list to let any senders from *ipswitch.com* send to this alias while denying all other *.com* addresses. Setting the default action will tell the server what to do with other domains, such as *.edu* or *.net*. These matches are good down the host name, but will not check user IDs.

To set access restrictions:

1 Click the **Access Restrictions** button. The “Access Restrictions” dialog box appears.



2 Add domain names to either the **Permitted Access** list or the **Denied Access** list.

To add a domain to a list, enter it in the list box, and then click **Add**. To remove a domain from the list, select it in the list, and then click **Remove**.

3 Set the default action, which tells the server how to handle any domain names not specified in the **Permitted Access** or **Deny Access** lists.

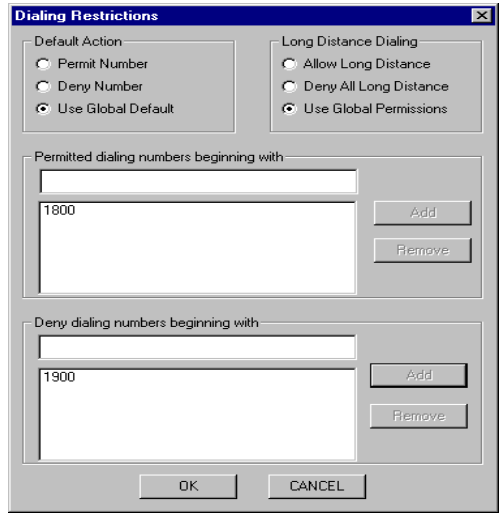
Permit Access means domain names not shown in either list are permitted access. *Deny Access* means domain names not shown in either list are denied access. **Use Global Default** (available only when setting restrictions for a specific alias) means use the global access restrictions.

4 Click **OK** to save the changes.

Dialing Restrictions let you restrict where faxes can be sent. You can specify that phone numbers beginning with a certain set of digits not be allowed. For example, you can enter 1900 to deny access to all 1-900 phone numbers. Or, you could deny access to all numbers, and allow access only to 1800 (1-800) numbers.

To set dialing restrictions:

1 Click the **Dialing Restrictions** button. The "Dialing Restrictions" dialog box appears.



2 Add phone numbers to either the **Permitted Dialing** list or the **Denied Dialing** list.

To add a phone number to a list, enter it in the list box, and then click **Add**. To remove a phone number from the list, select it in the list, and then click **Remove**.

3 Set the default action, which tells the server how to handle any phone numbers not specified in the **Permitted Dialing** or **Deny Dialing** lists.

Permit Number means phone numbers not shown in either list are permitted access. **Deny Number** means phone numbers not shown in either list are denied access. **Use Global Default** (available only when setting restrictions for a specific alias) means use the global access restrictions.

4 Set the Long Distance Dialing action.

Allow Long Distance means allow dialing of all long distance numbers. **Deny All Long Distance** means deny dialing of all long distance numbers. **Use Global Permissions** (available only when setting restrictions for a specific alias) means use the global dialing permissions.

5 Click **OK** to save the changes.

Sending Mail to a Fax Alias

After you have set up a fax alias on the IMail Server system, users can send mail from any mail client to the alias, and the mail message will automatically be routed to the fax (provided a fax modem is configured for the IMail Server system). The user needs only to specify the fax alias in the **To:** field when creating the mail message.

Attachments

Users can attach MIME-encoded and UUENCODE files to the mail message and IMail Server will translate them for fax transmission. You can use only files with the following extensions: *.bmp*, *.pcx*, *.dcx*, *.tif*, *.tmp*, *.fmf*, and *.fmp*. Files with *.bmp*, *.pcx*, and *.tif* extensions must be monochrome graphics. Files with *.txt*, *.tmp* extensions must be ASCII text files. Files with *.fmf* and *.fmp* extensions are files that are already in fax format.

If an encoded attachment has an unsupported file name, it will not be included in the fax, but a notice to this effect will appear in the text portion of the message. If an encoded attachment has a supported file name extension, but is in fact an unsupported type (i.e. a color graphic), the entire fax will fail.

Sending Mail to a Dynamic Dialing Alias

To send mail to a dynamic dialing alias, users must do the following:

- Specify the fax alias in the **To:** field when creating a message.
- Enter the fax dial-up number in the **Subject:** field or in the first line of the body of the message using the following syntax:

  `FAXNUM=telephone_number`

  where FAXNUM is all capitals and there are no spaces between FAXNUM and the last digit of the specified telephone number.
- If you created a password for the dynamic dialing alias, enter the password on the same line as the FAXNUM entry, using the following syntax:

  `PASSWD=password`

  where PASSWD is in all capitals and there are no spaces between PASSWD and the end of the specified password. (Spaces are used as field delimiters here.)

Viewing the Fax Queue Files

To view the faxes in the queue, select **Queue** from the **View** menu.

If there are faxes in the queue, you can select one to display the header information. You can select one or all faxes in the queue and select to send them. Only one instance can try to send a fax at a time, so if the fax process has already started, you will receive a message. Each time a fax is successfully sent, the current process checks the queue for another fax to send.

You can select a fax in the queue and select to remove it.

If there are no messages in the queue, a message states that there are no messages.

Appendix A. File Locking

IMail employs a built-in locking system for files in the *Spool* directory to eliminate concurrency problems. Locks are created by modifying the first character of a file name and creating a special file in the same directory as the locked file.

Files in the *Spool* directory are only locked while critical reads or writes are being performed on the file. Old locks are removed if they are more than one hour old. This means a user may be locked out of accessing a file or a service for up to one hour as a result of a system crash during a critical time period.

It is possible to manually remove a locked file if you are *positive* that no process is actually accessing that file. One reason for the long time period is to allow for the time required to transmit large files over slow links. For example, the timeout should be long enough to transmit a 2+ megabyte file across a 2400 baud dial-up connection with processing delays caused by the remote end.

Appendix B. Backups

This appendix covers how to make backups of IMail Server information.

Backing Up the IMail Server Configuration

The IMail Server configuration is saved in the registry.

Using IMail Administrator to Back Up the Registry

To perform a backup manually:

1 Select the "**localhost**" folder.

2 On the **General** tab, click the **Backup** button.

A dialog box prompts you to specify a filename to which it will back up the IMail Server section of the registry.

To restore the registry from a backup file:

1 Select the "**localhost**" folder.

2 Click the **General** tab.

3 Click the **Backup** button.

4 In the box labelled "Possible backup files…" select the backup file you want to use.

5 Click the **Restore** button.

If you restore a backup file, you will lose any changes made between the time of the backup and the time of the restore.

Using a Command Line Utility

A command line utility (regback.exe) is provided to perform the same backup described above. Its name is *regback.exe* and you can use it to perform a backup from another system, or you can use a scheduling program to run it on a regular basis.

Using Regedit

You can also back up the IMail Server registry settings by using **Regedit** to save the key HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail. This saves the system configuration settings and all user settings.

If you want to back up *only* the user settings, save the key

```
HKEY_LOCAL_MACHINE\Software\Ipswitch
       \IMail\Domains\domain_name\Users
```

Users saved in this way can be imported into *any* domain by editing the registry text file and changing the 'domain.'

Backing Up IMail Server System Files

IMail Server stores its system files in the *imail* directory (unless you gave it a different name). You can make a backup copy of the IMail Server directory tree.

Backing Up User Mail

Users' mail is stored in directories below *imail* (usually under *imail**users*, but other domains may have other directories), so daily backups should include these directories.

Appendix C. Command Line Applications

IMail Server's command line applications are useful for automating tasks that would otherwise be tedious to perform. These applications can accept input from the Windows NT Command Prompt; likewise, they send messages to the Command Prompt display.

You can run these applications in a number of ways. You can type commands at the Command Prompt, run commands in a batch file, or run commands that are saved in a text file.

Command line applications can be used in conjunction with input from a web browser. For example, a system administrator can have users fill out a web form specifying a host name; the administrator can then use a script to execute adddomain.exe to create a virtual host on the IMail Server. Or, the administrator can take text from a web form and call imail1.exe to create a mail message from the text.

This appendix covers the following IMail Server command line applications:

- *addalias.exe* - adds, modifies, and deletes aliases
- *adddomain.exe* - adds, modifies, and deletes virtual hosts
- *adduser.exe* - adds, modifies, and deletes users
- *imail1.exe* - creates a mail message
- *immsgexp.exe* - deletes old messages from a user's directory
- *ldaper.exe* - populates the LDAP database
- *mailall.exe* - sends a mail message to all users on a host
- *regback.exe* - backs up IMail registry keys
- *smtp32.exe* - delivers a message
- *isplcln.exe* - deletes old messages in the *Spool* directory

Note

In most command line utilities, you can use either a hyphen or a forward slash as a delimiter, the argument may or may not be preceded by a space, and most flags can be upper or lower case. In other words, `-hhostname`, `-h hostname`, `/hhostname`, `/h hostname`, and `-H hostname` are equivalent.

Adding Aliases (addalias.exe)

Addalias.exe is a utility for adding batches of aliases stored in a text file, or for modifying or deleting aliases on the IMail Server system. If you invoke *addalias* with no command line options (by typing only *addalias* at the MS-DOS prompt), you can manually input command lines, pressing **Enter** after each line. If you do this, press CTRL-Z to exit the utility when you are done.

Basic Command Syntax

```
addalias [-h hostname] [-cX] [-{a|d|m}] alias[=destination]
```

Argument	Explanation
-a *aliasname*	Use -a to add an alias if the alias doesn't already exist, where *aliasname* is the alias you want to add. Only one alias may be added in a single command line.
-cX	Use -c to specify to specify an alternate delimiting character. This tells Addalias to replace the default delimiter (the equal sign) with the desired delimiter. Note that a space is not allowed. (When you use -c in a text file, it affects all lines in that file.)
-d *aliasname*	Use -d to delete an alias that already exists, where *aliasname* is the alias you want to delete. Only one alias may be deleted in a single command line.
-f *filename*	You can put multiple commands into a text file for one execution of Addalias. Use -f to specify the name of the text file containing the Addalias commands. (All the above commands are valid for the text file, but note that -h and -c persist across multiple lines of input.)
-h *hostname*	Use the -h argument to specify the virtual host for the alias. The primary IMail Server host is used if no host is specified. (When you use -h in a text file, it affects all lines in that file.)
-i groupname	Use -i to import a NT group as a group alias if the alias does not already exist, where groupname is the group that you want to import. Only one alias can be added in a single command line.
-l	Use -l to list current aliases. This argument may not be used in a text file.
-m *aliasname*	Use -m to modify or add an alias even if the alias exists, where *aliasname* is the alias you want to modify. Only one alias may be modified in a single command line.
-?	Use -? to see a summary of argument options.

Adding an Alias to the Default Domain

The following examples add an alias of *newalias* to a domain named *email*.

```
addalias -c: -a newalias:email
addalias -a newalias=email
addalias -c: newalias:email
addalias newalias=email
addalias newalias email
```

Adding an Alias to a Specific Domain

The following example adds an alias of *newalias* to a domain named *email* in the host named *secondhost.com.*

```
addalias -h secondhost.com -a newalias email
```

Deleting an Alias

The following examples delete an alias.

```
addalias -d oldalias
addalias -h another.net -d alias1
```

Importing a Windows NT Group as a Group Alias

The following example converts an existing NT group into an alias.

addalias -h NThost.com -i groupname

This feature is only intended to work for local and global groups only. It is not intended to work with Microsoft Active Directory Services (ADS) "Universal" Groups.

Note: This option is only for hosts using the Windows NT database. Global groups will be ignored if the server is not a primary domain controller (PDC).

Return Codes

Addalias returns 1 if it performed at least one of the requested operations; it returns 0 if it failed.

Using a Text File

Instead of entering commands at the MS-DOS prompt, you can use a text file to input multiple commands for one execution. You can use this technique to add aliases to your IMail Server system from another mail system *if the other mail program can create a delimited text file of aliases*.

For example, you could create a text file named *test.txt* that contains the following lines.

```
test1=me
test2=test1
test3=test2
-h virtual001 test1=me
test3=me
-m test2=him
-d test3
```

At the MS-DOS prompt, you enter:

```
addalias < test.txt
```

The < symbol tells addalias to use test.txt as input.

You then get the following messages:

```
current host is mail1.ipswitch.com
added [mail1.ipswitch.com] test1 -> me
added [mail1.ipswitch.com] test2 -> test1
added [mail1.ipswitch.com] test3 -> test2
current host is virtual001
alias exists [virtual001] test1 -> someone
added [virtual001] test3 -> me
modified [virtual001] test2 -> him
deleted [virtual001] test3 -> me
```

Adding Virtual Hosts (adddomain.exe)

Addomain.exe is a utility for adding virtual hosts. It can be used to simply add a single host, but is especially useful in a batch file to add multiple hosts.

Basic Command Syntax and Example

```
 adddomain -hHostname -iIPAddress -tTopDir
     [-a Aliases -uIM | NT -x MaxMBXSize -s MaxMBXMsgs -rMaxUsers
adddomain -hHostname -m
     [-tTopDir -aAliases -xMaxMBXSize -sMaxMBXMsgs -rMaxUsers]
          adddomain -hHostname -delete
adddomain -fFilename
```

where:

-h	Fully qualified host name; if modifying must match IMail official host name
-i	IP address or VIRTUAL for IP-less host
-t	Path (full or relative to IMail TopDir) to top directory for domain

-m	Flag to modify settings instead of creating
-a	Alias list for host
-u	User data base to use (IMail or NT)
-x	Default max mailbox size (in bytes)
-s	Default max number of messages for mailbox
-f	Path to file with settings to modify/change
-r	Maximum number of users on this host
-delete	Remove virtual host

Note

AddDomain.exe does not warn when assigning already used IP addresses to new hosts. Assigning an already used IP address to another host will orphan the original host without warning.

Adding Users (adduser.exe)

Adduser.exe is a utility for adding, modifying, or deleting users, but can only be used *if the domain is based on either an IMail database or on an external database*. (*Adduser.exe* cannot be used to add users to domains which use the Windows NT database.)

You can use *adduser.exe* to add users whose user IDs and passwords are stored in a text file. Passwords must be between 3 and 30 characters.

If you invoke *adduser* with no command line options (by typing only *adduser* at the MS-DOS prompt), you can then manually input command lines, pressing **Enter** after each line. If you do this, press CTRL-Z to exit the utility when you are done.

Basic Command Syntax

```
Adduser.exe [-h hostname] [-k userid] [-m userid] [-u userid]
       [-p password] [-n name] [-f filename] [-l] [±chgpass] [±web]
        [±active] [±info]
```

Argument	When to use
-h *hostname*	Use the -h argument to specify the user's virtual host, where *hostname* is the name of the host. The primary IMail host is used if no host is specified. (When you use -h in a text file, it affects all lines in the file.)

-k *userid*	Use the -k argument to delete a user id, where *userid* is the id you want to delete. Only one user id may be deleted in a single command line.
-m *userid*	Use the -m argument to modify a user id, where *userid* is the id you want to modify. Only one user id may be modified in a single command line.
-u *userid*	Use -u to add a user id, where *userid* is the id you want to add. Only one user id may be added in a single command line.
-n *"name"*	Use -n to specify the full name of the user in double quotes. where *name* is the user's full name.
-l	Adds the reply-to address and user address to the LDAP database
-p *password*	Use -p to specify a password for the user, where *password* is the user's password. If you omit this parameter, the user's password is 'password.'
-q	Use -q to disable alias duplicate check.
-c*X*	Use -c to specify an alternate delimiting character where *X* represents the delimiting character. This tells *adduser.exe* to replace the default delimiter (a comma) with the specified delimiter. A space is not allowed. (When you use -c in a text file, it affects all lines in the file.)
-f *filename*	You can put multiple commands into a text file for one execution of *adduser.exe*. Use the -f argument to specify the name of the file containing the *adduser.exe* commands. (All commands are valid for the text file, but note that -h and -c persist across multiple lines).
-chgpass	Use -chgpass to disable the user's ability to change password.
+chgpass	Use +chgpass to enable the user to change password.
-web	Use -web to disable the user's ability to use Web Messaging.
+web	Use +web to enable the user to use Web Messaging.
-active	Use -active to disable the user's ability to log on.
+active	Use +active to enable the user to log on.
-info	Use -info to disable display of the user in whois, finger and LDAP queries.
+info	Use +info to enable display of the user in whois, finger and LDAP queries.
-?	Use -? to see a summary of argument options.
# : ;	Comments (for use in a text file)

Adding a User ID

The following examples add a user ID of *test01*.

```
Adduser -h myhost.com -u test01 -n "ms test" -p yourpass
Adduser -u test01 -n "mr test" -p nopass
Adduser -u test01
Adduser test01
```

Deleting a User ID

The following examples delete a user ID.

```
Adduser -k -u test01
Adduser -h another.net -k test01
```

Return Codes

Adduser returns 1 if it performed at least one of the requested operations; *adduser* returns 0 if it failed.

Using a Text File

Instead of entering commands at the MS-DOS prompt, you can use a text file to input multiple commands for one execution of *adduser.exe*. You can use this technique to add users to your IMail Server system from another mail system *if the other mail program can create a delimited text file of user ids, passwords, and user names*.

Let's suppose you want to add four user IDs (*userid*, *smith*, *test1*, and *jones*) to the *wks013 server. Adduser.exe* assumes that if there are no arguments in a text file, then the information on each line is userid, password, and full name – in that order.

For example, you could create a text file named *addfour.txt* that contains the following lines:

```
userid,password,full name
smith,whypass,Mrs Smith
test1,Mr Smith
jones,okpass,Tom Jones
```

At the MS-DOS prompt, you enter:

```
Adduser -h station1.ipswitch.com -f addfour.txt
```

You then get the following messages:

```
current host is wks013.augusta.ipswitch.com
OK: added userid to host station1.ipswitch.com
OK: added smith to host station1.ipswitch.com
OK: added test1 to host station1.ipswitch.com
OK: added jones to host station1.ipswitch.com
```

Note that the user named *test1* will have “password” (the default) as his password.

Disabling Web Options

New users have all the Web options enabled unless you disable one of the Web options (-/+chgpass, -/+web, -/+active, -/+info) in the command line. Modifying a user does not change the user’s Web options unless you include at least one of the Web arguments in the command line: if you include *any* web argument, then all Web options are enabled except those you specifically disable.

Sample File

```
#Entries below default to Primary domain automatically.
#Adds user test100 with password nopass, and full name Mr. Test100
test100,nopass,"Mr. test100"
#adds user test101 with password nopass, name of Ms. Test101,
#has ability to #change own password, access from web,
#account is not disabled, user info is accessible from outside.
-u test101 -p nopass -n "Ms. test101" +chgpass +web +active +info
#Add user killthisone
-u killthisone
#Remove user killthisone
-k killthisone
#Change domain(host)
-h virtual001
#Change delimiter from default(,) to a (+).
-c+
#Add user test100 with password of password and name of Mr. Test100
test100+password+"Mr. Test100"
#Modify user test100 with new name of Mrs. Test100
-m -u test100 -n "Mrs. Test100"
#Change domain(host)
-h virtual002
#Change delimiter back to default
-c,
#Add user test101 with password nopass and name Mrs. Test101
test101,nopass,"Mrs. test101"
#Add user test103 with default password, with default name test103,
has #ability to change own password, access from web, account is not
disabled, user #information is accessible from outside.
-u test103 +chgpass +web +active +info
#Add user test104 with default password, with default name test103,
has #ability to change own password, access from web, account is not
disabled, user #information is not accessible from outside.
```

```
-u test104 -chgpass +web +active -info
#Modify user test103 so user information is not accessible from
outside.
-m test103 -info
```

Results from running the above file:

```
current host is mail.some.where.com
OK: added test100 to host mail.some.where.com
OK: added test101 to host mail.some.where.com
OK: added killthisone to host mail.some.where.com
OK: User "killthisone" removed from " mail.some.where.com ".
INF: current host is virtual001
OK: added test100 to host virtual001
OK: user test100 modified in virtual001
INF: current host is virtual002
OK: added test101 to host virtual002
OK: added test103 to host virtual002
OK: added test104 to host virtual002
OK: user test103 modified in virtual002
```

Sending Mail (imail1.exe)

Imail1.exe creates and delivers mail messages to a local mailbox or to a remote host via SMTP. (SMTP delivery is accomplished by the *smtp1.exe* application.) *Imail1.exe* is similar to the UNIX *sendmail*.

Note that the message must get its body from a file. When naming files, give the complete path and filename.

Imail1.exe currently has a limitation of the body size of a created message (in the editor only) of 32K or less depending on available memory. Final message size (including attachments) is limited only by available disk space.

Imail1.exe can currently create multi-part MIME messages with Content-transfer-encoding of binary and base64 and Content-types of text, multi-part and application.

Command Syntax

Imail1.exe supports the following command line options:

-u "*userid*"	Use -u to specify the user sending the message (the **From:** field); quotation marks around the user ID are recommended.
-t "*recipient1*[,*recipient2*][,...]"	Use -t to specify primary recipients (for **To:** field).
imail1 -s "*subject*"	Specifies the subject line of the message.
-c "*recipient1*[,*recipient2*][,...]"	Specify carbon copy recipients (for the **cc:** field).

-b "*recipient1*[,*recipient1*][,...]"	Use -b to specify blind carbon copy recipients (for the **bcc:** field).
-f *filename*	The -f parameter indicates what the body of the message will be. Specify the file to send without editing (provided a recipient is also specified on the command line).
-i *filename*	-i displays an interactive Create Mail window which displays the contents of *filename* for editing.
-r	Use -r to add an Army "Registered:" header.
-a *filename*	(IMail 4.01 or later) Use -a to specify the name of file to attach (MIME format) to the message.

Deleting Old Messages (immsgexp.exe)

Immsgexp.exe is a utility that deletes messages older than a specified number of days.

Basic Command Syntax

```
immsgexp -t startdirectory -d #of_days_to_save
```

Any mailbox found beneath *startdirectory* will be scanned and any message older than *#of_days_to_save* will be deleted. A log of *exYYMMDD.log* (or *exYYMMDD.###* if *.log* already exists) will be created and log which directories/mailboxes were scanned, how many messages were deleted, and the amount of disk space saved (by file and directory).

Example

```
immsgexp -tc:\imail -d60
```

Populating the LDAP Database (ldaper.exe)

Ldaper.exe populates the LDAP database, by placing the specified information on the **General** tab of user properties into the LDAP database. This is handy when you have added a large number of users at once using *adduser.exe*.

Basic Command Syntax

```
ldaper [options]:
```

Ldaper.exe supports the following command line options. Options can be prefixed with a hyphen or a forward slash.

-H	Host name
-U	User ID
-P	Password
-GN	First name (Given Name)
-SN	Last name (Sur Name)
-S	Street address
-C	City
-ST	State
-CO	Country
-Z	Postal code
-T	Telephone
-O	Organization
-OU	Organizational Unit (Department)

Sending Mail to All Users (mailall.exe)

Mailall.exe is a command line utility that sends mail to all users on a particular host or on all hosts on the IMail Server system.

Basic Command Syntax

```
mailall -h hostname|ALL> -f sender -d [-s Subject] <FullPathToMessageFile>
```

-h *hostname* or -h ALL	The -h parameter is required. You can specify a host name or use the word ALL to specify all hosts on the IMail system.
-f *sender*	The -f parameter specifies what address appears in the **From:** field. A value is required if you are using a text file that has no **From:** header line
-s *subject*	The -s is an optional parameter that specifies the content of the Subject field.
-d	Optional. Use -d if you want the source file deleted when mailing is completed
FullPathToMessageFile	Required

Examples

```
mailall -h myhost -f admin@myhost -s"Admin note" C:\mailnotes.txt
```

The above example sends the file *mailnotes.txt* to all users on *myhost*. The message is from *admin@myhost*; the **Subject** is *Admin Note*.

```
Alias1=|mailall -h myname -d
```

The preceding example creates a program alias that is used to send mail to all users on the *myname host*. Then, you can send a message to *Alias1@myname.com*, and it will go to everyone on the *myname* host.

Backing Up IMail Server Configuration (regback.exe)

Regback.exe backs up the SOFTWARE\Ipswitch\IMail registry key and all its sub-keys.

Basic Syntax Command

regback [options]

Regback.exe supports the following command line options. Options can be prefixed with a hyphen or a forward slash.

-?	**Displays help.**
-b filename	**Backs up the registry to a file named filename.***

*The filename must be eight characters or less and can have up to a three-character file extension. Any file name or file extension exceeding the maximum number of characters will be truncated to the maximum number of characters. If a filename is omitted, regback.exe will use the default imyymmdd.reg where yymmdd is the two-digit current year, month and day.

Delivering Mail (smtp32.exe)

The *smtp32.exe* program is the SMTP send program for use with IMAIL Server SMTP Service. This program contains DNS Mail Exchanger (MX) support as well as support for list servers, etc. This program is called by *smtpd32* to do the final delivery of any received messages and to perform queue runs to clear the outbound mail queues.

Smtp32 processes messages in the *Spool* directory, attempting final delivery both to local addresses and remote addresses (by way of SMTP)

Smtp32 delivers mail only to addresses found in the *users.sys* and *aliases.sys* files. Aliases are expanded, although aliases that resolve to

file names are considered invalid and are the responsibility of the program that placed the message in the *spool* directory. (*Smtp32.exe* will expand group aliases on receipt of the message and *imail1* will expand groups on creation of a new message. Thus, it is not possible to dump a message into the queue that references a group without doing the expansion yourself.)

Smtp32 (and *imail1*) has a probable limitation of 100 recipients in a message but is determined by length of the recipient addresses, number of duplicates, etc. This is in accordance with RFC 821 section 4.5.3.

Smtp32 does not parse any headers that are contained in the message itself and expects to find properly-formatted information in the queue control file, thus there are no size restrictions on line lengths.

Whatever is passed to *smtp32* is passed along to the final system with no input checking.

Processing Rules for *smtp32* (and *imail1*)

Smtp32 and *imail1* process messages as follows:

1 Check to see if recipient host is the local host.

- If so, strip host name if present and add a host of LOCALHOST.
- If no host is specified and the user is listed in *users.sys*, set the host name to LOCALHOST.
- If the user is not listed in *users.sys*, set the host to the "Default host name."

2 Sort all recipients by host name.

3 Deliver to all local recipients.

4 If any recipients left in the list, if the **Send Direct** option is enabled, for each of the hosts, connect to that host and deliver the mail to all recipients located on that host.

- If the delivery succeeds, remove from the list.
- If the connection fails, leave in the list.

5 If any recipients left in the list, connect to the "Smart gateway" and deliver to all remaining addresses

- If the delivery succeeds, remove from the list.
- If the connection fails, leave it in the queue.

6 Return any invalid recipients to sender.

smtp32 supports the following command line options:

smtp32	With no options, *smtp32* attempts to deliver all messages in the mail queue.
smtp32 *queue_filename*	Cause *smtp32* to process the single messages pointed to by the queue_filename.
smtp32 -qr -x	Cause *smtp32* to attempt to deliver all messages in the mail queue.
smtp32 -v	Activates full display of the conversation (verbose)

Cleaning the Spool Directory (isplcln.exe)

Isplcln.exe deletes all files in the spool directory that are older than a specified number of days.

Basic Command Syntax

```
isplcln -n x -l y
```

where *x* is the number of days old a non-log file has to be before it is deleted, and *y* is the number of days old a log file has to be before it is deleted.

Note that *isplcln.exe* deletes all files in the spool directory based on the parameters supplied *without regard to whether a file is locked or not*.

Example

```
isplcln -n 5 -l 30
```

The above example deletes all non-log files that are five days old or older and delete all log files that are thirty days old or older.

Appendix D. Spool, Queue, and Log Files

The *Spool* directory is also known as "the queue," since it is the place where messages wait to be delivered. Messages in the queue include incoming messages, outgoing messages, and attachments, as well as error messages generated by IMail Server or other mail servers.

You view the files in the queue by clicking the **View Queue** button on the **General** tab (when "**localhost**" is selected in the left panel). The **Number of times** box shows the number of times IMail Server has attempted to deliver the selected message.

Also in the spool directory are the IMail Server log files.

The files in the *Spool* directory are all plain text and can be viewed using Windows Notepad. Note, however, that if you edit a D (data file) or Q file (message awaiting delivery), you *could* render the file incompatible with IMail Server.

Files in the Queue

Files in the queue are mail messages on their way in or out. When you look at the files in the queue, you can determine what stage a message is in; this is indicated by the first character in the file name and by the file extension.

Beginning Character in File Name

When an e-mail message is in the queue, it is a "data file" whose name begins with D. Data files have matching T or Q files as they get processed.

File name	Description
D*.txt	A data file in process; deleted when message is delivered.
T*.txt	A file that matches the data file while the message is inbound; when the message is fully received, the T file is renamed with a Q.
Q*.txt	A file that matches the data file while the IMail server attempts to deliver the message.

File name	Description
_*.~??	A locked file that is being processed; these files also have a tilde (~) in the file extension. (If three characters of the file name are *nex*, the file is being processed via Web Messaging or *imail1.exe*.)
F*.txt	Mail to Fax file.

Normally, messages are processed in a few seconds or a few minutes. However, if there's a problem with delivering a message, the associated files may stay in the queue longer. IMail Server automatically attempts to reprocess messages in the queue each time the **Queue Timer** reaches zero. If a message is still not delivered when the "number of tries" equals the **Number of tries** setting on the SMTP tab, the message is returned to the sender.

IMail Server does not delete the data file when a message is not deliverable, not returnable, and there is no *postmaster* alias (or there is a problem with the *postmaster* or *root* alias accounts). Thus no message is ever truly lost even if it can't be delivered to anyone.

If you happen to reboot your system while a message is being received, IMail Server *may* leave behind the T and the D files. You can use the Spool Cleaner utility to clean up files older than a certain number of days. For more information, see "Cleaning the Spool Directory (isplcln.exe)" on page 272.

File Extensions

The file extension also indicates the type of file.

- .*smd* and .*smp* file extensions indicate regular mail messages being processed by SMTP.
- .*fwd* and .*fwp* file extensions indicate forwarded messages.
- .*LST* file extensions indicate messages to subscribers of a list server mailing list.
- .*tmp* are Web Messaging, or Mail to Beeper/Pager, or Mail to Fax files.
- .*GSE* and .*GSP* file extensions indicate error messages being returned to the senders. These are usually generated by the server (*postmaster*)

Files that contain a tilde (~) in the file extension, such as *.~mp* and *.~md*, are locked files that are in process. These files also have an underscore as the first character in the file name.

Attachments

Attached files also appear in the queue. For multiple attachments, the Windows Explorer naming convention is used, so you could have *attach.txt*, *attach(1).txt*, *attach(2).txt*, and so on.

Troubleshooting

Normally, IMail Server cleans up its *.tmp* and attached files as part of the delivery process. However, as with SMTP, if there is some catastrophic failure during delivery, these files may not get deleted.

You can also run the Spool Cleaner utility to delete old files. For more information, see “Cleaning the Spool Directory (isplcln.exe)” on page 272.

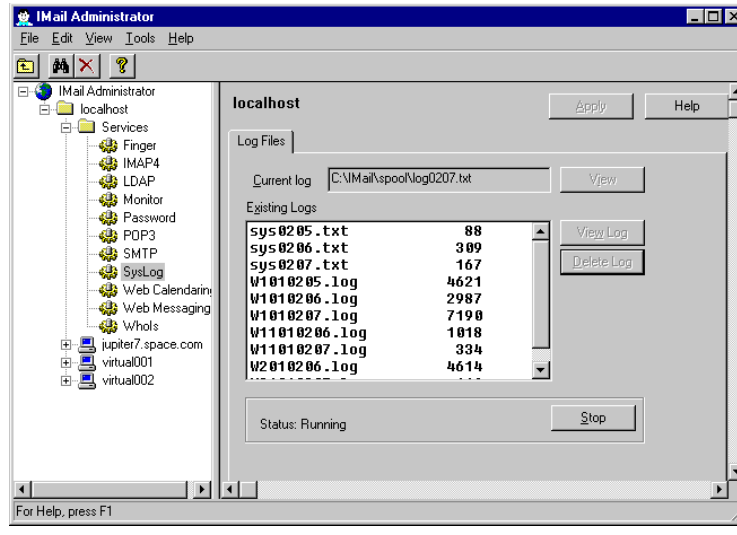
A damaged or corrupt file in the queue can prevent mail from being received correctly. If you suspect that this might be the cause of a problem you’re having, you can try moving all files from the *Spool* directory to some other temporary location (such as IMAIL\SPOOL\SAVE), and then see if you can receive mail. If you *can* receive mail, copy back pairs of files to the *Spool* directory and see if they get sent. Messages that aren’t sent *may* be damaged.

Log Files

The Log Files

Click the **Log Files** tab, when “localhost” is selected in the left panel, to display the log files in the IMail Server *Spool* directory as shown below.

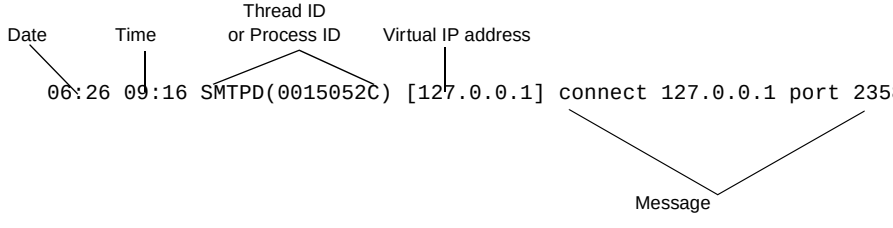
The first characters of the file name represents the type of log, and the digits represent the date.



The **Current log** box shows the currently active log file. Click **View** to view the file in the Windows Notepad.

The **Existing Logs** box lists recent log files. You can select a log file in the list and click **View Log** to open it in the Windows Notepad.

The generic format of a log file entry is



Typical Log Files

Some typical log files are the following:

- Files with names in the form of *logMMDD.txt* contain all messages sent to IMail's log server.
- File names in the form *sysMMDD.txt* are messages from IMail services.

- The *W1yymmdd.log* is the daily log file for the Web Administration server (when the Web Administration capability is enabled in the Monitor server.)
- *W2yymmdd.log* is the daily log file for the Web Messaging server.

Large Log Files

You have the following options for logging events related to IMail services (such as POP3 or IMAP4):

- **No Log**. Select this to turn off the logging of events.
- **sysMMDD.TXT**. This sends event information to a file of this name where *MM* is the month and *DD* is the day the log was written. This file is stored in the Spool directory.
- **App Log**. This sends event information to the Windows NT Application Log (viewed with the Windows NT Event Viewer.)
- **Log Server**. This sends event information to the Log Server file indicated on the **Log Files** tab.

If you have all or many of your services logging to the Log Server file, and your computer sees a lot of traffic, the Log Server file can become very large.

Disabling Logging

You can disable logging for those services where you don't need the log information. Normally, logging is only necessary if you are having problems with a service.

To disable logging:

1 Select "**localhost**" in the left panel and click the tab that corresponds to the appropriate service.

2 For each service for which you want to disable logging:

   - If you want to disable just the debug messages, turn off **Debug Messages**.
   - To disable all logging for the service, set **Log** to **No Log**.
   - Stop and restart the service to make sure the setting takes effect.

Appendix E. Default Registry Values

The following entries in the Windows NT registry are included for the benefit of system administrators. In all the examples shown, C:\IMail represents the directory where IMail Server is installed.

Global Settings

HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global

TopDir	REG_EXPAND_SZ	C:\IMAIL
CfgDir	REG_EXPAND_SZ	C:\IMAIL\cfg
SpoolDir	REG_EXPAND_SZ	C:\IMAIL\spool
UsersDir	REG_EXPAND_SZ	C:\IMAIL\users
HostName	REG_EXPAND_SZ	(full workstation name)
SendName	REG_EXPAND_SZ	C:\IMAIL\SMTP32.exe

Finger Server

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FINGRD32

DisplayName	REG_SZ	IMail FINGER Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\FINGRD32.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

The following setting is created only if you install the service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\FINGRD32\Parameters

LogLevel	REG_DWORD	0x0
Version	REG_EXPAND_SZ	(set only)

IMAP Server

HKEY_LOCAL_MACHINE_SYSTEM\CurrentControlSet\Services\EventLog\Application\IMAP4D32

EventMessageFile	REG_EXPAND_SZ	C:\IMail\mailmsg.dll
TypesSupported	REG_DWORD	0x7

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\IMAP4D32

DisplayName	REG_SZ	IMail IMAP4 Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\IMAP4D32.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

The following setting is created only if you install the service:

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\IMAP4D32\Parameters

LogLevel	REG_DWORD	0x1
IMAP4Flags	REG_DWORD	0x10
Version	REG_EXPAND_SZ	(set only)

LDAP Server

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\ILDAP

DisplayName	REG_SZ	IMail LDAP Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\ILDAP.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

The following setting is created only if you install the service:

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\ILDAP\Parameters

LogLevel	REG_DWORD	0x1
QueriesOnly	REG_DWORD	0x1
Port	REG_DWORD	0x6e(389)
Version	REG_EXPAND_SZ	(set only)

Password Server

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\PSERVE

DisplayName	REG_SZ	IMail PWD Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\PSERVE.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

The following setting is created only if you install the service:

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\PSERVE\Parameters

Version	REG_EXPAND_SZ	(set only)

POP3 Server

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\POP3D32

DisplayName	REG_SZ	IMail POP3 Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\POP3D32.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

The following setting is created only if you install the service:

HKEY_LOCAL_MACHINE_SYSTEM\SYSTEM\CurrentControlSet\Services\POP3D32\Parameters

LogLevel	REG_DWORD	0x1
POP3Flags	REG_DWORD	0x73
Version	REG_EXPAND_SZ	(set only)

SMTP Server

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Application\SMTPD32

EventMessageFile	REG_EXPAND_SZ	C:\IMail\mailmsg.dll
TypesSupported	REG_DWORD	0x7

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\SMTPD32

DisplayName	REG_SZ	IMail SMTP Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\SMTPD32.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPD32\Parameters

	Version	REG_EXPAND_SZ(set only)

Whois Server

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\WHOISD32

EventMessageFile	REG_EXPAND_SZ	C:\IMail\mailmsg.dll
TypesSupported	REG_DWORD	0x7

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WHOISD32

DisplayName	REG_SZ	IMail WHOIS Server
ErrorControl	REG_DWORD	0x1
ImagePath	REG_EXPAND_SZ	C:\IMail\WHOISD32.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x3
Type	REG_DWORD	0x10

The following setting is created only if you install the service:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WHOISD32\Parameters

Database	REG_EXPAND_SZ	C:\IMAIL\cfg\whois.db
LogLevel	REG_DWORD	0x1
Version	REG_EXPAND_SZ	(set only)

Appendix F. Special Registry Values

System administrators can use the following settings in the Windows NT/2000 registry.

Before doing any of the procedures described in this chapter, you should always back up your Windows NT/2000 registry. That way, if you make a mistake, you can restore the registry from the backup.

You can also back up your IMail Server Registry by selecting **Backup IMail Registry** from the **File** menu in IMail User Manager.

Deleting an IP Address No Longer in Use

If the IP address of your IMail Server system changes, you will need to delete the IP address that is no longer in use. To do so, you must edit the Windows NT/2000 registry.

1 Locate the following key

```
HKEY_LOCAL_MACHINE/Software/Ipswitch/IMail/Domains
```

2 You will see keys for both the old and new IP addresses. Make sure the new IP address shows the correct host name.

3 Delete the old address.

4 Highlight the host name associated with that IP address, and make sure its “Address” value is pointing to the correct (current) IP address for that host. If it is not, change it.

5 Stop and restart the SMTP server.

Appendix G. Changing the Look and Feel of Web Messaging

Each page that can be displayed in the Web Messaging interface is generated by a web template. You can edit the web templates to change the look and feel of the Web Messaging interface. If you have multiple mail hosts, each mail host can have a different Web Messaging interface.

Some examples of changes you can make are:

- You can easily change the “welcome” message and logo on the Logon page.
- You can change page background colors and styles, and button colors, styles, and labels by using the butontxt.ini file.
- You can rearrange the components of a page (such as columns, buttons, list boxes and text boxes), and move or delete functions by editing the HTML code in the web templates.
- You can use IMAIL “tags” within a template to change the display of dynamic information, such as mailboxes and messages. For a complete guide to using tags in a template, see the “IMail Server Web Messaging Templates” document (*tags.doc* file in the [*IMail top dir*]*Web* directory).

The following sections describe how the Web Messaging directories are structured and how to make changes to the interface.

Web Files and Web Directory Structure

When you install IMail Server, you can choose to install a default set of Web Messaging files in *[IMail Top Directory]\IMail\Web*). IMail Server uses this default set of files to create the Web Messaging interface for the primary mail host and for any virtual mail hosts on the server. If you upgraded from a previous Web Messaging version, see “Upgrading” on page 110.

Note

If you chose to save but not install the new IMail Web Messaging templates during the install, then the templates are located at *[IMail Top Directory]\Web\New.*

In the *Web* directory, you will see the following files:

- .html — These files are the "web templates." Each template contains the HTML code used to create a particular Web Messaging page. For example, the *login.html* file contains the code used to create the Logon page.

  For a complete list of the web templates and their associated pages in the Web Messaging interface, see "Which Pages Use Which Templates" on page 292.

- *.gif* — These files are used for graphics, such as logos, buttons, and icons. The *.gif* files are "called by" the web templates, or by a *.txt* file, where needed. Thus, you can change the look of a logo, button, or graphic throughout the Web Messaging interface by replacing the associated *.gif* file.

  For a complete list of the graphic files, see "List of graphic files in the Web Directory" on page 301.

- *.txt* — These files contain ASCII text for the Welcome message and News, as well as for any advertisements that you may have set up. The *.txt* files are "called by" the web templates where needed. You can change the text in these files.
- .cgi —These files accept and return data from the web server.
- *.jar* — These are the executable files for the IMail Web Messaging Spell Checker.

If you have one mail host or you want all your mail hosts to look the same, you can make your changes on the default files in the [*IMail Top Directory*]*\Web* directory.

Web Directories for Multiple Hosts

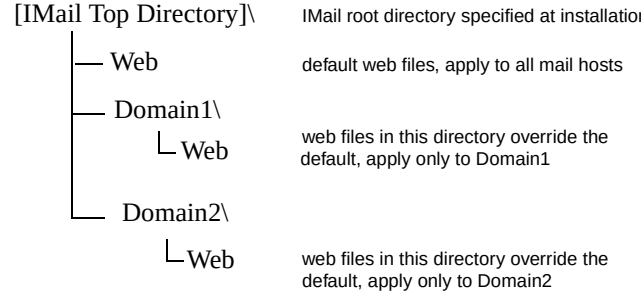
If you have multiple mail hosts on your IMail Server, you can create a web directory for each host.

You can copy a web template from the default web directory to the web directory specific for a mail host — the [*IMail Top Directory*]\[*Domain Name*]*Web*\ *directory,* and customize the template for that host only.

For example, to customize the Logon page for domain1, you copy the *login.html* file from the default web directory to the domain's web (*domain1**web*\) directory. You can then make edits to the file and save it. If the Web directory does not already exist in the domain's directory, you may need to create it. You cannot rename templates.

When a Web Messaging page is requested by the web server, the Web Messaging application reads the domain specific web directory first ([*IMail Top Directory*]\[*Domain Name*]*Web*\), then reads the default web directory ([*IMail Top Directory*]*Web*) — if a web template is found in the domain's web directory, it uses that, if not, it uses the default web template.

Directory structure for multiple mail hosts



Changing Text, Background Colors, Buttons, and Logos

You can easily change text messages, graphics, buttons, and colors on the Web Messaging interface. The following sections describe the text and graphic files in the default web directory (*[IMail Top Directory]*\ *Web*) and the changes you can make. If you have multiple mail hosts, you can copy any of the files to a mail host's web directory and

customize the file for that mail host. You can replace any of the graphics (*.gif*) files with your own *.gif* file, provided you use the same file name.

Editing the Welcome Message

The Welcome Message and a logo appear on the Web Messaging Logon page.

You can enter up to 1000 characters of plain text and/or raw HTML code in the *mailwelc.txt* file. The message displays in the Logon page above the logon box. The message persists across reboots.

You can also edit the Welcome message in the following ways:

- In the IMail Administrator — From the **Start** menu, select **Programs -> IMail -> IMail Administrator**. Select the mail host, then click the **Web Messaging Content** tab. Select *mailwelc.txt*.
- In the Web Messaging interface — To do this, log on to Web Messaging, and then under the Administration functions, click **Edit Welcome Message**.

Editing the News of the Day

The News of the Day appears after you log on to Web Messaging. If nothing is entered for the News of the Day, then the Menu page appears after log on. You can enter between 10 and 1000 characters of plain text and/or raw HTML code in the file *mailnews.txt*. The News message persists across logons.

You can also edit the News of the Day as follows:

- In the IMail Administrator — From the **Start** menu, select **Programs -> IMail -> IMail Administrator**. Select the mail host, then click the **Web Messaging Content** tab. Click the **News OTD** button.
- In the Web Messaging interface — Log on to Web Messaging, and then, under the **Administrative Account Options**, click **Edit News Message**.

Changing Button Labels

For buttons that have a *.gif* file, you can replace them with your own *.gif* file. To create your own button, you can use one of the blank button *gif* files. These files are in the IMail Top directory.

blank_button_57_24.gif (small button: height 57 pixels, width 24)

blank_button_74_24.gif (large button: height 74 pixels, width 24)

For buttons generated by the browser, you can change the text label on a button by editing its label in the *butontxt.ini* file, which is in IMail Top Directory.

Using the *butontxt.ini* file, you can easily edit buttons and links. For more information see “Customization Using the butontxt.ini File” on page 289.

Note

If you have multiple mail hosts, you can copy a *.gif* file or *butontxt.ini* to any mail host’s web directory and change the file for that mail host.

Customization Using the *butontxt.ini* File

The butontxt.ini file can be used to rename a button or link without having to edit every location where that button or link is displayed. Simply make the changes in this file, and the change will automatically occur wherever the IMail tag is being called.

For example, the following line can be found in the *butontxt.ini* file:

RemoveButton=Remove

This tag <!--IMAIL.RemoveButton--> is used on the compose page of Web Messaging. When this tag is parsed by the server, it will replace the tag with the data found in the *butontxt.ini* file. In this case the tag would be replaced with the word “Remove”.

Changing Text in Messages

You can change the text shown in some of the confirmation and error messages generated by Web Messaging. The messages that you can change are in the *message.ini* file, in *[IMail Top Directory]*. Like the *butontxt.ini* file, phrases can be modified within *message.ini*, and the changes will affect every occurrence of the respective IMail tag.

Using Files with Multiple Hosts

If you have multiple mail hosts, you can copy any of the text, graphics, or .ini files to a mail host’s web directory and customize the file for that mail host.

Editing Web Templates

Web Messaging pages are compiled from "templates" that contain HTML code and JavaScript code. The JavaScript code runs internal processing and we recommend that you do not change this code.

Before you edit a web template, you should be aware of:

- The structure of the web directories and how templates in the web directories are processed (see "Web Files and Web Directory Structure" on page 285).
- How IMAIL "tags" are used in templates (see "IMail Tags" on page 298).

Web Templates and Their Associated Web Pages

Each page in the Web Messaging interface has an associated web template that is used to generate that page. For example, the Logon page is generated by the *login.html* template and the Address Book page is generated by the *ab.html* template.

You can view and edit the HTML code for a web template by:

- Opening the template in a text editor.

  We do not recommend using a WSYWIG editor (such as Microsoft's FrontPage) because it may alter the special tags used in the templates.

- From the **Start** menu, select **Programs -> IMail -> IMail Administrator**. Then, select a mail host and click the **Web Messaging Content** tab. Select a file, and then click **Edit**.

Note

The primary mail host has the default web files. Each mail host can have its customized Web Messaging interface. For more information, see "Web Directories for Multiple Hosts" on page 287.

You can view a Web Messaging page by:

- Logging on to Web Messaging and selecting the menu option that displays the particular page.

- Using Windows Explorer, go to the *[IMail Top Directory]\Web* directory and double-click the web template. The file opens in a web browser. This will show you the pre-compiled version of the web page. It can be useful for getting a quick view of the page components. (Note that you must have your Windows NT/2000 file associations set to open HTML files in your browser.)

See “Which Pages Use Which Templates” on page 292 for a list of all the web templates and their associated web pages.

Customizing a Web Page

To customize a web page for a mail host, you must edit the associated template in the host’s web directory.

1 In **IMail Administrator**, select a mail host and click the **Web Messaging Content** tab.

Note

The primary mail host holds the default templates. Any template in the primary host’s *Web* folder applies to all mail hosts on your IMail Server. If you want to customize a template for a mail host, you need to copy (using Windows Explorer or click **Get Default**) the template from the primary mail hosts’s folder to the other mail host’s folder, and edit it there.

---

2 If the folder is empty (no + sign), click **Get Default** to copy all templates and files to this mail host’s folder. In the mail host’s folder, you can delete any templates that you will not customize.

3 Select the template for the page you want to customize and click **Edit**. The template opens in Windows Notepad. You can then directly edit the HTML code in the template. You can change the default editor so that when you open a template, it opens in a different editor.

Note

When you click on **Get Default**, all files are copied into the mail host’s folder. However, only HTML and .txt files will be displayed in IMail Administrator for editing.

---

4 When you have completed your changes, save the template in the mail host’s folder.

Which Pages Use Which Templates

The following tables list each web template and its corresponding Web Messaging page. The tables categorize the templates by their Web Messaging function as follows:

E-Mail pages — includes templates for the logon, compose message, read mail, and mail summary pages.

Personal information pages — includes templates for the address book, mailboxes, preferences, vacation and finger messages, mail forwarding, changing password, and other user information pages.

Administration pages — includes templates that create the pages used by list, host, and system administrators for remote administration of mail hosts, users, aliases, and lists.

Online help pages — help for the Web Messaging functions. If you customize the interface, you can modify these help files.

E-mail Web Pages

These templates create the web pages that users see when performing mail functions.

Template	Web page
autoresp.html	Autoresponse message
dispuser.html	Display the user information and mailbox summary
draft.html	Displays saved (draft) mail message for editing, sending.
fwdmsg1.html	Forward a message
login.html	Logon screen .
logout.html	Page displayed on logging out.
menu.html	Main menu page, shows all mailboxes and options
mntlst.html	Administration of list server mailing lists
msgsum.html	Message summary for mailbox
readmail.html	Page for reading a message
replymsg1.html	Form for replying to a message when Reply or Reply All button is clicked.
search.html	Form for searching for a message.
sendmail.html	Form for sending a message.
sysstat.html	Displays system statistics
userstat.html	Displays user account statistics

Status and error pages:	
badact.html	Displayed when the server process is interrupted due to a user action.
badreqst.html	
delconfirm.html	Prompts to confirm deletion of message.
disableaccount.html	Displayed when an account has been disabled
disabledlist.html	Displays the disabled users for a domain
fwdmsg.html	When forwarding, displays error condition when a message number is wrong or mailbox is invalid. Otherwise, fwdmsg1.html is used.
msgdel.html	Shows results of a message delete
msgmove.html	Shows status of a moved message
psearch.html	Shows the results of a search of a mailbox
psndmail.html	Shows status of sent mail
readfail.html	If user tries to read an empty mailbox, shows this page
replymsg.html	When replying to a message, shows this page if the message number is wrong, or the mailbox is invalid; otherwise, uses replymsg1.html.
suspendaccount.html	Displayed when an account has been suspended
unlock.html	Shows the status of an unlocked mailbox

Personal Information Web Templates

These templates create the web pages that users see when changing personal information related to their account, such as mail forwarding, vacation messages, and delivery rules for incoming mail.

Template	Web form
ab.html	Address Book
addrule.html	Add or change the user's rules for filtering mail
chgfwd.html	Change the user's mail forwarding
chgldap.html	Change the users's LDAP user information
chgpass.html	Form that allows users to change their password
chgplan.html	Change the user's Finger information
chgrule.html	Change the user's incoming mail delivery rules
chguser.html	Change the user's name, mailbox size, etc.
chgvac.html	Change the user's vacation message
editrule.html	Edits an inbound rule for a user
modrule.html	Modify a user's mail processing rule

pchgplan	Change Finger information or status
pchguser	Change user status
pref.html	Form for setting user preferences.
subfold.html	Form for managing folders (mailboxes) – used to create, rename, and delete mailboxes.
viewvac.html	Form for viewing vacation message recipients.
Status and error Pages	
pchgauto.html	Shows the status after a user changes their autoresponse message
pchgfwd.html	Shows the status after a user changes their mail forwarding information
pchgldap.html	Shows the status after a user changes their LDAP information
pchgpass.html	Shows the status after a user changes their password
pchgsign.html	Shows status after a user changes their signature file
pchgvac.html	Shows the status after a user changes their vacation message
plogin.html	Shows the user logon status

Administrator Web Templates

These templates create the web pages used for remote administration of mail hosts, users, aliases, and lists.

Template	Web form
addalias.html	Add a new alias
addhostrule.html	Add or change a mail host's rules for filtering mail
addoutrule.html	Add an outbound delivery rule for a mail host.
adduser.html	Add a new user
aliasadmin.html	Display list of aliases and Add, Delete, Modify buttons
aliasdisplay.html	Display information for an alias
aliasmodify.html	Modify the alias destination
avsvradm.html	Anti-Virus administration page.
chpasuad.html	Change a user's password
chghostrule.html	Overview of the delivery rules for a mail host.
chguser.html	Change the user's name, mailbox size, etc.
delalias.html	Delete Alias
dghedlst.html	Change digest header information

dgseplst.htm	Change digest separator information
dgtralst.html	Change digest trailer information
diglst.html	List digest maintenance
disabledlist.html	Displays a list of disabled users
displayuserlist.html	Displays user account information
edithostrule.html	Edits an inbound delivery rule for a host.
editlistrule.html	Edits an inbound delivery rule for a list.
editnews.html	Change the news message
editoutrule.html	Edits an outbound delivery rule for a mail host.
editwelc.html	Change the welcome message
headlist.html	Change the header.txt file for a list
helplst.html	Change the help.txt file for a list
listaddrule.html	Create a rule for a mail list
listadm.html	Display list administration functions
listchgrule	Change a rule for a mail list
listmaintain.html	Set or change list properties
listmodrule.html	Modify a rule for a mail list
mnacclog.html	Display contents of IMail Monitor Access log
mnsyslog.html	Display contents of IMail system log
mntlst.html	Display maintenance functions for a list
mntlst1.html	Set kill list parameters
mntlst2.html	Set digest parameters
modhostrule.html	Modify a mail host's mail processing rule
plfile.html	List maintenance status
shspool.html	Shows contents of the spool directory
subjlst.html	Change subject.txt file for list
subslst.html	Change subscribe.txt file for list
syntax.html	List maintenance page
syslog.html	Display contents of IMail system log
sysstat.html	Displays system statistics
traillst.html	Change trailer.txt file for list
usradmin.html	Displays list of users and Add, Modify, Delete buttons
userstat.html	Displays statistics for all users
vh.html	Display virtual host administration functions
vh_add.html	Add a virtual host
vh_modify.html	Modify a virtual host

welcome.html	Change the news message

Status and error pages	
nolist.html	Displayed if mail is sent to a list that is not valid
nolistfile	Displayed if mail is sent to an invalid list
nouser.html	Displayed if user cannot be authenticated on logon
ntaddusr.html	Displayed if user in NT database cannot be authenticated
padduser.html	Shows status after adding a user
pchgalis.html	Shows status after adding an alias
pdeluser.html	Shows status after deleting a user
pedtnews.html	Shows status after changing the news message
pedtwelc.html	Shows status after changing the welcome message
plistadm.html	Shows status after creating or updating a list
plistdig.html	Shows status after setting list digest options
plistset.html	Shows status after setting list parameters
plogin.html	Shows user logon status
plstaddr.html	Shows status after modifying, adding, or deleting a user from address list, digest address list, or kill list.
plstfile.html	Shows status after modifying list and digest related files, such as header, trailer, subject
pshspool.html	Shows status after deleting a file in the spool directory; or, shows the selected spool file
puchgpass.html	Shows status after changing password through user administration
suspendaccount	Shows that a user account has been suspended.
vaddstats.html	Shows the status after adding a virtual host
vhdelete.html	Shows status after deleting a virtual host
vmodifystatus.html	Shows the status after modifying a virtual host

Help Pages

These are the help pages for the Web Messaging functions. Files that have a *cs_* prefix are called by Help buttons on the Web Messaging pages. Files with a *t_* prefix are not called directly by buttons, but are

accessible through the Table of Contents.

Files	Web page
cs_ab.html	How to use the address book
cs_addalias.html	How to add an alias
cs_addhostrule.html	How to add a delivery rule for a host
cs_addoutrule.html	How to add an outbound delivery rule for a mail host.
cs_addrule.html	How to add or change the user's mail rules
cs_adduser.html	How administrator can add a user
cs_aliasadmin.html	Alias administration
cs_aliasmodify.html	How to modify an alias
cs_autoresp.html	How to set up an autoresponse message
cs_avsvradm.html	How to set up IMail Anti-Virus.
cs_chgfwd.html	How to change the mail forwarding address
cs_chghostrule.html	How to change a delivery rule for a host
cs_chgldap.html	How to change the user's LDAP attributes
cs_chgpass.html	How to change the user's password
cs_chgplan.html	How to change the user's Finger plan file
cs_chgrule.html	Working with inbound delivery rules for a user.
cs_chgsign.html	How to change the user's signature file
cs_chgvac.html	How to change the user's vacation message
cs_disabledlist.html	Working with suspended accounts.
cs_displayuserlist.html	How to view the user list in status of accounts
cs_edithostrule.html	How to edit an inbound delivery rule for a host.
cs_editnews.html	How to edit the news message
cs_editlistrule.html	How to edit an inbound delivery rule for a list.
cs_editoutrule.html	How to edit an outbound rule for a mail host.
cs_editrule.html	How to edit a delivery rule for a user.
cs_editwelc.html	How to edit the welcome message
cs_listaddrule.html	How to add a delivery rule for a mailing list
cs_listadm.html	How administrator can add, modify lists
cs_listchgrule.html	Working with inbound rules for a list
cs_login.html	How to logon screen
cs_menu.html	How to use mailboxes and options
cs_mnacclog.html	How to view the Monitor Access log
cs_mnsyslog.html	How to view the Monitor System log
cs_mntlst.html	How administrator can set list properties

cs_mntlst1.html	How to use the kill list
cs_mntlst2.html	How to set mailing list digest options
cs_msgsum.html	How to use the mailbox message summary
cs_nolistfile.html	How to use the No list file
cs_pref.html	How to use set user preferences
cs_readmail.html	How to read a message
cs_search.html	How to search a mailbox for a message
cs_sendmail.html	How to compose and send a message.
cs_shspool.html	How to view the spool directory
cs_spell.html	Spell Checker table of contents
cs_syntax.html	How to use the syntax file
cs_syslog.html	How to view the syslog
cs_sysstat.html	How to use system statistics
cs_systmlog.html	How to view the system log
cs_sysusradmin.html	How to use User Administration
cs_tableC.html	Table of contents
cs_userstat.html	How to read user statistics information
cs_usradmin.html	How administrator can change user properties
cs_vhadd.html	How to add a virtual host.
cs_vh_modify.html	How to modify a virtual host
cs_welcome.html	Help for Welcome page
t_*topicname*.html	Assorted help topics for Web Messaging tasks

IMail Tags

The templates used to create Web Messaging pages consist mostly of HTML code. Some templates also contain JavaScript code.

A specialized “tag” language is used within the templates to generate “dynamic” information, such as mailboxes and messages, at run-time — in other words, when a browser requests the information. You can use these tags to customize any Web Messaging page, add pages of your own, add or rename components of a page.

Tag Syntax

All tags start with the label **IMAIL**. An IMAIL tag is always embedded in the standard HTML comment tag. For example:

<**!**--IMAIL.UserID -- >

- IMAIL.TagName — This type of tag returns a value, such as the UserID of the currently logged on user, or the IMail Server host name.
- IMAIL.*TagName*.*Value* — where *TagName* is the name of the item, such as a button, hyperlink, or check box. You cannot edit the *TagName*. For text that appears on a button, the *TagName* has the suffix Button, (for example: LogonButton, SaveButton); for text that appears in a hyperlink, the suffix is Link; for simple text tags, the suffix is Text. *Value* is the actual text that appears on the button, in the hyperlink, or next to the check box. You can edit the *Value* to change the text to whatever you want

The document "IMail Server Web Messaging Templates" *(tags.doc* file in the [*IMail Top Directory*]*Web* directory), lists all IMAIL tags.

Types of Tags

You can use the tags to do the following types of operations.

- **Normal** tags return a value or values. These tags are used to build dynamic information, such as the name of the logged in user, into the web pages.
- **Conditional** tags check whether a condition is true or false, and then continue processing based on the answer. These tags use If-Then-Else constructs.
- **While** tags populate a table, such as a list of messages in a mailbox. These tags use For-Each constructs.
- **Include** tags let you name an HTML, ASP, CGI, CSS or other file to be included at the tag location. If the file extension is *.asp* or *.cgi*, then the included file will be further parsed for IMAIL tags. For example, you can use the **Include** tag to include a standard header in all files.

For a complete guide to using tags in a template, see the document "IMail Server Web Messaging Templates," (*tags.doc* file in the [*IMail Top Directory*]*Web* directory).

ParseExtensions

If you would like to parse the IMail tags for an included document, you may use ParseExtensions to parse the IMail tags for any included file, regardless of its file extension. This is useful for people who are unable to manually change the file extension. Note that this feature works when you use the IMail “include” tag. You can now use the IMail “include” tag to parse whatever file extension that is listed in the registry. For example, the following IMail tags can be made valid by using ParseExtensions:

<!--IMAIL.Include filename.asp-->

<!-- IMAIL.Include filename.cgi-->

<!--IMAIL.Include filename.js-->

<!--IMAIL.Include filname.txt-->

Basically, this feature allows you to control whether the IMail tags are parsed for an included document (of a specific file extension), or wether the IMail tags are simply displayed.

ParseExtensions Directory Location

The ParseExtensions REG_MULTI_SZ value goes in the following registry location:
[HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global]

If ParseExtensions does not exist in the registry, the IMail “include” tag will parse files with the following extensions automatically, allowing IMail tags to be executed within the given file: cgi, asp, htm and html.

All other file extensions will be parsed, however, the IMail tags will be displayed as written and NOT executed. The IMail “include” tag will also parse all file extensions, but it will NOT execute the IMail tags within these files.

If ParseExtensions is located in the registry but does not contain any file extensions, the IMail “include” tag will parse all file extensions given to the tag. It will also execute all IMail tags found within the parsed file.

Adding ParseExtensions to the Registry

To add ParseExtensions to the registry, do the following:

1 Launch the “Run” command line.

2 Type “regedt32” and press **Enter** on the keyboard.

3 Go to the following registry location:

[HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global]

4 Add a value of ParseExtensions, with type, REG_MULTI_SZ

5 Enter the extensions of the files, which you want to have executable IMail tags, into the textbox without any delimiters. For example, if you would like to only parse the IMail tags for CGI, HTML, and ASP files, enter the desired extensions on each line.

Each extension should occupy its own line as follows:

cgi

html

asp

6 In order for the changes to take effect, you must restart Web Messaging.

Note

Only the file extensions listed will have the ability to execute IMail tags when included in a document via the IMail “include” tag.

List of graphic files in the Web Directory

The following table lists the default graphic files and indicates where they are used in the Web Messaging interface. Most of these *.gif* files represent buttons used in Web Messaging pages.

Graphic	Where used
ascend.gif	Icon that indicates a column is in ascending order
att_new.gif	Icon that indicates a new message with an attachment
attach.gif	Icon that indicates a read message with an attachment
blank_button_57_24.gif	Blank button sized 57 by 24 pixels. For use in creating new buttons

blank_button_74_24.gif	Blank button sized 74 by 24 pixels. For use in creating new buttons
bottom.gif	Arrow icon moves to the bottom of the mailbox summary page
checked.gif	A checked selection box
contentsbtn.jpg	The contents button for the Spell Checker
descend.btn	Icon that indicates a column is in descending order
del.gif	Trashcan Icon used for deletion
downrule.gif	Icon that moves a delivery rule down in the list
down.gif	IMonitor Icon for a down service.
edit.gif	Pencil icon that allows you to edit
forward.gif	
imailc.gif	Logo on Logon page; called from mailwelc.txt
ipswitch.gif	The Ipswitch logo
mail.gif	Icon that indicates a read message
mail_new.gif	Icon that indicates a new (unread) mail message
mail.gif	Icon that indicates a mail message has been read
movedown.gif	Moves a condition down in the processing order
moveup.gif	Moves a condition up in the processing order.
replied.gif	Icon that indicates a message has been replied to
spell.gif	Icon for the Spell Checker
ssl-key.gif	Keys logo shows SSL is not in use
ssl-lock.gif	Lock logo that signifies SSL is in use
up.gif	Used by IMonitor to report an up condition
top.gif	Arrow icon that moves to the top of the mailbox summary page
unchecked.gif	An unchecked selection box
uparrow.gif	Up arrow
uprule.gif	Icon that moves a delivery rule up in the list
urgent.gif	Icon that identifies an urgent message
xlinex.jpg	Help file example of X-IMail-Rule header.

Appendix H. Changing the Look and Feel of Web Calendaring

Each page that can be displayed in the IMail Web Calendaring interface is generated by a web template. You can edit the web templates to change the look and feel of the interface. If you have multiple mail hosts, each mail host can have a different IMail Web Calendaring interface.

Some examples of changes you can make are:

- By editing HTML code in the templates, you can change page background colors, button colors, and labels as well as rearrange the components of a page (such as columns, buttons, list boxes and text boxes), and move or delete functions by editing the web templates used to generate the web pages.
- You can use calendar "tags" within a template to change the display of dynamic information, such as calendar view. For a complete guide to using tags in a template, see the "Calendar HTML Template Document" (*iwebcaltags.doc* file in the [*IMail top dir*]*\Web\Calendar* directory).

The following sections describe how the IMail Web Calendaring directories are structured and how to make changes to the interface.

Web Files and Web Directory Structure

When you install IMail Server, you can choose to install a default set of IMail Web Calendaring files in the Calendar folder of the IMail top directory *[IMail Top Directory]\IMail\Web\Calendar.* IMail Server uses this default set of files to create the IMail Web Calendaring interface for the primary mail host and for any virtual hosts on the server. In the *Calendar* directory, you will see the following files:

- .html — These files are the "web templates." Each template contains the HTML code used to create a particular Web Calendaring page. For example, the *login.html* file contains the code used to create the Logon page.

For a complete list of the web templates and their associated pages in the IMail Web Calendaring interface, see “Which Pages Use Which Templates” on page 308.

- *.gif* — These files are used for graphics, such as logos, buttons, and icons. The *.gif* files are “called by” the web templates, or by a *.txt* file, where needed. Thus, you can change the look of a logo, button, or graphic throughout the IMail Web Calendaring interface by replacing the associated *.gif* file.

  For a complete list of the graphic files, see “List of Graphic Files in the Web Directory” on page 312.

- *.cgi* —These files accept and return data from the web server.
- *.txt* — This file contains ASCII text for advertisements and for the News of the Day. The *.txt* file is “called by” the web templates where needed. The text in this file can be changed as needed.

If you have one mail host or you want all your mail hosts to look the same, you can make your changes on the default files in the [*IMail Top Directory*]*Web**Calendar* directory.

Note

If you installed a beta version of IMail Web Calendaring, and then installed version 7.0 the default Web Calendaring files may be located in *[IMail Top Directory]\Web\New.* This is an option that is selected during the install to prevent overwriting customized web templates.

Web Directories for Multiple Hosts

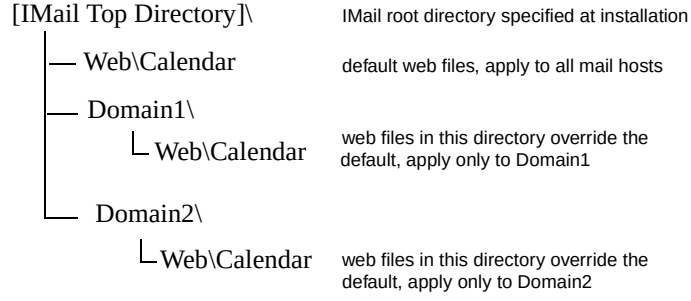
If you have multiple mail hosts on your IMail Server, you can create a Web\Calendar directory for each host.

You can copy a web template from the default web directory to the web directory for a specific mail host — the [*IMail Top Directory*]\[*Domain Name*]*Web**Calendar* directory, and customize the template for that host only.

For example, to customize the Login page for domain1, you copy the *login.html* file from the default web directory to the domain’s web (*domain1**web**calendar*) directory. You can then make edits to the file and save it. If the Web directory does not already exist in the domain’s directory, you may need to create it. You cannot rename templates.

When an IMail Web Calendaring page is requested by the web server, the calendar application reads the domain specific web directory first ([*IMail Top Directory*]\[*Domain Name*]*Web**Calendar*). It then reads the default directory ([*IMail Top Directory*]*Web**Calendar*) and if a web template is found in the domain's web directory, it uses it. If no web template is found, it uses the default web template

Calendaring directory structure for multiple mail hosts



Changing Text, Background Colors, Buttons, and Logos

You can easily change text messages, graphics, buttons, links, and colors on the Web Calendaring interface. The following sections describe the text and graphic files in the default calendar directory (*[IMail Top Directory]*\ *Web**Calendar*) and the changes you can make. If you have multiple mail hosts, you can copy any of the files to a mail host's web directory and customize the file for that mail host. You can also replace any of the graphics (*.gif*) files with your own *.gif* file, provided you use the same file name.

Editing the News of the Day

The News of the Day appears after you log on to Web Calendaring. If nothing is entered for the News of the Day, then the Menu page appears after log on. You can enter between 10 and 1000 characters of plain text and/or raw HTML code in the file *mailnews.txt*. The News message persists across logons.

You can also edit the News of the Day as follows:

- In the IMail Administrator — From the **Start** menu, select **Programs -> IMail -> IMail Administrator**. Select the mail host, then click the **Web Calendaring Content** tab. Click the **News OTD** button.

Changing Buttons

For buttons that have a *.gif* file, which includes most of the buttons in the interface, you can replace them with your own *.gif* file. To create your own button, you can use one of the blank button *gif* files. These files are in *[IMail Top directory]/Web*:

blank_button_57_24.gif (small button: height 57 pixels, width 24)

blank_button_74_24.gif (large button: height 74 pixels, width 24)

If you have multiple mail hosts, you can copy a *.gif* file to any mail host's web directory and change the file for that mail host.

Using Files with Multiple Hosts

If you have multiple mail hosts, you can copy any of the text, graphics, or .ini files to a mail host's web directory and customize the file for that mail host.

Editing Web Templates

IMail Web Calendaring pages are compiled from "templates" that contain HTML and JavaScript code. The JavaScript code runs internal processing and we recommend that you do not change this code.

Before you edit a web template, you should be aware of:

- The structure of the web directories and how templates in the web directories are processed (see "Web Files and Web Directory Structure" on page 303).
- How ICAL "tags" are used in templates (see "IMail Tags" on page 311).

Web Templates and Their Associated Web Pages

Each page in the Web Calendaring interface has an associated web template that is used to generate that page. For example, the Logon page is generated by the *login.html* template and the Address Book page is generated by the *addressbook.html* template.

You can view and edit the HTML code for a web template by:

- Opening the template in a text editor.

  We do not recommend using a WSYWIG editor because it may alter the special tags used in the templates.

- From the **Start** menu, select **Programs -> IMail -> IMail Administrator**. Then, select a mail host and click the **Web Calendaring Content** tab. Select a file, and then click **Edit**.

Note

The primary mail host has the default web files. Each mail host can have its customized Web Calendaring interface. For more information, see "Web Directories for Multiple Hosts" on page 304.

You can view a Web Calendaring page by:

- Logging on to Web Calendaring and selecting the menu option that displays the particular page.
- In Windows Explorer, go to the *[IMail Top Directory]\Web\Calendar* directory and double-click the web template. The file opens in a web browser. This displays the pre-compiled version of the web page. It can be useful for getting a quick view of the page components. (Note that you must have the Windows NT/2000 file associations set to open HTML files in your browser.)

See "Which Pages Use Which Templates" on page 308 for a list of all the web templates and their associated web pages.

Customizing a Web Page

To customize a web page for a mail host, you edit the associated template in the host's web directory.

1 In **IMail Administrator**, select a mail host and click the **Web Calendar Content** tab.

Note

The primary mail host holds the default templates. Any template in the primary host's *Content* folder applies to all mail hosts on your IMail Server. If you want to customize a template for a mail host, you must copy (using Windows Explorer or **Get Default**) the template from the primary hosts's folder to the other host's folder, and edit it there.

---

2 If the folder is empty (no + sign), click **Get Default** to copy all templates to this mail host's folder. In the mail host's folder, you can delete any templates that you will not customize.

3 Select the template for the page you want to customize and click **Edit**. The template opens in Windows Notepad. You can then directly edit the HTML code in the template. You can change the default editor so that when you open a template, it opens in a different editor.

Note

When you click on **Get Default**, all files are copied into the mail host's folder. However, only HTML and .txt files will be displayed in IMail Administrator for editing.

4 When you have completed your changes, save the template in the mail host folder.

Which Pages Use Which Templates

The following table lists each web template and its corresponding Web Calendar page.

Online help pages — help for the Web Calendar functions. If you customize the interface, you can modify these help files.

Calendar Web Pages

These templates create the web pages that users see when performing mail functions.

Template	Web form
addevent.html	Page for adding an event
addjournal.html	Page for adding a note
addressbook.html	Page for adding, and editing e-mail addresses used for sending reminder
addtask.html	Page for adding a task
bulkdelete.html	Page for deleting all events, tasks, and notes
cal_pref.html	Page for editing calendar preferences
createcalendar.html	Page for creating, editing, and deleting calendars
day_view.html	Displays the selected calendar day.
displayalltask.html	Task list in which all scheduled tasks are displayed

editevent.html	Page for editing an event
editIMIPRequest	Page for responding to an IMIP invitation
editjournal.html	Page for editing notes
edittask.html	Page for editing a task
invitation.html	e-mail invitation for an event
login.html	Displays the Log In page
logout.html	Displays the Log Out page
monthlyview.html	Displays the selected calendar month
receivedIMIP.html	Page that displays invitations that have been received
reminder.html	e-mail reminder for a scheduled event or task
searchresult.html	Displays the search results for scheduled events and tasks
showjournal.html	Page for displaying notes
tail.html	contains the Calendar trailer message
user_pref.html	Displays viewing and calendar preferences
view_pref.html	Page for editing calendar viewing preferences
weekview.html	Displays the calendar one week at a time
welcome.html	Displays the welcome message
yearview.html	Displays the calendar one year at a time
Status and error pages	
CalEnableError.html	There was an error in opening the calendar
createcalendarwarning.html	The current calendar does not exist
createcalfailed.html	Shows the status of a calendar creation, edit, or deletion
disableaccount.html	User account has been disabled
entrynotfound.html	Displays the status of a calendar entry not found
invalidpostaction.html	Invalid post submission to the server
nouser.html	Invalid user
plogin.html	Login failed
servererror.html	Displays a server error
suspendaccount.html	User account is suspended
usererror.html	Displays a user error
wrongversion.html	Incorrect Web Calendaring Version

Help Pages

These are help pages for the Web Calendar functions. Files that have a

*cs_* prefix are called by Help buttons on the Web Calendar pages. Files with a *t_* prefix are called from the index file, contents file, and other help topics.

Files	Web page
cs_addevent	How to add an event to the calendar
cs_addressbook	How to add an address to the address book
cs_addtask	How to add a task to the calendar
cs_cal_pref	How to change calendar viewing preferences
cs_choosing_a_calendar	How to choose a calendar from the current calendar page
cs_createcalendar	How to add a new calendar to the calendar list
cs_day_view	How to display a day view on the current calendar page
cs_deleting_addresses	How to delete an e-mail address from the address book
cs_deleting_a_calendar	How to delete a calendar from the calendar list
cs_deleting_notes	How to delete notes from the current calendar
cs_deleting_reminders	How to delete reminders from a calendar view
cs_deleting_tasks	How to delete tasks
cs_displayalltask.html	How to display all tasks in the Task List.
cs_editevent	How to edit an event on the current calendar page
cs_editing_addresses	How to edit an e-mail address in the address book
cs_editing_notes	How to edit Notes
cs_editing_reminders	How to edit an e-mail reminder for a task or an event
cs_editing_tasks	How to edit a task from the current calendar page
cs_generate_an_email_reminder	How to generate an e-mail reminder
cs_intro	Introduction to Web Calendar
cs_login	How to login to Web Calendar
cs_marking_tasks	How to mark tasks from the current calendar page
cs_monthview	How to select a monthly view of the current calendar page
cs_printing	How to print the current page
cs_printing_an_event	How to print an event
cs_printing_notes	How to print notes
cs_printing_reminders	How to print an e-mail reminder for an event or task
cs_printing_tasks	How to print a task

cs_printing_the_address_book_page	How to print an e-mail address from the address book
cs_receivedimip.html	How to view invitations that you receive from other users
cs_renaming_a_calendar	How to rename a calendar from the current calendar list
cs_searchresult.html	How to read the search results
cs_showjournal	How to add notes to the current calendar
cs_tablec.html	The Table of contents for Help topics
cs_user_pref	How to customize your calendar views
cs_view_pref	How to change your viewing preferences
cs_viewing_a_task	How to view a task
cs_viewing_an_event	How to view an event
cs_viewing_notes	How to view notes
cs_viewing_reminders	How to view e-mail reminders
cs_viewing_the_calendar	How to view the current calendar
cs_web_access	How to access Web Calendaring using a web browser
cs_weekview	How to select a weekly view of the current calendar page
cs_yearview	How to select a year view of the current calendar page
t_*topicname*.html	Assorted help topics for Web Calendar tasks

IMail Tags

The templates used to create Web Calendar pages consist mostly of HTML code. Some templates also contain JavaScript.

A specialized “tag” language is used within the templates to generate “dynamic” information, such as mailboxes and messages, at run-time — in other words, when a browser requests the information. You can use these tags to customize any Web Calendar page, add pages of your own, and add or rename components of a page.

Tag Syntax

All tags start with the label **ICAL**. An **ICAL** tag is always embedded in the standard HTML comment tag. For example:

<**!--ICAL**.UserID -- >

- **ICAL**.TagName — This type of tag returns a value, such as the

UserID of the currently logged on user, or the IMail Server host name.

- **ICAL**.*TagName*.*Value* — where *TagName* is the name of the item, such as a button, hyperlink, or check box. You cannot edit the *TagName*. For text that appears on a button, the *TagName* has the suffix Button, (for example: LogonButton, SaveButton); for text that appears in a hyperlink, the suffix is Link; for simple text tags, the suffix is Text. *Value* is the actual text that appears on the button, in the hyperlink, or next to the check box. You can edit the *Value* to change the text to whatever you want

The document "IMail Server Web Calendar Templates" *(iwebcaltags.doc* file in [*IMail Top Directory*]*\Web*), lists all ICAL tags.

Types of Tags

You can use the tags to do the following types of operations.

- **Normal** tags return a value or values. These tags are used to build dynamic information, such as the name of the logged in user.
- **Conditional** tags check whether a condition is true or false, and then continue processing based on the answer. These tags use If-Then-Else constructs.
- **While** tags populate a table, such as a list of messages in a mailbox. These tags use For-Each constructs.
- **Include** tags let you name an HTML, ASP, CGI, CSS or other file to be included at the tag location. If the file extension is *.asp* or *.cgi*, then the included file will be further parsed for IMAIL tags. For example, you can use the **Include** tag to include a standard header in all files.

For a complete guide to using tags in a template, see the document "IMail Server Web Calendar Templates," (*iwebcaltags.doc* file in the [*IMail Top Directory*]*\Web* directory).

List of Graphic Files in the Web Directory

The following table lists the default graphic files and indicates where they are used in the Web Calendar interface. Most of these *.gif* files

represent buttons used in Web Calendar pages.

Graphic	Where used
addtodo.gif	Add button found on the Task List dialog box
advert.gif	Advertisement banner for WhatsUp Gold
bdc.gif	Birthday cake icon that is displayed in the day and week calendar views to indicate the event is a birthday
bell.gif	Bell icon that is displayed in the day and week calendar views to indicate that a reminder has been set for the event or task
calemail.html	Example of a calendar e-mail invitation
close.gif	Closes out the popup toolbar.
del.gif	Trash can icon that symbolizes the ability to delete the event or task that it is assigned
ftpgrphw.gif	Advertisement banner for WS_FTP Pro
gotobtn.gif	The GoTo button for the search feature.
left.gif	Left button found on the current calendar views
nextleft.gif	Left button found on the monthly calendar list box
mail.gif	Graphic that represents a mail message that has been read.
mail_new.gif	Graphic that represents a new, unread mail message
nextleft.gif	Left arrow found on the monthly calendar list box
nextright.gif	Right button found on the monthly calendar list box
pdate.gif	Small calendar in the Date section on the Add Event and Add Task pages.
repeat.gif	Repeat icon used to indicate the repetition of an event or task in the day and week calendar views
right.gif	Right button found on the current calendar views
ssl-key.gif	Keys logo shows SSL is not in use
ssl-lock.gif	Lock logo that signifies SSL is in use

Appendix I: Mail Servers and the DNS

This appendix provides some background information on the Domain Name System (DNS) and how mail servers use the DNS. The section briefly describes the DNS, but the focus is on mail servers and the DNS records that mail servers use to find other mail servers.

If you are not familiar with how DNS operates, we recommend the book “DNS and Bind” published by O’Reilly and Associates, for general DNS information. Refer to your DNS server’s documentation for information about making entries in your DNS server.

What is DNS?

DNS is the mechanism by which applications on your network can locate the address of other hosts on the Internet, and by which other hosts on the Internet can locate you. The DNS essentially provides a map of the structure of the Internet.

To participate in the Internet, organizations must register a domain name with the InterNIC and obtain addresses to use for the hosts in their domain. For example, *ipswitch.com* is a registered domain name, and some addresses assigned to *ipswitch.com* are 156.21.50.1 through 156.21.50.255. For information about registering a domain name, see the InterNIC’s web site at **http://rs.internic.net**.

All hosts on the Internet must have a host name and an IP (Internet Protocol) address. You can give a host any host name you want, as long as it is unique within your domain. For example, some host names and addresses in the *ipswitch.com* network are:

```
test1.ipswitch.com  156.21.50.1
test2.ipswitch.com  156.21.50.2
test3.ipswitch.com  156.21.50.3
```

DNS servers provide the mapping of host names to their addresses. The DNS server for *ipswitch.com* lists each Ipswitch host and its corresponding address. Thus, any host outside of *ipswitch.com* can query the DNS server for *ipswitch.com* to find the address of a particular host. Once it has the address, the requesting application can communicate directly with the host.

Note that querying a DNS server is also called a “DNS lookup” or a “lookup.”

When a host outside *ipswitch.com* wants to send mail to a user on the *ipswitch.com* network, it queries the DNS server for *ipswitch.com* to find the mail server for users on *ipswitch.com*. The host can then send mail to the mail server, which will deliver it to the appropriate user.

How the Mail Server Uses DNS

All SMTP mail servers that communicate with other Internet hosts use a DNS server to look up mail addresses. The basic communications between a mail server and a DNS server work as follows for incoming mail and outgoing mail.

Incoming Mail:

To illustrate how a DNS server is used to look up mail addresses, we use the example of what happens when a user on another Internet host sends mail to a user on your IMail Server host (for example to *fred@domain.com*).

1 A user sends mail to your user, *fred@domain.com*.

2 The sending mail server asks the DNS server on the *domain.com* network for the host name of the mail server. The MX (Mail eXchanger) record in DNS identifies the Host Name of the mail server.

3 The DNS server for *domain.com* returns the value of the MX record, which is the host name of the mail server, in this case, *mail.domain.com*.

4 The sending mail server now asks the DNS server on the *domain.com* network for the address of the mail server host (*mail.domain.com*). The A record in DNS maps the host name to an IP address.

5 The DNS server for *domain.com* returns the value of the A record for the mail server host (*mail.domain.com*), which is the IP address (156.50.1.5).

6 The sending mail server connects to the receiving mail server’s IP address and sends the mail.

Outgoing Mail:

When one of your IMail Server users sends mail to a user on another Internet host (for example, to *sam@widgets.com*), the same process occurs, except that it is your mail server that does the lookups for MX and A records on the DNS server for the *widgets.com* network.

Reverse Lookups

Note that some mail servers, upon receiving a mail, will do a "reverse lookup" on the address to make sure it is valid. This is done in an attempt to thwart bulk mailers who may be illegally using someone else's mail server to relay mail. To do a reverse lookup, the receiving mail server asks the DNS server on the sending mail server's network to confirm that the IP address of the sending server matches the host name of the sending server.

Reverse lookups are enabled in DNS by creating a PTR record for the mail host. The PTR record maps an IP address to a host name.

Setting Up Mail Server Records in the DNS

To set up your mail server in the DNS, you must create the records that other mail servers use to find and connect to your mail server. Making these entries requires that you first have:

- A registered Internet domain name for your local network (for example, *domain.com*).
- A DNS server for your local network.

Your Local Network's DNS server

Before your mail server can communicate with other mail hosts, you must configure the DNS server to recognize your mail server. Without a functional and correctly set DNS, IMail Server cannot deliver mail, except to domains that are within IMail Server.

For each mail host on your network, you must make the following entries in your DNS:

- An MX record for the mail domain (for example, *domain.com*). The MX record identifies the host name of the mail host.

  Note that mail hosts (virtual hosts) that do not have an IP address require only an MX record. See "Setting Up DNS for Multiple Mail Hosts" on page 43 for more information.

- An A record for the host name of the mail host. The A record maps a host name to an IP address.
- A PTR record for the IP address of the mail host. The PTR record maps an IP address to the host name and is used for reverse lookups.

Since there are DNS servers from many vendors available, we cannot describe how to create the records for your specific DNS server. Instead, we show an example using a basic configuration for a single mail host.

Example of a Basic Configuration

In this example, we use a DNS lookup tool to query the DNS server and show the responses. You can use the Windows NT command line program, NSLOOKUP, to query a DNS server. If you are not familiar with this tool, we suggest the Ipswitch WS_Ping ProPack application, which provides a graphical interface for querying a DNS server. Use the Lookup tool in WS_Ping ProPack.

To describe the DNS entries for a mail server, we use examples from a typical small network and start with the following assumptions:

- You have one computer with a network interface card (NIC) installed.
- You have set the IP address for this computer to a valid address within your range of addresses. In the example, we will use 156.21.50.5.
- You have assigned this computer a host name that is valid in your domain. In the example, we will use *mail.domain.com*.
- You have designated another SMTP server to act as a backup if your mail server is down. In the example, we will use *cecil.domain.com*.

You must set up the following records for the computer:

- An MX record for the domain *domain.com* that points to the host name of the computer running IMail (*mail.domain.com*).
- An A record for *mail.domain.com*
- A PTR record for *mail.domain.com*

E-mail for the users on this mail host is addressed to *user@domain.com*.

First, we do an MX lookup (just as a sending mail server would do) to find the mail host for the *domain.com* network. To simulate this, in the WS_Ping ProPack's Lookup tool, we enter *domain.com* in the Name/Address box and **MX** as the Query Type, which returns the following:

```
domain.com
   10, mail.domain.com
   50, cecil.domain.com
```

This shows that *mail.domain.com* and *cecil.domain.com* are both mail hosts for the *domain.com* network. The *cecil.domain.com* host is a backup mail server. The number indicates the priority of the mail host — it tells the sending mail server which mail host to try first. The lower the number, the higher the priority. In our case, *mail.domain.com* is the one we want other mail servers to use first; *cecil.domain.com* is used only if *mail.domain.com* is down.

For information about how a backup mail server works, see "Setting Up IMail Server as a Backup Mail Spooler" on page 50.

Only a host name is returned in response to an MX query. The sending mail server needs the IP address of this host name so it can connect to the mail host. The sending mail server performs another DNS lookup to get the IP address (defined in the A record) of highest priority mail host. To simulate this, in the Lookup tool, we enter *mail.domain.com* in the **Name/Address** box and A as the Query Type, which returns the following:

```
mail.domain.com
   156.21.50.5
```

If we query the A record for *cecil.domain.com*, we get:

```
cecil.domain.com
   156.21.50.100
```

With the IP address for the *mail.domain.com* host, the sending mail server can now connect to that host and deliver the mail. If the attempt is successful, there is no need to go any further. However, if the *mail.domain.com* host is down, the connection attempt fails and the sending mail server will have to try the next highest priority MX record, in this case, *cecil.domain.com*.

Sample DNS Records

If we use a DNS lookup tool to query the DNS server for the network in our example (for all information, in verbose mode), you would see entries like the following:

```
domain.com.  IN MX   50 cecil.domain.com.
             IN MX   10 mail.domain.com

cecil.domain.com.  IN A  156.21.50.100
mail.domain.com.   IN A  156.21.50.5

5.50.21.156.in-addr.arpa.,type = PTR
 host = mail.domain.com
5.100.21.156.in-addr.arpa.,type = PTR
 host = cecil.domain.com
```

Other Configurations

If you have multiple mail hosts on your IMail Server, you will need an MX, A, and PTR record for each host. “Chapter 3: Configuration” on page 33 describes some advanced configuration topics and describes the DNS entries you must make for these advanced configurations.

Glossary

A record

A records map a host name to an IP address.

Alias

An alias is another name assigned to a host name that can be used in place of the host name (plus domain name). Aliases are often used to shorten long host names for convenience.

Baud rate

The rate (measured in bits per second) at which the serial port for the MONITOR server will communicate with the modem.

Cache

Each time a Domain Name Server processes a lookup request for a host not in its domain, it must query another name server for the information. When a reply is received, the Domain Name Server saves the address information in a cache. The next time it receives a query for the same information, it does not have to query another name server for the information. Because address data in the Domain Name System changes frequently, the system administrator assigns a Time to Live (**TTL**), after which the cache is cleared.

Client

A client is a program running on a networked computer that requests services from a **server** program, which is usually running on another networked computer. The client communicates with the server using a protocol. For example, an FTP client communicates with an FTP server using the FTP protocol.

DLL

Dynamic Link Library is a library of executable functions that can be used by an application. A DLL provides one or more functions and a program accesses the functions by creating a link to the DLL.

Domain

A term that refers to the subdivisions of the Internet network. Domain can mean the major subdivision of which your network is a part (.com, edu, .gov, .net, .us, .uk) or it can refer to your part of the network (ipswitch.com). See also **Domain Name System**.

Domain Name System

A distributed database system that translates host names (for example, tortoise.ipswitch.com) to IP addresses (for example, 156.21.50.10). All hosts on the Internet are named using the conventions specified by the Domain Name System. Host Names are used because they are easier to remember than numerical addresses (IP addresses). An example host and domain name is tortoise.ipswitch.com, where tortoise is the host name, and ipswitch.com is the domain name. The domain represents the network where the host is located.

Domain name server

A host that keeps a table of host names and IP addresses, and provides the lookup service for client programs. A domain name server is used by client programs to look up the IP address of a host. A domain name server provides host name to IP address mapping for the local network and provides access to the Domain Name System to look up hosts in other domains.

A *primary* name server contains all the information for the domain in its database files. If you add a second name server for backup or to off-load the primary server, you can set it up as a *secondary* server. A secondary name server obtains its domain information by copying the database files from the name server that is primary for that domain. The advantage of using secondary servers is that you can maintain the domain information on one name server (the primary).

Finger

Finger protocol is a common Internet language that allows remote users to see information about users registered on a system. This includes the full name of the specified user, his or her complete e-mail address and a “plan” file provide by the user that contains additional information the user wishes to provide in response to Finger requests.

FTP

FTP stands for File Transfer Protocol. This is one of the standard protocols defined for use on a TCP/IP network and used to transfer files between systems.

Gate host

Gate Host is the name of another host to send mail to when the mail cannot be delivered directly to the destination host.

IMAP4

Internet Message Access Protocol version 4 (IMAP4) is a method of accessing electronic mail messages that are kept on a (possibly shared) mail server. It permits a client e-mail application to access remote message stores as if they were local.

in-addr.arpa domain

A special domain on the Internet that maps IP addresses to domain names. This domain is used to do reverse lookups, where the IP address is known and the application is querying for the host name.

IP (Internet Protocol)

The protocol that determines how packets (bundles of data) traverse the Internet network to find their destination. See also **TCP**.

IP address

All hosts on the Internet are identified by a unique numeric code, called the IP address. 156.21.50.1 is an IP address. The Domain Name System is used to map the IP address to a name.

LDAP

Lightweight Directory Access Protocol is a way of accessing directory information stored on a server. It permits an LDAP-enabled client to search for and view user information stored in an LDAP directory.

List Administrator

The User ID on the current mail host who can administer the list using Web Messaging. This person can modify list properties, add/delete users, and edit all related files. The list administrator and the list owner are usually the same person.

List Owner

The person who receives all messages (such as *Subscribe* and *Unsubscribe* requests, and error messages) to the list. It is also the account to which all messages are sent to the list, from anyone who requests information about the list, and in response to invalid attempts to post to the list. The list owner and list administrator are usually the same person. On a moderated list, the list owner is also the list moderator.

List server

A List server provides an automated way to manage mail discussion groups. All messages for a mail discussion group received by a List server are sent to all the members of that mail discussion group.The List server manages the adding and removal of users from the subscriber list and the distribution of messages to all subscribed users.

MX record

The MX record identifies the host name of the computer running the mail server (in this case, the IMail Server computer).

Name server

See **domain name server**.

namespace

Synonymous with domain.

ODBC

Open DataBase Connectivity is a standard database access method that makes it possible to access data from any application, regardless of which database management system(DBMS) is handling the data. ODBC inserts a layer, called a database driver, between an application and the DBMS. This layer translates the application's data queries into commands that the DBMS understands.

POP3

Post Office Protocol version 3 (POP3) is the most common protocol for communicating with a mail server (otherwise known as a post office) to retrieve messages for a user. Since POP3 servers are always available to receive incoming mail, individual users do not have to have their PCs turned on at all times. POP3 servers hold mail for users until they connect to download their messages.

Processing rules

Delivery rules direct incoming mail based on the contents of To, From, Sender, Subject, the message Header, or the message Body. Delivery rules can be applied for a domain, individual user or list-server mailing list.

Protocol

A set of rules that define how computers will exchange information.

PTR record

The PTR record maps an IP address to the host name and is used for reverse lookups.

Relay

A message that originates on a computer other than the IMail Server host and is destined for another host, must pass through IMail Server. IMail server (or any SMTP server) then accepts the mail and redelivers it to that host.

Request for Comments (RFC)

A set of documents that define the Internet standards. RFCs are also used to propose new standards, or extensions to existing standards.

Reverse lookups

When the client program requests the host name of a given IP address, the DNS server does a reverse lookup. This is the reverse of the normal DNS lookup procedure, where the IP address for a given host name is sought. Reverse lookups use a special domain, the **in-addr.arpa** domain, which maps IP addresses to domain names.

Server

A server is a program running on a networked computer that processes requests for services from a **client** program, which is usually running on another networked computer. The client and server communicate using a protocol. For example, an FTP client communicates with an FTP server using the FTP protocol.

Service

“Service” is a formal Windows NT/2000 term for an executable object installed in a registry database maintained by NT/2000’s Service Control Manager. A service can be automatically started when the system is booted and continues to run until the system is shut down. It will continue to run even when no one is logged on the system.

SSL

Secure Sockets Layer(SSL) is used for communications between a browser and server. SSL encrypts mail communications so they can be read only by the intended recipients. SSL uses “certificates” to authenticate the client and server, and uses a public/private key “pair” to encrypt and decrypt communications. All of the major browsers are SSL enabled.

SMTP

Simple Mail Transfer Protocol (SMTP) is designed to efficiently and reliably transfer mail across TCP/IP networks, including the Internet. SMTP defines the interaction between mail systems to facilitate the transfer of electronic mail even when the mail systems are on different types of computers or running different operating systems. SMTP is required to send or receive mail over the Internet. IMail Server is an SMTP server.

Spamming

When a bulk mailer sends unsolicited mail to other people, it is known as “spamming.” Spam mailers may try to use your system to relay their messages to other Internet mail users, tying up your valuable system resources. IMail Server provides anti-spamming features.

TCP

Transmission Control Protocol; the protocol that controls how data is assembled and disassembled in packets. See also **IP**.

TTL

The Time to Live (TTL) specifies an amount of time (usually in seconds) for which a secondary name server can use the DNS database files that it copied from the primary server before it needs to refresh the data.

UDP

User Datagram Protocol; a transmission protocol for uses that do not require the control and error checking of TCP.

Whois

The Whois protocol is a common Internet language that allows remote users to search for mail addresses of users.

Winsock

Winsock is a specification that developers of TCP/IP network software for Microsoft Windows use as a guideline for the standard application programming interface to their network software.

Index

A

A record 35, 43, 316, 321
Absence. See vacation.
Accept.txt 160
Addalias.exe 260
Adddomain.exe 262
Adding
  aliases 75
  aliases in batches 260
  groups of users 263
  multiple hosts 262
  users 16
Add-on products 13
Adduser.exe 263
Administrator. See host administrator, list administrator, system administrator.
Advertisements 129, 143
Alias
  "nobody" 79
  administration from a web browser 124
  description 75
  for peer servers 53
  host 36, 39
  postmaster 75
  to process unregistered users 79
Ampersand
  in user IDs 63
Antispamming. See spam mail.
Attachments
  in Spool directory 275
Authenticating users 15, 16
Automated response. See Info Manager.

B

Backing up
  IMail Server configuration 257
  system files 258
  user mail 258
Backup mail server 50
Backup mail spooler 50
Baud rate 204
Beeper notifications 200
  using external program 202
Blocking mail. See spam mail.
Bulk mail See spam mail.
Buttons in Web Messaging. See Web Messaging templates.

C

Cfg directory 27
Command line utilities 259
Conditions See Delivery rules 91
Copying mail 164

D

Data Source Name. See System DSN
Database
  external 55
  IMail (proprietary) 16
  Windows NT 16
Default host 24
Default NT registry values 279
Default settings
  for new users 65
Delay between recipients 151
Deleting
  messages by date 68
  old messages 268
  users 16
Delivery application 151
Delivery rules
  creating 85, 88
  description 83
  examples 83
  external files 99
  inbound 85
  limitations 101
  multiple conditions 91
  Orules.ima 84
  outbound 88
  processing 84
  rules.ima
    orules.ima 84
  syntax 93
  testing 92
  text patterns 95
Dial string 201
Dial-up connection 46, 47, 55
Dictionaries 127
Directory structure 27
  Web Calendaring 303
  Web Messaging 285, 287, 304
Distribution lists. See Group Alias.
DLL 57
DNS 12, 15, 33, 53, 315
  and mail servers 315
  description 315
  lookup 316
  lookup(Windows 2000) 15, 34
  lookup(Windows NT) 15, 34
  multiple hosts 43
Domain forwarding. See unregistered users.
Domain Name Server. See DNS.
Domain Name System. See DNS.
Domain. See mail domains.
DSN 17, 55

E

E-mail notifications 205
ETRN 54
Eudora 62
External database 17, 55
External program
  beeper notifications 202
  sending mail to 76

F

Fax
  mail to fax 241
Features
  new 2
  standard 10
File extensions
  Spool directory 274
File locking 255
File names
  queue files 273
  spool directory 273
  web messaging templates 285, 303
Finger Server 9, 188
  configuring 188
  introduction 187
  registry values 279
  security 187
Finger server 9
Finger support 69
Forward.ima 74
Forwarding mail 11, 73, 237, 238

G

Gate Host 23, 323
Gateway. See mail gateways.
Global settings
  for new users 65
  registry values 279
Graphics for Web Messaging 286
Group alias 76, 78, 161
Groups. See group alias.

H

Hack attempts 156, 162
Headers in list-server mailing lists 225
Host administrator 62, 122, 123, 142
Host delimiters 151
Hosts
  alias 36, 39
  multiple 12
  primary mail 34
  virtual 36
  web directories 287, 304
HTML
  using in news message 288, 305
  using in online ads 130, 144
  using in tail message 144
  using in web templates 290, 306
  using in welcome message 288

I

IMail Anti-Virus 13
  processing order 82
IMail Client 13
IMail database 16
IMail Server 1
IMail System Administrator. See system administrator.
IMAIL tags. See Web Messaging templates.
Imail1.exe 267
IMAILSECDB 18, 57
IMAP Server 5, 179, 180
  configuring 180
  description 177
  implementation 177
  mailbox management 178
  port 26
  public mailboxes 179
  registry values 279
  security 179
  welcome message 182
IMAP server 5
Immsgexp.exe 268
Importing
  users into a domain 258
Importing users from Windows NT 63
Incoming mail 81
  DNS and 316
  validating 155, 162
Info Manager 101
  creating an automated response 101, 104
Installation 15
Internet service provider.
  receiving mail from 46
IP address 112, 134
  deleting when no longer in use 283
  for virtual host 36
  relay for 159
  virtual 37
Ipswitch products xiv
Ipswitch web site xvi

J

JavaScript. See templates.
Junk mail. See spam mail.

K

Kill file 163, 228

L

LDAP
  attributes 62, 72
  information 72
  protocol 72
LDAP server 9, 175
  configuring 175

description 171
implementation 171
port 26
registry values 280
security 174
List administrator 62, 122, 123
List alias. See Group Alias.
List Server 215
commands 219
forwarding mail 231
kill file 228
program aliases 231
setup 216
List server 9
Lists 10
access to 161
administering from Web Administration function of Monitor server 210
administering from Web Messaging 125
headers 225
number of subscribers 226
recipients per message 226
trailers 225
Lists directory 27
Local host
relay for 160
Locking files 255
Log files 275
large 277
viewing from Web Messaging 124
Log server 275
Logon screen
Tail message 130, 144, 288
Title 288
Welcome message 288
Lookup, DNS 316

M

Mail accounts 60, 124
adding 124
deleting 64
Mail delivery rules. See Delivery Rules.
Mail domains
DNS and 316
multiple 12
virtual hosts for 36
Mail Forwarding. See forwarding.
Mail gateways 13, 23, 151, 157, 323
remote 151
sending mail 23, 151, 323
setting up 45
using IMail 45
Mail gateways See also relay.
Mail host
primary 15, 34
virtual 36
Mail relay. See relay.
Mail to Fax 13, 241
adding an alias 243
dynamic dialing 246
files in the queue 274
global properties 248
installing fax support 241
modem port 242
viewing queue files 253
Mail to Pager/Beeper 12
Mailall.exe 269
Mailbox Delimiters 151
Mailboxes 66
sub-areas 68
Mailing all users on a host 269
Mailing list (groups). See Group Alias.
Mailing lists (list server). See lists.
Main.inf 74
Max Mailbox Messages 65, 67
default 42
Max Mailbox Size 65, 67
default 41
Maximum recipients per message 151
Messages
maximum number of 40
size 40
Modem initialization string 204
Monitor Server 9
configuring 196
definition 195
logging on 198
Web Administration 208, 210
Web Administration port 26
MX record 35, 37, 43, 316, 321

N

New features 2
News of the Day
editing 288, 305
Non-existent users 79
Notifications 9, 197, 199
beeper 200
defining 199
e-mail 205
enabling 207
pager 202
NULL senders 156, 162
NuPop 62

O

ODBC 18, 57
ODBCUSER.DLL 57
Online advertisements 129, 143
Online advertising 129
Optional products 13
Order of processing 81
Orphan mail accounts 64

P

Pager notifications 202
Password server 191
  configuring 191
  introduction 191
  port 26
  registry values 280
  security 192
Peering
  example 53
  how it works 51
  setting up 51
Plan.ima 69, 74
POP3 Server 5, 165
  access 168
  advanced options 168
  configuring 166
  description 165, 239
  logging on 165
  port 26
  protocol 12
  registry values 280
  security 198
  welcome message 168
POP3 server
  security 165
Port number 112, 134
  for IMail services 26
  Web Calendaring 134
  Web Messaging 112
Postmaster alias 19, 274
PPP connections. See dial-up connection.
Primary host 15, 34
Primary mail host. See primary host.
Processing rules for smtp32 and imail1 271
Processing sequence 81
Program Alias 76, 79
PTR record 35, 43, 317

Q

Queue 25
  time 50
Queue files 273
Queue Timer 55, 150

R

RAS connections. See dial-up connection.
Registering users 15, 16
Registry
  values 283
  Windows NT 279
Relay 153
  for groups 161
  for local hosts 160
  for local users 160
  options 154, 157
Remote administration 123
Restoring IMail data from a backup file 257
Retrieving mail 54
Reverse lookups 317
RFCs 147
Root user ID 19, 274
Rules See delivery rules.
Rules.ima 74

S

Security 111, 134
  access to SMTP server 163, 209
  anti-spamming feature 157
  checking sender 162
  denying sender 163
  incoming mail 162
  mail lists 161
  null sender 162
  remote administration 107
  setting user access 122, 141
  SMTP kill file 163
  SMTP server 156
Servers (services). See SMTP server, POP3 server, IMAP4 server, LDAP server, Log server, Finger server, Whois server, and Monitor server
Service agreements xvi
Size
  maximum message 225
SMTP
  AUTH command 155
  kill file 163
  mail gateways. See mail gateways.
  protocol 5
  RFCs supported 147
  security 153
  VRFY command 162
SMTP send program 270
SMTP Server 5, 147, 281
  access 163
  advanced options 151
  configuring 149
  logging on 148
  maximum processes 151
  port 26
  registry values 281
  security 148, 156
  welcome message 151
SMTP server
  configuring 149
  security 156
Smtp32.exe 270
Software patches xvi
Spam mail 13, 153, 155, 157
Spell Check 125
  dictionaries 126, 127
  editing dictionaries 127
  enabling 126
Splcln.exe 272
Spoofing. See spam mail.
Spool Cleaner utility 272
Spool directory 27, 273
  viewing 124

viewing from Web Messaging 124
Spooler
backup 50
SSL
installing 28
troubleshooting 116
with Web Calendaring 135
with Web Messaging 113
Standard Alias 76
Subnet mask 159, 164
System administrator 122, 123
System DSN 17, 18, 55
System requirements 2, 110, 133

T

Table name (for external database) 58
Tags, for Web Messaging templates 298, 311
Tail message
Web Calendaring 144
Web Messaging 130
TCP ports 26
TCP/IP 34
Technical support xvi
Templates 308–311
Web Calendaring 303
Web Messaging 286
Testing IMail Server 23
Tilde character
in file names 274
Timeout 110
Title
editing 288
Top directory 27
Trailers in list-server mailing lists 225

U

Uninstalling 30
Unknown users 79
Unregistered users 79
Upgrades xvii
Upgrading 28
User ID. See mail accounts.
Users
backing up mail 258
directory 27
importing from Windows NT 63
maximum 1
Utilities 259

V

Vacation processing 11, 70
clearing sender addresses 71
responding to every e-mail 71
viewing sender addresses 71
Vacation.ima 71, 74
Vacation.snt 71
Validating incoming mail 155, 162
Virtual hosts 12, 36, 113, 135
configuring 38
IP addresses 36
Virtual IP address 37
VRFY 156, 162

W

Web address 112, 134
Web Administration through the Monitor server 9, 208, 210
Web Calendaring
advertisements 143
customizing 145
customizing pages 311
customizing templates 308
description 131
directory structure 303
e-mail pages 308
graphics 313
help pages 310
interface 145
IP address 134
logging on 133
port 134
security 133
server configuration 138
setting access 141
tail message 144
templates 303, 308–311
thread pool 141
web pages 306
Web Messaging
access 122, 141
advertisements 129
connection timing out 109
customizing 130
customizing templates 292
description 107
directory for multiple hosts 287, 304
directory structure 287, 305
e-mail pages 292, 293
files 285
graphics 286
help pages 297
IMAIL tags 298, 311
interface 130
IP address 112
list administration 125
logging on 109
port 26, 112
remote administration pages 294
server configuration 117
spell check 125
tags 298
tail message 130
templates 286, 292, 298, 311
thread pool 120

upgrading 110
web pages 290, 292, 308
welcome message 288
Web Remote Administration utility 62
Welcome message (for Web Messaging) 288
Whois server 9
configuring 184
description 183
registry values 281
security 183
Windows NT
importing users 63
Windows NT database 16, 62
Windows NT registry 30
Windows NT registry values 279