

IPSWITCH

IMail Server

IMail Administration Help

IPSWITCH

CHAPTER 1 Introduction to IMail Administrator

About Help 1
Web Administrator and Client 3
IMail Administrator Requirements 5
System Requirements 6
New for Version 11.01 11
Accessing the IMail Web Administration 19
Using Internet Information Services (IIS) Virtual Directories 20
Additional Resources 20
IMail Getting Started Guide Links 22
Installing Patches and Upgrades 23
Table of Features 23
Helpful Definitions 26
File Attachment Settings 26
IMail Processing Order 27

CHAPTER 2 Installing

Installing IMail Server Administrator 29
Setting the E-Mail Domain Name (Official Host Name) 30
Setting Up an Alias for a Host 30
Setting Database Options 31
Installing SSL Keys 32
Folder Permissions and IIS Configuration 32
IIS Settings 35
Using IIS Virtual Directories 37
    Changing IIS Virtual Directory names 37
Installing Patches and Upgrades 37
Using the IMail Installation Log File 38

CHAPTER 3 Mail Domain (Host) Configuration

Domain Properties 41
Adding a New IMail Domain 47
Configuring an NT/AD database 52
    Example of Active Directory "built-in" 52
About Virtual Mail Domains (Hosts) 53
LDAP Settings 54
Bouncing Spam Messages using Rules 55

Setting up a Dial-up Internet Connection 57
Method 2 Example 59
Using ETRN to Retrieve Mail on a Dial-up Connection. 59
Method 3 Example 60
Changing the IP Address of a Host 60
Setting Up a Mail Gateway 61
Setting up IMail Server as a Backup Mail Spooler 62

CHAPTER 4 User Mail Accounts

Creating User Database 65
Using the Windows NT/Active Directory Database 65
Importing Windows NT Users 66
Using the IMail Database 68
Creating External User Database for a Mail Domain 68
Working with Individual User Accounts 70
Vacation Message 70
Customizing the Full Mailbox Notification Message 71
Full Mailbox Notify Example 71

CHAPTER 5 System Administration

System Settings 73
Archiving (If Installed) 75
System Trailer 76
HTML Online Editor 76
System WebMail Message 78
Microsoft Exchange ActiveSync 78
Synchronizing With Microsoft Exchange ActiveSync 80
DomainKeys / DKIM 82
System Selector List (Signatures) 83
DNS Black Lists (Server Level) 89
Understanding DNS Black Lists 90
How Black Lists Work 91
Add/Edit DNS Black List 92
Spool Manager 94
Managing Spool Manager 95
Cleaning the Spool Directory (Isplcln.exe) 96
File Extensions of Files in the Spool 96
Beginning Character of Files in the Spool 97

System Default User Settings 98
System Default Web Mail Preferences 101
Registry Backup 105
Back Up IMail Registry 105
Restoring IMail Registry 106
Backing Up IMail Server System Files 107
Backing Up User Mail 107

CHAPTER 6 Domain Administration

System Administrator 109
Domain (Host) Administrator 110
Domains 110
Domain Properties 111
User Administration 124
Change Password 125
User Properties 126
ActiveSync Domain Level Checkbox 149
ActiveSync -User Level Checkbox 149
Rename User ID 150
LDAP Information 150
File Directory 151
Deleting Messages by Date for User 152
Inbound Delivery Rules for Users 153
Vacation Message 157
Auto Responder 158
Example: 159
DomainKeys / DKIM 162
Domain Selector List (Signatures) 164
DomainKeys / DKIM Verification Settings 171
DomainKeys / DKIM Wizard 179
Spam Filtering (Domain Level) 182
Alias Administration 183
Add / Edit E-mail Alias 185
Adding Aliases using "addalias.exe" Utility 188
List Administration 192
Types of List Server Mailing Lists 194
Creating and Managing Lists 196
Managing Lists 211
LDAP Settings 217

InBound / Outbound Rules 218
How Rules are Stored and Processed 219
Using IMail Rules to Filter Spam 220
Inbound Delivery Rules for Domains 220
Outbound Delivery Rules for Domains 222
Adding Rule for Domains 223
Attachment Blocking 227
Storing Search Strings in an External Text (.rul) File 230
Rules Syntax 232
Example for Entering Rules in the Rules.ima File 236
White List Administration 242
Wild Card Examples for Trusted Addresses 243
Peer List 244
Creating Peer List 244
Setting Up Peering 245
How Peering Works 246
Example of Peering 246

CHAPTER 7 Anti-virus

IMail Antivirus powered by BitDefender - Settings 249
Overview of IMail Anti-virus powered by Bitdefender® 251
Logging for IMail Anti-virus powered by BitDefender 252
IMail Anti-virus powered by Symantec - Settings 252
Overview of IMail Anti-virus powered by Symantec 254
Anti-Virus Administration (Symantec) 254
Alert Administrator Email 255
Updating Symantec Virus Definitions 255
Enabling Symantec Anti-virus Logging 255
Error Codes in the SMTP Log 256
Understanding Anti-virus Entries in the Mail Queue 256

CHAPTER 8 Antispam

Antispam Overview 259
Types of Antispam Filters 261
Antispam Configuration Overview 262
About Your Spam Signature 263
IMail Antispam Processing Order 263
Installing Updated Antispam Files 265

Forwarding Spam to CommTouch 266
Antispam FAQs 267
Server Level Antispam Options (Black Lists) 270
Understanding DNS Black Lists 270
How Black Lists Work 271
DNS Black Lists (Server Level) 272
Spam Filtering (Domain Level) 279
Commtouch Premium Filter (Only Premium Versions) 280
Statistical Filtering 283
Phrase Filtering 288
HTML Features Filter 291
URL Domain Black List 299
Broken MIME Headers 301
Enable Content Filtering 303
SPF Filtering 303
The action to be taken when the query result is Pass 312
Connection Checks 313
Antispam Logging 317
Using Antispam Log Entries 317
Setting the Antispam Logging Options 319
Antispam Log Messages 319
Spam X-Header Explanations 330
Antispamseeder Utility 333
Overview (antispamseeder.exe) 333
Preparing Mailboxes for use with antispamseeder.exe 334
Antispamseeder Parameters 335
Identifying spam with double byte characters 336
Merging Antispam-table.txt files 336
Adding a New Word to the antispam-table.txt File 337
Deleting Words from Antispam-table.txt 338
Resolving Incorrectly Identified E-mail 339
Creating Separate antispam-table.txt Files for Multiple E-mail Domains 340
Customizing an E-Mail Domain's antispam-table.txt File 342
Example - Spam Word Counts 343
Example - Non-Spam Word Counts 343
Modifying Word Counts of Existing Words 343
Ensuring Mailing List and Newsletter Delivery 344
Creating URL Domain Black List with antispamseeder.exe 344
Example: 345

Creating URL Domain Black List and Antispam-Table.txt Files 346
Using Antispamseeder.exe to identify wildcards 346
Using the antispam-table.txt File 347
Modify Subject for URL Domain Black List 347
Mailbox Path 347
Word (defined for the antispam-table.txt file) 348
Do I need to alter the word tables in the antispam-table.txt file? 348
Changing the Word Count for a Word (Example) 348
Word count 349
Troubleshooting 349
Troubleshooting Antispam 349
Minimizing False Positives 350
Identifying spam with double byte characters 351
Pager Problems 351

CHAPTER 9 Collaboration

Collaboration Users 353
Add Collaboration User 354
Collaboration User Account Details 354
Collaboration User Folders and Access 354
Granting Access to a User's Personal Folders 355
Managing Collaboration Groups 356
Adding a New Collaboration Group 356
Granting Access to Group 357
Deleting a Collaboration Group 357
Public Folders 358
Public Folder Properties 358
Public Contacts Management 360
Collaboration Settings 365
Granting Access 366

CHAPTER 10 Services

Service Administration Overview 367
Configuring IMail Services 369
Viewing the Status of IMail Services 369
Logging into IMail Services 369
Setting Service Administration Options 370
Premium Antispam (Commtouch) 371

IP Ignore List ... 372
IMAP Settings ... 373
Creating Public Mailboxes ... 374
Managing Mailboxes ... 375
LDAP ... 375
About LDAP Server ... 375
About LDAP Data ... 376
LDAP Service Settings ... 377
LDAP Settings ... 379
LDAP Information ... 380
Populating the LDAP Database (ldaper.exe) ... 381
Initializing and Synchronizing LDAP Databases (iLDAP.exe) ... 382
POP3 ... 382
POP3 Settings ... 383
POP3 - Control Access ... 385
Add/Edit POP3 Control Access ... 386
Queue Manager ... 386
Queue Manager Options ... 387
Queue Manager - Daily Count Report ... 390
Troubleshooting the Spool Directory ... 391
SMTP ... 392
SMTP Service Options ... 392
SMTP Control Access Settings ... 400
SMTP Kill File ... 401
SMTP Accept List ... 402
SMTP White List ... 403
SMTP Domain Forwarding ... 404
Supported SMTP RFCs ... 406
Web Calendaring (Old) ... 407
Web Calendaring Settings (Old) ... 407
Setting Access to Web Calendaring ... 409
Web Address For Web Calendaring ... 410
Setting Up SSL for Web Calendaring ... 410

CHAPTER 11 Logging

About Logging ... 411
Log Manager ... 412
Sys Log Access Control ... 412
Add / Edit Sys Log Access Control List ... 413

IMail Log Analyzer 414
Using the IMail Installation Log File 414
Enabling Web Client Logging 415

CHAPTER 12 Command Line Utilities

Adding Aliases using "addalias.exe" Utility 417
Adding Alias to a Domain Using "addalias.exe" 419
Adding Alias to Primary Domain Using "addalias.exe" 419
Deleting an Alias using "addalias.exe" Utility 419
Addalias Text File Example 419
Import NT Group as Group Alias using addalias.exe 420
Adding a Virtual Host (adddomain.exe) 421
Adding Users (adduser.exe) 422
adduser.exe Options 424
Example Text File (Adduser.exe) 425
Using a Text File (adduser.exe) 427
Rename a User (RenameUser.exe) 428
Overview (antispamseeder.exe) 429
Merging Antispam-table.txt Files Example 430
Understanding the antispam-table.txt file 430
Antispamseeder.exe Wildcard Example 2 430
Antispamseeder.exe Wildcard Example 1 431
Registry Backup 431
Back Up IMail Registry 431
Restoring IMail Registry 433
Backing Up IMail Server System Files 433
Backing Up User Mail 434
Web Site Updater (IClientUpdater.exe) 434
Initializing and Synchronizing LDAP Databases (iLDAP.exe) 435
Cleaning the Spool Directory (Isplcln.exe) 436
Deleting Old Messages (immsgexp.exe) 436
Populating the LDAP Database (ldaper.exe) 438
Sending Mail to All Users (mailall.exe) 439
Checking the Registry (regcheck.exe) 440
SMTP Delivery Application (smtp32.exe) 443
Self-Signed SSL Certificate(sslutility.exe) 443
Creating Config_CommonAddrBook.cgi 445
Command Line Installations (Silent Installs) 445

CHAPTER 13 Using IMail Web Messaging (Web Client)

What is Web Messaging? 451
Access and Login to IMail Web Messaging Client 451
Low Bandwidth Web Messaging Lite 453
LBW - Enable Cookies 453
User Impersonation by System Administrators 454
Changing the Web Client Default Directory (setting a redirect for Web Messaging)..... 455
Configuring Web Messaging Email List Auto-Refresh Frequency 455
Accessing Spell Check Dictionary..... 456
Setting Up SSL for IMail Web Messaging 457

Index

CHAPTER 1

Introduction to IMail Administrator

In This Chapter

About Help 1
Web Administrator and Client 3
IMail Administrator Requirements 5
System Requirements 6
New for Version 11.01 11
Accessing the IMail Web Administration 19
Using Internet Information Services (IIS) Virtual Directories ... 20
Additional Resources 20
IMail Getting Started Guide Links 22
Installing Patches and Upgrades 23
Table of Features 23
Helpful Definitions 26
File Attachment Settings 26
IMail Processing Order 27

About Help



About Ipswitch IMail Server Help

Copyrights© 1995-2009 Ipswitch, Inc. All rights reserved.

IMail Server Help

This help file, 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 help file 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.

Ipswitch Collaboration Suite (ICS), the ICS logo, IMail, the IMail logo, WhatsUp, the WhatsUp logo, WS_FTP, the WS_FTP logos, Ipswitch Instant Messaging (IM), the Ipswitch Instant Messaging (IM) logo, 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.

Revision History

IMail Server (Administrator) v11.01 - October 2009

IMail Server (Administrator) v11 - April 2009

IMail Server (Administrator) v10.02 - November 2008

IMail Server (Administrator) v10.01 - June 2008

IMail Server (Administrator) v10 - February 2008

IMail Server (Administrator) 2006.22 (v 9.22) October 2007

IMail Server (Administrator) 2006.21 (v 9.21) July 2007

IMail Server (Administrator) 2006.2 (v 9.2) February 2007

IMail Server (Administrator) 2006.1 (v 9.1) July 2006

IMail Server (Administrator) 2006.04 (v9.04) April 2006

IMail Server (Administrator) 2006.03 (v9.03) March 2006

IMail Server (Administrator) 2006.02 (v9.02), January 2006

IMail Server (Administrator) 2006.01 (v9.01), December 2005

IMail Server (Administrator) 2006, November 2005

IMail Server v8.14 October 2004

IMail Server v8.2 April 2005

Web Administrator and Client

Web-based Administrator and Client

Ipswitch IMail Server V11 and Later

- IMail Server (Administrator) is an Internet standards-based mail server system for Microsoft® Windows® 2000, Microsoft® Windows® 2003 and Microsoft® Windows® 2008. It includes powerful administrative and antispam management tools all accessible via the Internet.
- The redesigned Administrator includes a series of programs that run as services: SMTP, POP3, IMAP4, LDAP3. These services can be stopped and restarted from a main Service Administration page as well as from their respective pages.
- Ipswitch IMail Server V11 and later provides local or remote access to IMail Server administration features via a Web browser. You can administer all e-mail functions, including users, groups, services, shared calendars and contacts, and antispam and anti-virus settings (available separately).
- *Dictionary Attack*[1] Options provide settings to secure your IMail Server from attacker security breaches on passwords and e-mail addresses.
- Spam protection provides the ability to put the IP address of a spammer into the Control Access list for a certain amount of time to keep the system from just reconnecting. Once the time period expires, the IP address is removed from the access list and is permitted to send mail again.

User Interface

A multi-featured main Web page allows easy administrative access to users, domains, collaboration settings for shared calendars and contacts, services configuration, log viewing and management.

IMail Web Messaging

Web Messaging (Web mail client) lets you send and receive mail using a Web browser. You can log on to Web Messaging from a browser on any computer with a supported browser, and manage e-mail without installing e-mail client software. IMail Web Messaging directly accesses the server to manage mail. When a user creates a mailbox in the Web client, the mailbox is created on the mail server and mail folders and messages reside on the server.

---

[1] A method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually entering each password. Also, an e-mail ...

IMail Web Messaging includes an integrated Web-based client. This client replaces the current Classic WebMail and Killer WebMail templates. The new client sends and receives e-mail, lets you create contacts, and lets you organize and manage mail in folders.

If you used contacts or contact lists (distribution lists) in a previous version of Ipswitch Web Messaging or in Microsoft Outlook with the WorkgroupShare plug-in, the contacts and contact lists are automatically imported into the new IMail Web Messaging client. A new Contacts folder is created that includes contacts and contact lists.

User Interface

A unified main Web page allows user-friendly access to critical e-mail functions: Inbox, folders, composing, personal settings, rule and contact management, and the ability to switch between the client and the administrator pages if you have Administrator privileges.

Ipswitch Instant Messaging

Ipswitch Instant Messaging (server) provides local or remote access to Ipswitch Instant Messaging administration features via a Web browser. You can administer all instant messaging functions, including users, public contact lists, stored conversations, and server access.

Additionally, Ipswitch Instant Messaging integrates with Microsoft® Office XP products by using Smart Tags. IIM Smart tags are person's names or e-mail addresses that are associated with an IIM contact. Microsoft Office automatically recognizes smart tags in any Office document.

WorkGroupShare (Collaboration)

Softalk's WorkGroupShare lets the people in your organization share their Outlook data, such as calendars, contacts, e-mail, tasks and notes, without the expense or expertise required by Microsoft Exchange Server.

Optional Enhancements

- **IMail Anti-virus powered by Symantec™**

  IMail Anti-virus, available separately, can be fully integrated with IMail Server and is powered by Symantec™ CarrierScan Server, a high performance, scalable, reliable solution to protect against viruses.

- **IMail Anti-virus powered by BitDefender®**

  IMail Anti-virus, also available separately, can be fully integrated with IMail Server and is powered by SOFTWIN's BitDefender®, one of the most comprehensive virus scanners available.

- **IMail Premium Antispam**

Premium Antispam filtering (optional in IMail Premium), powered by **Commtouch Advanced Security Daemon (a.k.a. ctasd™)** a plug-and-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. The daemon adds a layer of e-mail filtering to your mail delivery system in order to provide real-time classification, already in the first minutes after a new outbreak is launched.

Commtouch's GlobalView™ Mail Reputation services are used primarily to weed out spam messages and email-borne malware at the entry point before these messages enter the customer's messaging network, thereby relieving the need for resource-consuming downstream filtering. This is accomplished by applying the most up-to-date IP reputation data to the sender IP, before the SMTP connection is accepted.

By applying GlobalView Mail Reputation services to the senders' IP addresses before or during the SMTP session and before their messages enter the messaging network



Important: See the *Table of Features* (on page 23) to find out more about your options in the Ipswitch family of IMail products.

IMail Administrator Requirements

The IMail Administrator provides local or remote access to IMail Server administration features via a Web browser.

IMail Web Administration supports:

- Microsoft® Internet Explorer 6.0 and later
- Mozilla 1.7 or later
- Firefox 1.0.6 for Microsoft Windows or later
- Firefox 2.0.0.2 for Macintosh or later
- Safari 2.0.4 for Macintosh, or, the upgraded version of Safari installed with Mac OS X version 10.4.8

You can access IMail Server Administrator options from the tabs across the top of the browser and the navigation links along the left side of the browser window. For more details, see *System Requirements.* (on page 6)

Access the following IMail Server Administration features from the tabs:

- **Home.** Provides easy access to other Installed Ipswitch Products.

- **System.** Provides access to system settings, server level DNS Black Lists , and the message *queue*[2].
- **Domain.** Provides access to IMail Server domains and lets you manage domain properties, users, spam filters, aliases, mailing lists, LDAP settings, attachment blocking, inbound and outbound rules, white lists, and peer lists.
- **Anti-Virus.** Provides access to enable and select the server Anti-Virus options.
- **AntiSpam.** Provides access to a variety of antispam features such as statistical and phrase filters (content filters), HTML feature filters, URL domain black lists, broken MIME headers, Sender Policy Framework (SPF), and connection checks for domain level DNS black lists and various verification checks.
- **Collaboration**. Provides access to options for sharing users' Outlook data, such as calendars, tasks, contacts, distribution lists, notes and e-mail. You can define data that users have access to through flexible access control lists.
- **Services.** Provides access to the services status and options that IMail Server supports:
  - *Simple Mail Transfer Protoco* (on page 392)l (SMTP)
  - *Post Office Protocol Version 3* (on page 382) (POP3)
  - *Internet Message Access Protocol Version 4* (on page 373) (IMAP4)
  - *Lightweight Directory Access Protocol* (on page 375) (LDAP)
  - *Queue Manager* (on page 386)
  - *Log Server* (on page 73)
  - *Web Calendaring* (on page 407)
  - *Logging* (on page 411)
- **Logging.** Provides access to the log files in the IMail spool directory. Log files are named with the format logMMDD.txt where MM is the month and DD is the date.

System Requirements

Required Hardware

- TCP/IP enabled network interface card (NIC) with a static IP address
- Disk space is dependent on the number of users and usage.

Minimum Requirement

Operating System	
Windows 2003 (32-bit)	▪ 550 MHz ▪ 512 MB RAM

[2] The mail queue also known as the spool, is a directory that stores mail messages that are waiting for delivery. Files in the queue include incoming messages, outgoing messages, attachments, and error messages. The queue releases messages one at a time in the order that they were received.

Windows 2003 (64-bit)	▪ 1.4 GHz ▪ 1 GB RAM
Windows 2008 (32-bit)	▪ 1 GHz ▪ 1 GB RAM
Windows 2008 (64-bit)	▪ 1.4 GHz ▪ 1 GB RAM
Windows 2008 R2	▪ 1.4 GHz ▪ 1 GB RAM

Recommended Minimum by Users

Number of Users	Light Use	Moderate Use	Heavy Use
1 - 25	▪ 2 GHz ▪ 512 MB RAM(4)	▪ 2.4 GHz ▪ 1 GB RAM(4)	▪ 2.4 GHz ▪ 1 GB RAM(4)
25 - 100	▪ 2 GHz ▪ 1 GB RAM(4)	▪ 2.4 GHz ▪ 2 GB RAM	▪ 2 GHz Dual-Core ▪ 2 GB RAM
100 - 250	▪ 2 GHz ▪ 1 GB RAM(4)	▪ 2.4 GHz ▪ 2 GB RAM	▪ 2 GHz Dual-Core ▪ 2 GB RAM
250 - 500	▪ 2.4 GHz ▪ 2 GB RAM	▪ 2 GHz Dual-Core ▪ 2 GB RAM	▪ 2 GHz Dual-Core ▪ 2 GB RAM
500 - 1000	▪ 2 GHz Dual-Core ▪ 2 GB RAM	▪ 2 GHz ▪ 512 MB RAM(4)	▪ 2 GHz ▪ 512 MB RAM(4)
1000 - 2500	▪ 2 GHz Dual-Core ▪ 2 GB RAM	▪ 2 GHz Dual-Core ▪ 2 GB RAM	▪ Quad-Core ▪ 4 GB RAM
2500+	▪ 2 GHz Dual-Core ▪ 2 GB RAM	▪ Quad-Core ▪ 4 GB RAM	▪ Quad-Core + ▪ 4 GB RAM

- **Light use** is defined by the system primarily supporting POP3 users with less than 10% of users accessing mailboxes via web mail and/or mobile devices concurrently.
- **Moderate use** is defined as a mix of IMAP and POP3 users accessing the system with an average mailbox size less than 200 MB and less than 40% using web and/or mobile devices concurrently.
- **Heavy use** is defined as a mix of IMAP and POP3 users accessing the system with an average mailbox size exceeding 200 MB and more than 40% of users using web and or mobile devices concurrently.
- Microsoft recommends at least 2 GB RAM for Windows 2008.

System Guidelines for Mobile Synchronization Usage

These are general guidelines and are an approximation based on in-house performance testing. There is no guarantee that the recommendations stated below will exactly match each particular clients needs. These estimates are based on moderate mobile synchronization usage. Initial mobile synchronization and complete resynchronization of

data tend to have very high cpu usage, depending on the amount of data being synchronized.

System performance will seriously be degraded should a large number of initial synchronizations happen simultaneously.

It may be necessary to run the IMailSync application pool with multiple processes should there be a large number of mobile users.

Warning: IMailSync, IAdmin, and IClient should never be run in the same application pool. Also, both IClient and IAdmin do not support multiple processes.

Mobile User Count	Mobile System Recommendation
10 Users	2 GHz Pentium 4 with 1 GB of RAM
25 Users	2.4 GHz Pentium 4 with 1 GB of RAM
100 Users	2 GHz Dual Core processor with 2 GB of RAM
250 Users	2.2 GHz Dual Core processor and/or up to 2.8 GHz Xeon Dual Core processor with 2 GB or RAM
500 Users	High end Dual Core or low end Quad Core with 3 GB of RAM
1000 or more users	Quad Core with 3 GB Memory or more

Required Software

- Microsoft® Internet Explorer 6.0 or later
- Firefox 2.0.0.2 or later (for Microsoft Windows and Macintosh)
- Microsoft Internet Information Services (IIS) 5.0 and later
- Microsoft® .NET Framework 2.0
- Safari 2.0.4 for Macintosh, or, the upgraded version of Safari included with Mac OS X version 10.4.8

Tip: Before installing on Microsoft Windows 2008 Server, be sure IIS 7 has "Metabase Compatability" enabled. See also *Installing IMail Server on Microsoft® Windows 2008* (http://docs.ipswitch.com/_Messaging/IMailServer/Server2008/Install.htm).

Required software	For best results	Where to get it if you don't have it
Microsoft	Apply late	For service packs: *www.windowsupdate.com* http://www.windowsupdate.com

Required software	For best results	Where to get it if you don't have it
Windows 2003 Server Microsoft Windows 2008 Server	st service packs Use NTFS file system (NOTFAT) Do not deploy IMail on a Windows 2000 Domain Controller in an Active Directory environ	Advice on NTFS vs FAT: *http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.mspx* http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.mspx

Required software	For best results	Where to get it if you don't have it
	ment. .	
Microsoft .NET Framework 2.0	via Windows Update	*http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en* http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en
Windows Script 5.6 (part of Microsoft Internet Explorer 6)		*http://www.microsoft.com/downloads/details.aspx?familyid=C717D943-7E4B-4622-86EB-95A22B832CAA&displaylang=en* http://www.microsoft.com/downloads/details.aspx?familyid=C717D943-7E4B-4622-86EB-95A22B832CAA&displaylang=en
Microsoft Internet Information	Version 5.0 or higher	*http://www.microsoft.com/WindowsServer2003/iis/default.mspx* http://www.microsoft.com/WindowsServer2003/iis/default.mspx

Required software	For best results	Where to get it if you don't have it
n Services (IIS)		
Microsoft Data Access Component (MDAC) 2.6 or later		*http://msdn2.microsoft.com/en-us/data/aa937730.aspx* http://msdn2.microsoft.com/en-us/data/aa937730.aspx

New for Version 11.01

What's New in IMail Server 11.01

- **DomainKeys and DKIM (Domainkeys Identified Mail)** is now available for IMail Server. DomainKeys is a domain-level e-mail authentication standard that uses public/private key encryption and DNS to prove the legitimacy and contents of an e-mail message. DKIM is very similar in functionality to DomainKeys, with an enhanced standard that provides more flexibility and security. **See the DomainKeys Getting Started Guide** (http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/PDF/DomainKeysGSG.pdf).
- **iPhone™ mobile devices** are now supported as part of IMail Server's mobile synchronization to include e-mail, contacts and calendar events.

Note: All mobile devices that use the Exchange ActiveSync® protocol are now supported.

- New user interface in your Web and Console Administrator to maintain your **Microsoft Exchange ActiveSync® user licenses**. For more details go to **System > Exchange ActiveSync®.**
- All **labeling** in the User Interface and Help for **Mobile Synchronization** has been changed to **Microsoft Exchange ActiveSync®**.

- New **System Message for Web Client** users. Capability for the Administrator to display a message for all Web Client users at the log in page. For more information see the Administrative Help under **System > System WebMail Message**.
- New Web Administration user interface available for **Public Contact Folders (Address books).** IMail Administrators now have capability to control and update both permissions and contents of the Public Contact folders within the Web Administration. For more details see the Administrative Help under **Collaboration > Public Folders**.
- **"RenameUser.exe"** - New Command Line utility for renaming a "username" has been created. This utility can be found under your /IMail directory. For more information see the Administrative Help under **Command Line Utilities > Rename a User.**
- **IMail Antivirus powered by BitDefender®** has new improved user interface functionality within the IMail Server, along with new automated virus definition updates. Queue Manager has been enhanced to handle all the virus definition updates without requiring service restarts.
  - New user interface can be found on the **IMail Administrator > Antivirus** page.
    - Days left to license expiration
    - Date/Time of the last successful Antivirus update.
    - Option to enable/disable the automatic virus definition updates. With a default setting of 4 hours to check for virus definitions.
    - **"Update Now"** button should a manual virus definition update be required.
  - `"AVUpdate.exe"` is no longer required to update your virus definitions with IMail Server v11.01 or later. The program is still delivered with the installation to allow all older versions of IMail Server to continue to update using the old method.

Important for BitDefender® Upgraders. New automated features for virus definition updates will be enabled. Be aware that any manual schedule that has been previously setup will continue. It is up to the IMail Administrator to disable any manual schedules that were previously set.

- Now compatible with Microsoft Windows 2008 Server.
- Ipswitch's DRM (Digital Rights Management) has replaced the HASP from Aladdin Knowledge Systems, Inc.

Note: Please visit *MyIpswitch.com* (http://myipswitch.com) for more information on managing licenses, and customer assistance.

What's New in IMail Server 11

IMail Mobile Synchronization

Users now have the capability to synchronize their mobile devices with their web client information to include e-mail, contacts and calendar events. Users can maintain their contacts and calendar appointments from either their computer or mobile device, and remain synchronized.

Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks between their web client, Outlook and their mobile devices.

Default Mobile Synchronization Settings

- New IMail Server installations will have all mobile synchronization settings turned on.
- Upgrades will have the following settings:
  - System setting for Enable Mobile Synchronization will be turned on.
  - System Default User Property setting for Enable Mobile Synchronization will be turned on.
  - Domain Property setting for Enable Mobile Synchronization will be turned on.
  - Domain Default User Property setting for Enable Mobile Synchronization will be turned on (all new users will have the setting checked).
  - Existing User Property settings for Mobile Synchronization will be turned **off**, giving the IMail Administrators the decision of who is allowed to begin mobile synchronization.

The new Console Administrator has the bulk edit user capability, and can turn on this feature by going to the **Domain > User List** page, select all users and checking the Enable Mobile Synchronization.

Warning: It is recommended that Mobile Synchronization is not turned on for all users simultaneously, as the initial mobile download will put a high stress on your IMail system. See System Requirements for mobile user recommendations.

See the **IMail Administration Help > System Settings** for more details on enabling this feature. Also available for mobile device owners is the *Mobile Sync White Paper* (http://docs.ipswitch.com/_Messaging/IMailServer/v11/Mobile/MobileSync.pdf).

Product Update

To allow integration for all users to receive the greatest benefit for mobile synchronization, Ipswitch has modified the Product Offerings. WorkgroupShare previously only offered with IMail Premium has the component necessary to allow mobile synchronization with Outlook to include e-mail, contacts, calendars, tasks and notes. **WorkgroupShare** and **Ipswitch Instant Messaging** has been integrated into IMail Server Plus and IMail Server, obsoleting IMail Plus, and leaving **IMail Server** and **IMail Premium**. See new *Table of IMail Product Features* (on page 23).

- **IMail Server** will now include **Ipswitch Instant Messaging** and **WorkgroupShare**.
- **IMail Premium** will include **Ipswitch Instant Messaging**, **WorkgroupShare** and **Premium Antispam.**

New IP Reputation by Commtouch (IMail Server Premium)

Ipswitch has integrated Commtouch's GlobalView™ Mail Reputation services into IMail Server Premium v11. By default upon installation the new IMailCommtouchIpRep service will be enabled (a wrapper for Commtouch's ctIPd™ daemon) and set to only logging. This default will need to be updated by your System Administrator to enable the full capability of Commtouch's IP Reputation daemon.

The Commtouch GlobalView Mail Reputation daemon (ctIPd™) is an embedded reputation engine with a small footprint. It is responsible for maintaining communication with the Commtouch Datacenter. ctIPd™ delivers reputation data to messaging, security and networking devices, providing an added layer of protection while saving valuable resources by enabling the messaging network to analyze and process requests before message reach the network. These querying devices post queries to ctIPd™ over HTTP, UDP, or RBL/RBL+ protocol requesting reputation data on source IP addresses attempting to establish SMTP sessions for sending messages to recipients.

See the **Administration Help** at **Antispam > Premium Antispam**, and **Services > Antispam** for more information.

IMail Console Administrator

Back by popular demand, the IMail Console Administration application has been rewritten with full functionality for handling all System Administration functions.



Note: WorkgroupShare (Collaboration) and Instant Messaging have been omitted, as separate Console applications already exist for both applications. Look for them at **Start > Programs > Ipswitch IMail Server**.

The **IMail Console Administrator** has the following **new** functionality:

- New Bulk-Edit User capability by domain for editing one or more users simultaneously.
- New User Interface to allow modification to current user Web Preference settings.
- New Domain Default User Settings (also available with the Web Administration).
- New Domain Default Web Preference Settings (also available with the Web Administration).

- New System Default Web Preference Settings (also available with the Web Administration).

New Web Administrator

The Web Administrator originally written using classic ASP has been rewritten to use ASP.Net 2.0 to provide better performance.

Note: Instant Messaging has been omitted from the Web Administration application, as a separate Console application is available. Look for it at **Start > Programs > Ipswitch IMail Server > Instant Messaging Server**

- **New Navigation Bar for the Administrator.** For all list display pages where there are too many rows to display on one page, there is now a Navigation Slider, Page Number and Total Count at the bottom of the page.



  -  Navigates to the first page.
  -  Navigates back one page.
  -  Clicking on slider bar will also display the key name at the top of the page.
  -  Navigates to the next page.
  -  Navigates to the last page.
- New **Domain drop down** to easily switch domains. No longer will you have to go switch domains then return to the User Administration screen to modify user options. The following pages will have this domain changing capability:
  - **User Administration**
  - **User Utilities**
  - **List Administration**
  - **Spam Filtering**
  - **Alias Administration**
  - **Attachment Blocking**
  - **Inbound/Outbound Rules**
  - **White List**
  - **Peer List**

- **New User Interface** for **System Trailer** (also available in the Console Administrator) to maintain the system-wide trailer for both HTML and Plain Text.
- **New Domain Default User Settings**. Previously the System-wide Default User Settings page resided under the User Administration page, which confused users to believe it was a domain level setting. This situation was corrected by moving this page to the System Settings menu, and creating a true Domain Default User Settings page.



Note: Domain Default User level settings override the System Default User level settings.

- **New Domain Default Web Client Preference Settings**. New capability to set Web Client Preferences for new users has been added.



Note: Domain Default Web Client Preference settings override the System Default Web Client Preference settings.

- **New System Default Web Client Preference Settings**. New capability to set Web Client Preferences for new users has been added.
- **New Domain Level Properties Settings**
  - **Enable Image Suppression for E-mail Messages.** Set by default. This new setting will block all images from being viewed, until the link at the top of the e-mail message is clicked to allow the images to always display when selected.
  - **Enable Javascript Removal for E-mail Messages.** Set by default. This new setting will detect and strip any javascript found in a message.

Services

- **SMTP** has been rewritten using .NET for improved plug-in capability. The new SMTP service also has improved performance and stability for a better and more reliable mail delivery.
- **IMail Web Calendar Service (old)** - Will no longer be delivered with new IMail Server installations. The new Web Calendar does not require a service and directly accesses the database. Upgrading from an older version will not delete the old service, allowing continued access to both calendars.

Web Client

- **Advanced Search** enhancement for searching a specific date has been replaced with a fixed format date panel to accommodate internationalized date formats. This date, when selected, can be changed by numerous methods:
  - Selecting the month can be modified in two ways:
    - Typing the first letter of the month or
    - Use of the up and down arrows to scroll through the months.
  - Selecting the date with the use of the up and down arrows to change the date.
  - Selecting the year with the use of the up and down arrows to change the year.

- **New Domain Level Properties Settings for the Web Client**
  - **Enable Image Suppression for E-mail Messages.** Set by default. This new setting will block all images from being viewed, until the link at the top of the e-mail message is clicked to allow the images to always display when selected.
  - **Enable Javascript Removal for E-mail Messages.** Set by default. This new setting will detect and strip any javascript found in a message.

FIXES & NEW FEATURES v11.01

Web Administration

- **Group Aliases** will now recognize the `"alias_name.txt"` file used in older IMail Server editions. It will continue to use the `".lst"` for new group aliases.
- **Active Directory** with large user counts can now be displayed in the User Administration without timing out.
- **Premium Antispam** web admin changes to the proxy settings now correctly update the `"ctipd.conf"` file.
- **Premium Antispam** - Should Premium Antispam (CommTouch) service not be installed, the IP Reputation Log will automatically be disabled. Also modified the user interface to be clear that the "Enable Premium Filter" pertains only to the Premium Content Filter, and not the IP Reputation Log settings.
- **Log Directory** set to non-default directory path now correctly includes ODBC log errors.
- **SQL User Database (ODBC)** has corrected the issue with user flags being reset.
- Required Password Strength was corrected to not allow spaces in the password.
- **"Add User to Collaboration"** which only displayed in the **User Properties** page when the Collaboration User did not exist, has been removed. The IMail Administrator will now be required to create this through the **Collaboration User** page.
- **Specifying a Collaboration User** was corrected to only update the Alternate WorkgroupShare ID when not blank.
- Modifications were made to improve the **page-loading performance** for all Web Administration pages.
- **Mail Archiva** - Search issue with Replies and BCC messages were corrected.

Services

- **SMTP -** Corrected where the received line was showing the IP Address instead of the HELO Host Name.
- **SMTP -** Corrected issue where IP Reputation was not checking the white list.
- **SMTP -** Corrected issue of postmaster bounce using the source IP address vs the domain that generated the bounce.
- **SMTP -** Mail will now relay and auth for 127.0.0.1 correctly.
- **SMTP -** RFC2822 dot stuffing now works correctly.
- **SMTP -** Corrected issue that caused the system logs to fill with errors due to the DATA Command that continued to send data without ending. Error will now log one time and a MAX_SIZE error will be returned before disconnecting.

- **SMTP -** Corrected issue with Access Control list creating exceptions when multiple threads were accessing the list at the same time.
- **SMTP -** Corrected the IPAccessFile error displayed int the api log.
- **SMTP -** Corrected issue with malformed messages where <CR> and <LF> are used individually.
- **SMTP - Syslog** was modified by adding exception handling with user friendly log lines when using verbose logging.
- **SMTP** - Corrected where session was not properly closing connections after max errors were reached, and causing IP addresses to be written over and over to the ACC file causing SMTP to crash.
- **SMTP** will strip trailing nulls on all in-coming messages, and messages generated using the web client will no longer have trailing nulls at the end of the message.
- **Queue Manager** - Copyall no longer crashing Queue Manager for archiving.
- **Queue Manager** - Corrected Attachment Blocking from logging to the root drive to log to the spool file designated path.
- Corrected Notes issue affecting WorkgroupShare setup with SQL database not synchronizing correctly, and displaying only the first character.
- **CommTouch Services** - Corrected the services page for IMailCommTouchAS and IMailCommTouchIpRep which were reversed for stopping and starting.

Web Client

- E-mail format of "test..@domain.com" will no longer be stopped as an invalid mail address format.
- Fixed e-mail not displaying message body correctly for Japanese charset Windows-31j also known as shift_jis.
- Corrected handling of "Q" encoding in the message header.
- Corrected Vacation message encoding to support internationalization.
- Corrected issue with image suppression where users were kicking back to the login screen.
- Corrected Firefox v3 issue with Group Contacts displaying incorrectly.

Install

- **Upgrading** from IMail Standard to v11 will no longer lose contacts and require renaming of the WorkgroupShare Database to recover.
- **Upgrading** from v10 to v11 with a SQL WorkgroupShare Database (not Access DB) will now correctly display the contacts folder for new users.
- **Regcheck.exe** has been corrected and now runs automatically during for repairs and upgrades.
- **IMail Server v11.01** is now compatible with **Microsoft® Windows 2008 R2 Server**.

Mobile Devices

- **Windows Mobile devices** now correctly hide's messages that are marked as deleted when using IMAP. Once a message is deleted and the message has been purged from the mailbox, it will be removed from the mobile device.

Online Help

- Corrected the help for Forwarding Spam to CommTouch.

Archiving

- Corrected the issue of BODxxx.tmp files being generated.

Accessing the IMail Web Administration

After installation, you have the option to launch the IMail Web Administrator automatically. If you choose not to launch the IMail Web Administrator automatically, in your browser address box, type the IP address or URL of the IMail Web Server followed by the Web Admin path.



Note: Administrators can access their web admin using localhost to bypass login, when issues with domain configuration arise. `"http://localhost/IAdmin"`.

Example:

1. http ://123.100.100.80/IAdmin, then press ENTER. The Ipswitch Web Admin login page appears.

   -OR-

   For IMail Server, click **Start** > **Programs** > **Ipswitch IMail Server** > **IMail Server Administration**. The Ipswitch Web Admin login page appears.
2. Enter your **Username** and **Password**. The Installed Ipswitch Products page appears.
3. Click **IMail Server**. The IMail Server Web Admin main page appears.



Note: Web Messaging directly accesses the server to manage mail, and no longer requires IMAP.



Important: Web Messaging requires Queue Manager and SMTP service to be running. Turn on the *Queue Manager* (on page 387) and *SMTP* (on page 392) service in the Web Admin, under the **Services** tab.

Using Internet Information Services (IIS) Virtual Directories

IMail Administrator and IMail Web Messaging (Web client) use Microsoft® Internet Information Services (IIS) virtual directories to identify where the administrator and client Web files are located. By default, the installation program installs the admin files in the IAdmin virtual directory and the client files in the IClient virtual directory.

Changing IIS Virtual Directory names

If you want to change the IMail Administrator virtual directory, you need to change the following registry key entries to the new virtual directory name that you changed in the IIS Console:

- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global\WebRoot
- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Messenger Server \Settings\WebRoot

If you want to change the IMail Web Messaging virtual directory, no registry key change is required.

See the IIS help for additional information about renaming virtual directories.

Additional Resources

The following is a list of resources that you can use to get help with your IMail Server:

IMail Administration Server Help

- Help is always available by clicking **Help** in all Ipswitch products. It provides information about IMail configuration, advanced configuration, services options, mailing lists, and more.

  This online help is also available online at:

  http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/Help/Admin/index.htm

Release Notes

- The release notes, located in the **Start** > **Programs** > **Ipswitch IMail Server > Documentation** folder, provide an overview of changes, known issues, and bug fixes for the current release. The notes also contain instructions for upgrading IMail Server and configuring external databases.

These release notes are also available at:

http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/ReleaseNotes/index.htm

DomainKeys / DKIM Getting Started Guide

- The DomainKeys / DKIM Getting Started Guide was created to assist IMail Administrators with initializing and setting up DomainKeys / DKIM selectors.

  http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/PDF/DomainKeysGSG.pdf

Mobile Device setup to use Microsoft Exchange ActiveSync®

- **Microsoft Exchange ActiveSync®** can be activated with the purchase of a user license.
- The Mobile Client Getting Started Guide is available to assist customers to configure their mobile devices to use Microsoft Exchange ActiveSync®.

  This document will help configure the following mobile devices:

  - Windows Mobile® 5
  - Windows Mobile® 6
  - Windows Mobile® 6.1
  - iPhone™ and iPod Touch™ with Software OS Version 2.2.1 and later

  http://docs.ipswitch.com/_Messaging/IMailServer/v11/Mobile/MobileSync.pdf

Microsoft Internet Information Services (IIS) Help

- Use the IIS help for additional information about IIS setup and configuration.

Archiving Getting Started Guide (Archiving products available separately)

- The Archiving Getting Started Guide will help IMail Administrators in deciding which Archiving option is best for them, and then also to install and setup.
  http://docs.ipswitch.com/_Messaging/Archiving/GettingStarted/Archiving.pdf

- **IMail Server Getting Started Guide**. Provides instructions for planning, installing, and testing your IMail Server software.
  - **http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/GettingStarted/index.htm**
  - **http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/PDF/GettingStarted.pdf**

    -OR-
  - **Start > All Programs > Ipswitch IMail Server > Documentation > IMail Getting Started Guide**.

IMail Support Center

The IMail Support Center provides a number of resources including the following:

User Guides

- Domain Name System (DNS) help
- Access to product updates, utilities, Knowledge Base (KB) articles, and other IMail resources.
- Technical support information, such as e-mail support forms, service agreements, and licensing information.
- IMail user forum, which gives you an opportunity to interact with other IMail and customers to share tips and tricks.

You can access the IMail Support Center at *http://www.imailserver.com/support/* (http://www.imailserver.com/Support/).

Visit Our Web Site

For more information about Ipswitch products and services, visit the Ipswitch web site at *http://www.imailserver.com* (http://www.imailserver.com) for IMail products and *http://www.ipswitch.com* (http://www.ipswitch.com) for all Ipswitch products.

Sales

IMail Sales - (706) 312-3540

Fax - (706) 312-0899

Technical Support

IMail Support - (706) 312-3550

Main Support - (706) 312-3500

Monday	9:00 am - 6:00 pm EST
Tuesday	9:00 am - 6:00 pm EST
Wednesday	10:30 am - 6:00 pm EST
Thursday	9:00 am - 6:00 pm EST
Friday	9:00 am - 6:00 pm EST

Be sure to have your Sales Agreement available before calling.

IMail Getting Started Guide Links

- **http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/GettingStarted/index.htm**

- **http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/PDF/GettingStarted.pdf**

  -OR-

- **Start > All Programs > Ipswitch IMail Server > Documentation > IMail Getting Started Guide**.

Installing 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.

To download software from the Ipswitch web site:

1. In your Web browser, go to: *http://www.imailserver.com/support/patch-upgrades.asp* (http://www.imailserver.com/support/patch-upgrades.asp)
2. Select the appropriate patch or upgrade.
3. Follow the on-screen instructions.



Important: If you are upgrading from IMail Server prior to version 8.1, an LDAP database conversion occurs during installation. The conversion can take a lengthy amount of time depending on the number of domains to convert. If the LDAP data is not available after the upgrade, run the LDAP Convert utility to correct the issue. In the command line utility, type: ldaper /CONVERT /Y

Related Topics

Upgrades/Repairs - *Checking the Registry (regcheck.exe)* (on page 440)

Table of Features

Feature	IMail	IMail Premium	Microsoft Exchange ActiveSync®	IMail Anti-virus powered by BitDefender®	IMail Anti-virus powered by Symantec™
Solid, scalable, standards-based **Email Server** with **Web Mail** and **List Server**	✓	✓			

Basic anti-spam with blacklists, Bayesian filters, phrase filters, and more.	✓	✓			
Basic security with **SMTP** authentication, dictionary attack sensing, and anti-hammering.	✓	✓			
Secure **Instant Messaging** is a network-based Client/Server system with Smart Tag support.	✓	✓			
DomainKeys / DKIM is a domain-level e-mail authentication standard that uses public/private key encryption and DNS to prove e-mail legitimacy.	✓	✓			
WorkgroupShare - Microsoft® Outlook contacts to transfer and sync with IMail Web Messaging and mobile devices.	✓	✓			
Premium Antispam -by **Commtouch** Advanced Security Daemon (aka ctasd™) a plug-and-play email-borne spam and malware outbreak detection daemon.		✓			

Premium Antispam by Commtouch's GlobalView™ Mail Reputation Service (IP Reputation) fights unwanted mail at the perimeter, reducing incoming messages at the entry-point, before these messages enter the network.		✓			
Microsoft Exchange ActiveSync® allows synchronizing their e-mail, contacts & calendars with their mobile devices.			✓		
IMail Anti-virus powered by **BitDefender®**.				✓	
IMail Anti-virus powered by **Symantec™**					✓
Twelve months **Support** and updates	✓	✓		✓	✓

Helpful Definitions

- **Address, Simple vs. Complete:** A complete e-mail address includes the user ID and the domain name; for example, userid@host.companyX.
- **Authenticated users:** Are users who have SMTP Authentication enabled on their e-mail client, or users who send mail from IMail Web Messaging.

  By default, IMail Server forces users to authenticate, unless you select another option such as **Relay Mail for Anyone** or **Relay Mail for Addresses** in the **Mail Relay Settings** (located at the **Services** tab **> SMTP**). This means that every time a user connects to the IMail Server, he/she must enter a user ID and password.
- **Domain (Host) Administrator:** A Domain Administrator can add, modify, or delete users or aliases (except program aliases) on the mail domain (host) he or she has permissions to. Domain Administrators also include all List Administrator permissions.

  Domain Administrators cannot delete System Administrator accounts, permissions, or change other System Administrator settings. Domain Administrators will not display System Administrator rules or file directory information.
- **List Administrator:** A List Administrator can add, modify, or delete any list server mailing list on the mail domain(s) he or she has list admin permissions to.
- **System Administrator:** A System Administrator has full administration capabilities for all IMail permissions and options. System Administrators have both domain and list administrator permissions.
- **User ID:** This is the user ID for the mail account. The user ID must be unique within the domain. It must be between 1 and 30 characters and cannot contain spaces.

  Hyphens can be used in the user ID, but be aware that IMail Server will use the last hyphen in the user ID to delimit a mailbox name.

  Example: If mail is sent to the address mr-fred-account@ipswitch.com, IMail Server reads "accounts" as a mailbox that belongs to mr-fred.



Note: You can change the character used to delimit the mailbox name in a user ID. In the Windows NT registry, add a "GLOBAL IMail key of MailBoxSplitChar" and specify the new character as the first character of the string value.

File Attachment Settings

The installation program automatically configures Microsoft Internet Information Services (IIS) 5.0 or later.

An IIS configuration file, Web.config, is installed during the installation routine. A file attribute, maxRequestLength, in the Web.config file is set to 102400 KB (100 MB). This attribute sets the maximum amount of data that can be uploaded using IIS.

Important: We recommend that you do not change the value of the `maxRequestLength` attribute in the `Web.config` file and that you manage the **Max. Outbound Message Size** and **Single Message Maximum Size** in the Domain Properties page of the Web Administrator. For more information, contact your e-mail administrator.

IMail Processing Order

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

1. **SMTP Access Control.** The SMTPD service checks if the connecting IP is listed in the Access Control dialog box. If it is listed in deny access list, the connection is denied. If it is listed in the grant access list, the connection is allowed and processing continues.
2. **SMTP Kill File.** The SMTP service checks if the e-mail address listed in the "Mail FROM" address command to see if it is listed in the Kill List.. If the address or domain present, the SMTP service returns an error to the connecting client and does not accept the message. If no match is found, the SMTP service accepts the message.
3. **Commtouch's GlobalView™ Mail Reputation Service (IP Reputation available with IMail Premium)**. If enabled, fights unwanted mail at the perimeter, reducing incoming messages at the entry-point, before these messages enter the network.
4. **DomainKeys / DKIM Verification**. If you have DomainKeys / DKIM verification enabled, you can control incoming e-mail identified as spam by signature errors.
5. **Connection Filtering (DNS Black Lists)**. If you have DNS Black Lists enabled, IMail compares the connecting IP address to the black lists to determine if a match occurs. If a match occurs, the e-mail may be deleted (depending on the DNS Black Lists configuration) or an X-Header may be added and processing continues.
6. **Verification Tests.** If you have the verification tests enabled, they verify the "Mail FROM" address, the HELO/EHLO domain, and perform a reverse DNS lookup. If any of these checks fail, the e-mail may be deleted (depending on the configuration) or an X-Header may be added and processing continues.
7. **Sender Policy Framework (SPF).** If you have the SPF feature enabled, it provides increased capability to stop incoming e-mail from forged e-mail addresses. Using a sender authentication scheme, a domain owner requires that legitimate messages from a domain must meet certain SPF criteria. Messages that do not meet the criteria are not accepted as a legitimate e-mail message and are processed according to the SPF options selected on the SPF tab.
8. **IMail Anti-virus.** If you have IMail Anti-virus installed, it checks the message for infected files or code. If infected, the mail is repaired, bounced, redirected, or deleted, according to the settings on the **Anti-Virus** tab. If the file is not infected, content filtering attempts to identify whether the message is spam .
9. **Premium Antispam.** If you have the optional Premium Antispam filter installed, it provides automated spam protection in addition to the Standard Antispam filter included in IMail. Premium Antispam filter settings are applied before Standard Antispam filter settings.

10 **Content Filtering.** If you have content filtering enabled, it determines if the message is likely to be spam. If the message is determined to be spam, it is either deleted, sent to the specified address, or an X-Header is inserted. If the message is not spam, aliases are checked.

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

- If there is a match to a program, IMail Server executes the program.
- 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.
- If there is a match to a list-server mailing list name, IMail Server (a) processes the mail according to the settings for that list, and (b) checks the user IDs specified in the list settings.
- If no match to any alias, IMail Server checks the user ID.

12 **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, the delivery rules for a list-server mailing list are checked.

13 **Delivery rules.**

a) **Delivery Rules for the List-Server mailing list.** If the message matches the rule criteria for a list, delivery follows according to the rule. If not, then the message is sent to the list server. If the message is not addressed to a list, **Forwarding** is checked.

b) **Delivery Rules for the Host.** IMail Server determines if the message matches a rule for the mail host. If so, delivery follows according to that rule. If not, then rules for the user ID are checked.

c) **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 the rule. If not, then **Info Manager** is checked.

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

15 **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.

16 **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.

CHAPTER 2

Installing

In This Chapter

Installing IMail Server Administrator 29
Setting the E-Mail Domain Name (Official Host Name) 30
Setting Up an Alias for a Host 30
Setting Database Options 31
Installing SSL Keys 32
Folder Permissions and IIS Configuration 32
Installing Patches and Upgrades 37
Using the IMail Installation Log File 38

Installing IMail Server Administrator

IMail Administrator uses InstallShield® Wizard to install the IMail Server on your computer. Use the on-screen instructions to select the installation features that set up the mail server to your requirements.

In addition to using the IMail installation program, the following software components should be installed on your mail server computer to make the mail server fully functional:

- Microsoft® .NET Framework 2.0
- Windows Script 5.6 (part of Microsoft Internet Explorer 6)
- (Recommended) Microsoft Internet Information Services (IIS) 5.0 or later
- Microsoft Data Access Component (MDAC) 2.6 or later

Install will prompt for any components that are not installed on the server and will cancel installation, until the component is installed.



Note: Administrators can access their web admin using localhost to bypass login, when issues with domain configuration arise. `"http://localhost/IAdmin"`.

Related Topic

Upgrades/Repairs Only - *Checking the Registry (regcheck.exe)* (on page 440)

System Requirements (on page 6)

Setting the E-Mail Domain Name (Official Host Name)

Enter the complete e-mail domain name (official host name) for your IMail Server. For example, mail.domain.com.

IMail Server installation wizard attempts to automatically enter the fully qualified domain name of the machine for this field. Confirm (or enter) the official host name of the system on which you are installing IMail Server. This will be the "primary host."

The mail server host name and domain must be registered in the DNS (Domain Name System) in order for remote hosts to be able to communicate with your e-mail server. Your DNS must contain the proper entries for the host name you see here.

If you have any doubts about what to enter for the e-mail domain name, you can exit the installation program and check the DNS information for the system on which you intend to install IMail Server (the primary host).

The DNS server for the local network must appear as the first listed item on the Domain tab menu list box. See *Managing Domains* (on page 110) for more information.

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 Host* (on page 30).

Setting Up an Alias for a 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 recognizes 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 must enter "domain.com" as an alias for the official host name. It can be entered in the **Domain Aliases** box on the Domain Properties page. To access the Domain Aliases box, see Getting to Domain Properties.

Example:

If the mail domain 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 fred@domain2.com.



Note: Host Alias requires also that the proper updates to DNS must be made to work correctly.

Setting Database Options

Select the database you want to store user accounts in:

- **NT/AD User Database.** IMail Server creates a user mail account for each user listed in the Windows NT Database, or Active Directory.



Note: Use the Windows NT User Manager to add or delete users. You cannot add or delete users using IMail Administrator.

- **IMail User Database.** User IDs and passwords for mail accounts are stored in a database on the IMail Server (in the registry).
- **External Database (ODBC Compliant).** IMail uses an *external database* (on page 68) to register and authenticate users. Users that you add and delete using IMail will be added to and deleted from that external database and vice versa.

System DSN

If you select *External Database* (on page 68), you must specify the ODBC System Data Source Name (DSN) for the database where the user information is stored. IMAILSECDB is the default name that the IMail ODBC link uses.

Installing SSL Keys

The IMail Server provides an SSL (Secure Sockets Layer) capability that lets Web Calendaring clients, SMTP , POP3 , and IMAP connect more securely. The SSL capability relies on keys that are stored in the Windows registry.

- If you have a third-party SSL certificate, click **No**. After installing IMail, create a *Self-Signed SSL Certificate(sslutility.exe)* (on page 443)
- If you do NOT 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 install default keys later.

Related Topic

Self-Signed SSL Certificate(sslutility.exe) (on page 443)

Folder Permissions and IIS Configuration

IMail Folder Permissions and IIS Configuration

Folder Rights

Product	Folder	User	Rights
Web Admin	Product Folder (C:\Program Files\Ipswitch\Messaging)	computername \IUSR_ computername Important:If using Microsoft Windows 2000: 1) Grant the Anonymous user listed in the IIS configuration rights to Act as part of operating system. - OR - 2) Create another account for the IIS virtual directory to run under. Any users created to run under IIS must be granted rights to Act as part of operating system. Note: If a user exists prior to installing ICS or	Full

		IMail, the Anonymous user permission settings in IIS are applied to all files and folders.	
Web Admin	C:\Program Files\Common Files\Softalk	computername \IUSR_ computername Important:If using Microsoft Windows 2000: 1) Grant the Anonymous user listed in the IIS configuration rights to Act as part of operating system. - OR - 2) Create another account for the IIS virtual directory to run under. Any users created to run under IIS must be granted rights to Act as part of operating system. Note: If a user exists prior to installing ICS or IMail, the Anonymous user permission settings in IIS are applied to all files and folders.	Full
Web Admin	WorkgroupShare install folder, if outside of ICS folder	computername \IUSR_ computername Important:If using Microsoft Windows 2000: 1) Grant the Anonymous user listed in the IIS configuration rights to Act as part of operating system. - OR - 2) Create another account for the IIS virtual directory to run under. Any users	Full

		created to run under IIS must be granted rights to Act as part of operating system. Note: If a user exists prior to installing ICS or IMail, the Anonymous user permission settings in IIS are applied to all files and folders.	
Web Admin	HKEY_LOCAL_MACHINE\Software\Ipswitch (Registry)	computername \IUSR_ computername Important:If using Microsoft Windows 2000: 1) Grant the Anonymous user listed in the IIS configuration rights to Act as part of operating system. - OR - 2) Create another account for the IIS virtual directory to run under. Any users created to run under IIS must be granted rights to Act as part of operating system. Note: If a user exists prior to installing ICS or IMail, the Anonymous user permission settings in IIS are applied to all files and folders.	Full
Web Client w/ IIS 6+	Product Folder (C:\Program Files\Ipswitch\Messaging)	computername \IUSR_WPG Note: If a user exists prior to installing ICS or IMail, the Anonymous user permission settings in IIS are applied to all files and	Full

		folders.	
Web Client w/ IIS 6+	Product Folder (C:\Program Files\Ipswitch\Messaging)	IIS_WPG Note: Typically, in Windows 2003, Network Service is the member of the IIS_WPG group.	Full
Web Client w/ IIS 5	Product Folder (C:\Program Files\Ipswitch\Messaging)	ASPNET Important: If using Microsoft Windows 2000, use IWAM_<machinename> instead of ASPNET. Also provide the user with with registry and folder permissions. Any user must be given rights to Act as part of the operating system.	Full
Web Client w/ IIS 6+	HKEY_LOCAL_MACHINE\Software\Ipswitch (Registry)	IIS_WPG Note: Typically, in Windows 2003, Network Service is the member of the IIS_WPG group.	Full
Web Client w/ IIS 5	HKEY_LOCAL_MACHINE\Software\Ipswitch (Registry)	ASPNET Important: If using Microsoft Windows 2000, use IWAM_<machinename> instead of ASPNET. Also provide the user with with registry and folder permissions. Any user must be given rights to Act as part of the operating system.	Full

IIS Settings

Enable ASP and ASP.NET	Path: C:\Program Files\Ipswitch\Collaboration

(Version 6+ only)	Suite\WebDir\WebAdmin Default Document: default.asp Application Pool (IIS 6): DefaultAppPool Application Protection (IIS 5): Medium
Create Virtual Directory: IAdmin	Path: C:\Program Files\Ipswitch\Messaging\WebDir\WebClient Default Document: default.aspx Application Pool (IIS 6): DefaultAppPool Application Protection (IIS 5): Medium
Create Virtual Directory: IClient	Disable anonymous access to the following directory: Directory: IMail/Services Under the Virtual Dir: IAdmin Disable anonymous access to the following file: File: IIM/Status.asp
Disable Anonymous Access	Disable anonymous access to the following directory: Directory: IMail/Services Under the Virtual Dir: IAdmin Disable anonymous access to the following file: File: IIM/Status.asp
Enable Parent Paths	Enable Parent Paths for the following virtual directories: IAdmin IClient

Important:

- If Microsoft .NET is installed, but not configured to work with IIS, run the following command: x:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i -enable (where x: is the appropriate drive letter).
- If your mail domain is using an external user database, then you must set user permissions for the external database for it to function correctly in ICS.

When you configure a DSN to an SQL data source in the Microsoft Windows ODBC Data Source Administrator, it may default to Named Pipes network library. Make sure that you set the connection type to TCP/IP in order for the external database to work correctly.

- If you are currently using an external user database with an earlier (pre-v7.0) version of IMail, you must add a new set of required columns to the database table in which user information is stored. Please refer to the "External Database Changes" entry in the Release Notes section of this document for details.
- If you are upgrading from IMail Server prior to version 8.1, an LDAP database conversion occurs during installation. The conversion can take a lengthy amount of time depending on the number of domains to convert. If the LDAP data is not available after the upgrade, run the LDAP Convert utility to correct the issue. In the command line utility, type: ldaper /CONVERT /Y
  For more information, see the IMail Administrator Help.
- If you select an install directory other than the default install directory, make sure that the IIS IUSR_<computer name> user has Administrative access to that install directory. For more information, see the Folder Rights section.

Using IIS Virtual Directories

IMail Administrator and IMail Web Messaging (Web client) use Microsoft Internet Information Services (IIS) virtual directories to identify where the administrator and client Web files are located. By default, the installation program will install the admin files in the IAdmin virtual directory and the client files in the IClient virtual directory.

Changing IIS Virtual Directory names

If you want to change the IMail Administrator virtual directory, you need to change the following registry key entries to the new virtual directory name that you changed in the IIS Console:

- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global\WebRoot
- HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\Messenger Server\Settings\WebRoot

  If you want to change the IMail Web Messaging virtual directory, no registry key change is required. See the IIS help for additional information about renaming virtual directories.

Installing 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.

To download software from the Ipswitch web site:

1. In your Web browser, go to: *http://www.imailserver.com/support/patch-upgrades.asp* (http://www.imailserver.com/support/patch-upgrades.asp)
2. Select the appropriate patch or upgrade.
3. Follow the on-screen instructions.

Important: If you are upgrading from IMail Server prior to version 8.1, an LDAP database conversion occurs during installation. The conversion can take a lengthy amount of time depending on the number of domains to convert. If the LDAP data is not available after the upgrade, run the LDAP Convert utility to correct the issue. In the command line utility, type: ldaper /CONVERT /Y

Related Topics

Upgrades/Repairs - *Checking the Registry (regcheck.exe)* (on page 440)

Using the IMail Installation Log File

The IMail installation wizard generates an install log file to help you troubleshoot software installation issues. If you selected the default installation folders, the log file is located in C:\install-log-mm-dd-yyyy.txt.

During installation each action that occurred with respect to permissions or IIS is prefixed with "***".

Permissions are logged as follows:

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program Files\Ipswitch\IMail" /T /E
/G IUSR_WIN2K3- SRVR:F

processed dir: C:\Program Files\Ipswitch\IMail

processed file: C:\Program Files\Ipswitch\IMail\ActivationStub.exe

processed file: C:\Program Files\Ipswitch\IMail\AVReadMe.htm

processed file: C:\Program Files\Ipswitch\IMail\IMailLogo.jpg

processed file: C:\Program Files\Ipswitch\IMail\css_releasenotes.css
```

Tip: If you want to search the log file for failures, search the log file for the strings **"No Mapping" or "!!!."**

The first line is the command string used to set the permissions. If this fails, instead of seeing "processed" lines in the log file, you will see:

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program
Files\Ipswitch\Collaboration Suite" /T /E /G IUSR_WIN2K3- SRVR:F
```

No mapping between account names and security IDs was done.

IIS settings in the log file are not as detailed. If the item is not prefixed with "!!!" followed by "Failed," then it was successful. For example, the first line in the following example is a success:

```
*** Disabling anonymous rights on "IIM /Status.asp".

*** Disabling anonymous rights on "IIM/StartStopServices.asp".
```

The following line, disabling the anonymous rights on IIM/StartStopServices.asp, failed because it is followed by an "!!! Failed.":

```
!!! Failed to disable anonymous rights on "IIM/StartStopServices.asp".
```

CHAPTER 3

Mail Domain (Host) Configuration

In This Chapter

Domain Properties 41
Adding a New IMail Domain 47
Configuring an NT/AD database 52
About Virtual Mail Domains (Hosts) 53
LDAP Settings 54
Bouncing Spam Messages using Rules 55
Setting up a Dial-up Internet Connection 57
Changing the IP Address of a Host 60
Setting Up a Mail Gateway 61
Setting up IMail Server as a Backup Mail Spooler 62

Domain Properties

How to get here

Use the Domain Properties to add a new mail domain, add or update a domain alias, enable virus scanning, and set other message and mailbox properties.

General Domain Settings

- **Domain Name (Official Host Name or OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **TCP /IP Address**. Select **Select an IP Address** to use an IP address (domain) for the mail domain or select **Virtual** (*virtual IP address* (on page 53)) to use a non-IP-ed domain.



Note: If you change a primary domain to a virtual domain, you must restart ALL services. See *Changing the IP Address of a Host* (on page 60) for more information.

- **Top Directory.** Enter the name or **Browse** to the directory where users, lists, and web files for this mail domain are stored.

- **Domain Aliases**. Specify alternate domain names for which you want the mail domain to accept mail. Multiple aliases are separated by a space. This field is limited to 255 characters.

Note: If the Domain Alias name is changed, stop and restart all services via the *Service Administration* (on page 367) page in order for the change to take effect correctly.

Example: If the mail domain 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 fred@domain2.com.

Note: Host Alias requires also that the proper updates to DNS must be made to work correctly.

Domain Options

- **Enable Microsoft Exchange ActiveSync®**. (Enabled by default) Allows all enabled users for the specified domain to use ActiveSync® for synchronizing mobile devices with their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. Once installed Outlook will synchronize e-mail, contacts, calendars, notes, and tasks with their mobile devices.

  See the **Mobile Synchronization Setup** (on page 80) for more information.

Warning: Disabling ActiveSync® at the domain level will disable all ActiveSync® users on the specified domain, overriding the User Property setting.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

- **Enable Web Calendar.** Specify whether the current mail domain allows access to the Web Calendaring Service (if available in software version).
- **Enable Ipswitch Instant Messaging** (selected by default if available in software version). Specify whether the current mail domain will allow access to the Ipswitch Instant Messaging service.

Note: If Enable Ipswitch Instant Messaging and/or Enable Web Calendaring is selected at the mail domain level, it can be selected or cleared for each user of the mail domain on the *User Properties* (on page 126) page.

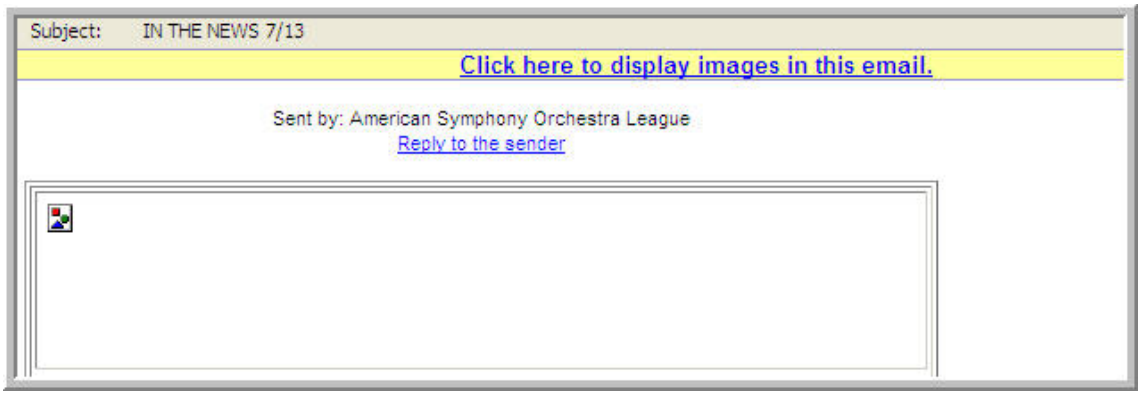
- **Enable Virus Scanning** (selected by default if available in software version).
  - If this option is selected, virus scanning is performed for:
    - the primary domain

- any virtual domain (IP-less) that is bound to the primary domain

- If this option is cleared, virus scanning is performed for:
  - any virtual domain (IP-less) that is bound to the primary domain and has the anti-virus option selected at the virtual domain level.

- **Enable image suppression for e-mail messages**. Checked by default. This feature will suppress images for all messages. Once the link has been clicked, the images will always display when the message is selected.

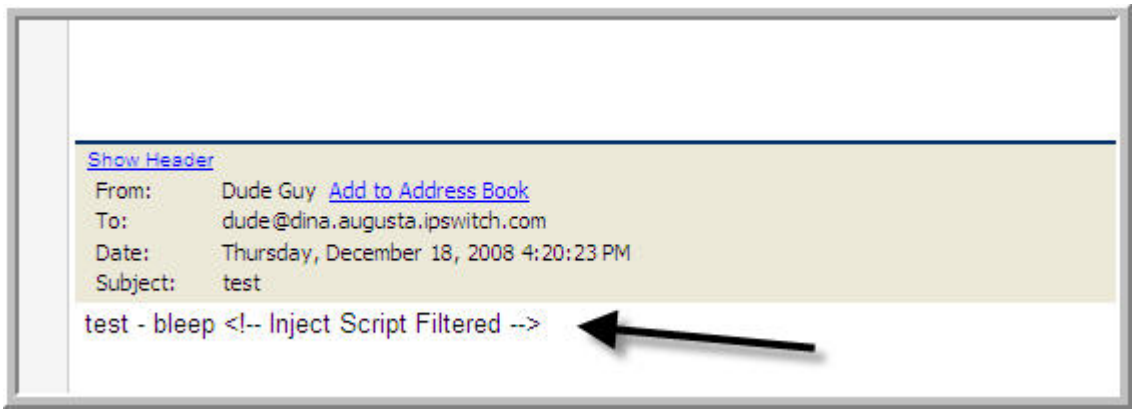
  A link will appear as seen below:



Note: Once this link is clicked, the images will always display when the message is selected.

- **Enable javascript removal for e-mail messages**. Checked by default. This feature when checked will search all messages and disable any javascript encountered.

  Example showing that a script was removed:



- **Enable content filtering for authenticated users.** Select this option to enable content filtering for all messages that are received from authenticated users.

Note: Even if the **Enable content filtering for authenticated users** option is selected, content filtering is not performed on messages that are sent from system and host administrators. This prevents mail from being filtered twice in cases where a message is misidentified as spam and the administrator then forwards it on to its intended recipient.

Note: The primary domain is identified in the **Domain Name** box.

Message and Mailbox Options

- **Default Maximum Mailbox Size.** (0 is default value). Enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account. Enter zero for an unlimited mailbox size for each user.
- **Max. Outbound Message Size.** (0 is default value). Enter the maximum size (in bytes, KB, MB, or GB) of an outbound message. Any message that is larger than the size entered will be bounced. Enter 0 for an unlimited maximum outbound message size. For more information, see *File Attachment Settings.* (on page 26)
- **Single Message Maximum Size.** (0 is default value). Enter the maximum size (in bytes, KB, MB, or GB) of a single message. Messages that exceed this size are returned to the sender. Enter 0 for an unlimited single message maximum size. For more information, see *File Attachment Settings.* (on page 26)
- **Full Mailbox Notify (percentage).** (0 is default value). Enter a percentage that users will be notified when their mailbox is within a specified percentage of being full. Enter 0 for no full mailbox notification. *Example* (on page 71). See also *customizing the notification message* (on page 71).
- **Full Mailbox Notify Address.** Enter 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 administrator's address.
- **Default Maximum Messages.** (0 is default value) Enter the default maximum number of messages allowed in each user's mailbox. Enter 0 for an unlimited number of messages.
- **Maximum User Count.** (0 is default value) Enter the maximum number of users that can be registered for this mail domain. Enter 0 for an unlimited number of users.
  - **Domain Administrators** will not be able to add users once the Max User Count has been met. A message on the User Administration page will also display: "The User Limit for the domain has been reached".
  - **System Administrators** will still be allowed to add users, but a message on the User Administration page will still display: "The User Limit for the domain has been reached".

Tip: The user count configured on the Domain Properties page **DOES NOT** include Root.

- **Current User Count**. Displays the current number of users registered for this mail domain.

- **Sub- mailbox Creation.** Select how to handle a message when it arrives for a user and is addressed to a sub-mailbox that does not exist. Select one of the following actions:
  - **Create.** (Default setting) Creates the sub-mailbox and delivers the message.
  - **Send to Inbox.** Does not create the sub-mailbox. Instead the message is delivered to the "main" mailbox.
  - **Bounce.** Bounces the mail back to the sender as an invalid e-mail address.
- **Minimum POP Frequency (minutes).** Enter the number of minutes delay between POP logins for each user. The default is 0 (or unlimited) logins.



Caution: If you enter any number of minutes for Minimum POP frequency, you are limiting popping to one mailbox per user per domain. If you create more than one mailbox for a user, that mailbox will receive mail, but the user will be unable to access it unless the POP frequency is set at 0 (zero). An error message is sent to the client and logging in is denied, Different e-mail clients may handle this error differently.



Example: Outlook and Outlook Express display the userid/password dialog box continuously. If you click **Cancel,** the error message the POP server returns is: "-ERR login frequency exceeded - try again later" User Database Setting.



User Login Settings



Tip: To reset a suspended account, go to User Properties page and uncheck "Account Suspended" check box. This will reset the user's failed login attempts to zero.



Tip: A successful login will also reset failed login attempts to zero.

- **Allowed Login Attempts Before Account Lockout** (Default Setting = 3). Allows the user "X" login attempts before displaying:

  "You have exceeded the maximum number of allowed login attempts. Please try again later."



Note: Setting **Allowed Login Attempts for Account Lockout to zero (0)** will disable this feature.

- **Allowed Lockouts Before Account Suspension**. (Default Setting = 3). Allows the user "X" of the above message before being suspended and requiring an Administrator intervention, with the message:

"Due to multiple failed login attempts, your account access has been suspended."



Note: Setting **Allowed Login Attempts for Account Suspension to zero (0)** will disable the feature.

Drop down text box contains the following password complexity settings:

- **0 - Weak** (Default Setting). Requires password to be:
  - Must be at least 3 characters in length
  - And not to exceed 30 characters
  - White space characters are not allowed
- **1 - Simple.** Requires password to be:
  - Must be at least 6 characters in length
  - And not to exceed 30 characters
  - Must contain at least 1 letter (regardless of case)
  - Must contain at least 1 number or special character
  - White space characters are not allowed
- **2 - Moderate.** Requires password to be:
  - Must be at least 6 characters in length
  - And not to exceed 30 characters
  - Must contain at least 1 letter (lower case)
  - Must contain at least 1 number
  - Must contain at least 1 special character or 1 capital letter
  - White space characters are not allowed
- **3 - Strong.** Requires password to be:
  - Must be at least 8 characters in length
  - And not to exceed 30 characters
  - Must contain at least 1 lower case letter
  - Must contain at least 1 capital letter
  - Must contain at least 1 number
  - Must contain at least 1 special character
  - White space characters are not allowed
- **4 - Extreme.** Requires password to be:
  - Must be at least 8 characters in length
  - And not to exceed 30 characters
  - Must contain at least 2 lower case letters

- Must contain at least 2 capital letters
- Must contain at least 2 numbers
- Must contain at least 2 special characters
- White space characters are not allowed



Note: Valid special characters `[! @ # $ % ^ & * ( ) _ + } { " : ' ? / > . < ; , ]`

User Database Setting

- **User Database Type** area, select one of the following:
  - *IMail Database* (on page 68)
  - *NT/AD Database* (on page 65)
    - **Configure.** Click to *Configure your NT or Active Directory database* (on page 52).
  - *External Database* (on page 68)
    - **Configure.** Click to *Configure an external database.* (on page 68)

Save. Click **Save** to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Related Topics

Adding a New IMail Domain (on page 47)

Adding a New IMail User (on page 143)

Creating an E-mail Alias (on page 185)

Changing the IP Address of a Host (on page 60)

Virtual mail domains with IP addresses (on page 123)

Virtual mail domains without IP addresses (on page 123)

Adding a New IMail Domain

How to get here

Use the User Properties to change a user's settings, such as: user password, user ID, maximum mailbox size and maximum number of mailbox messages, add user to Collaboration, and change other user mailbox properties.

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **Domain Name(OHN)**. This clickable link displays only for existing users. This link will take you to the **Domain Properties** page.
- **Username.** Enter a unique user ID (user name) for the e-mail account. User IDs are limited in length to 1 to 30 characters and must be created from alphanumeric characters. The User ID cannot include spaces and must be a unique name within the domain you are adding the user to.
- **Full name.** Enter the user's First Name and Last Name.
- **Reply To Address.** Enter an e-mail address that you want to have IMail Server automatically use as your Reply To mail address. You can leave this text box empty to let recipients of this user's messages reply to the User ID you entered. You can also enter an e-mail address that omits the domain 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 Stephanie@mail.ipswitch.com, you can enter Stephanie@ipswitch.com.
- **Forwarding Address.** Enter an e-mail address that you want to have IMail Server automatically forward a user's mail to.



Example 1: To forward messages to another mailbox besides INBOX by entering the forwarding address as `"yourUserID-othermailbox@domainname.com".`



Example 2: To forward e-mail to another mailbox and also keep a copy in the original mailbox by preceding the e-mail address with `"."` allowing no spaces in between. `".,userid@domainname.com"`

- **Maximum Mailbox Size.** (0 is default value) Enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account. If the user's Maximum Mailbox Size is zero, the defaults for the e-mail domain are applied to the user. If the domain's default is also zero, the Maximum Mailbox Size for the user is unlimited. If a new message will cause the total size of all mailboxes in a user's account to exceed the Maximum Mailbox Size value, the mail is returned to the sender.



Note: Currently the maximum allowed mailbox size is 2 GB.

When the Maximum Mailbox Size value is non-zero, it will override the e-mail domain's default settings. In this case, the 0 value is no longer unlimited for the domain default settings.

The following will occur when a users mailbox is over the **Max Mailbox Size**:

- All new incoming mail will no longer be received, they will get bounced.
- New messages can still be sent.

- Other users sending messages to a users full mailbox will receive a postmaster message stating the user's mailbox is exceeding the allowed limit.
- When users mailbox is below the **Max Mailbox Size**, it will begin receiving mail again.

- **Maximum Mailbox Messages.** (0 is default value) Enter the default maximum number of messages allowed in each user account. If the user's Maximum Mailbox Messages is zero, the defaults for the e-mail domain are applied to the user. If the domain's default is also zero, the Maximum Mailbox Messages for the user is unlimited.

  When the Maximum Mailbox Messages value is non- zero, it will override the e-mail domain's default settings. In this case, the 0 value is no longer unlimited for the domain default settings.



Note: If the **Max Mailbox Messages** option is set to 5, and the user's main mailbox already has five messages stored, then the next message sent to the user's main mailbox is bounced. However, if the next message is sent to a sub-mailbox instead, the message is delivered as long as there are less than five messages currently stored in the sub-mailbox.

- **Encoding**. Default message encoding used for sending messages. Default setting is Unicode (UTF-8).
  - **Unicode (UTF-8).** Choose this character set for multi-language mail. In IMail, this includes English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish.
  - **English (US-ASCII).** For composing e-mail for English-speaking readers, based on the English alphabet.
  - **Western European (ISO-8859-15).** For composing e-mail in French, Italian, German, or Spanish.
  - **Chinese Traditional (BIG5).** For composing e-mail in traditional Chinese.
  - **Chinese Simplified (GB2312).** For composing e-mail in simplified Chinese.
  - **Japanese (ISO-2022-JP).** For composing e-mail in Japanese.
- **Allow Password Change** (selected by default). Select to let the user change his/her password in Web Messaging.
- **Account Enabled** (selected by default). Select to let the user use the e-mail account remotely through POP3 or IMAP4. You can clear this option to disable the account without changing the user's password or removing him/her from the domain.
- **Access Information Services** (selected by default). Select to make the user's LDAP information available in the LDAP database.

Caution: Clearing the **Access Information Services** check box permanently deletes the user's information from the LDAP database and prevents distribution of user information via the IMail LDAP service. There is currently no method available to hide information within an OpenLDAP database, except to use this option to clear user information. If you want to show LDAP information for this user after clearing this option, you must add the LDAP information back into the user information.

- **Access LDAP Attributes** (selected by default). Select to let the user modify his/her LDAP attributes (name, address, organization, etc.).
- **Allow Web Calendaring.** Select to let a user access IMail Web Calendaring.
- **Allow Use of Ipswitch Instant Messaging.** (Only present if Ipswitch Instant Messaging is installed). Select to let the user have access to Instant Messaging. Clear the check box to disable the user's access.
- **Allow Web Access.** Select to let a user access his/her IMail Web Messaging client.
- **Account Suspended.** Automatically becomes enabled if a user's web access becomes suspended from the settings set in the **Domain Properties > User Login Settings.** To re-enable web access web access for the user Account Suspended must be manually unchecked.

Note: This feature is controlled on a per domain basis in *Domain Properties* (on page 41) under **User Login Settings**.

- **Allow Microsoft Exchange ActiveSync®**. (Not set by default) Enables a user with a mobile device to synchronize using ActiveSync® to their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

  Disabling this feature at the User Property level will disable synchronization for only the specified user.

  See the **Mobile Synchronization Setup** (on page 80) for more client help.

Note: Disabling Exchange ActiveSync® at the User Property Level will disable mobile synchronization for only the specified user.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

- **List Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete any list server mailing list on the mail domain(s) he or she has List Administrator permissions to.
- **Domain Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete users and aliases (except program aliases) on the mail domain (host) he or she has domain administrator permission to.

- **System Administrator Permissions** (cleared by default). Select to let a user have full administration capabilities with all IMail features and options. System Administrators have Domain Administrator and List Administrator permissions.

Lists and Groups Aliases

- **Lists**. Select the available domain's list(s) from the list box to which the user wants to subscribe.
- **Group Aliases.** Select the available domain's group alias(es) from the list box to which the user wants to belong.

 **(Add to)**. Select row and click to add.

 **(Remove from)**. Select row from user text box and click to remove.

 **(Add All)**. Click to add all rows to users text box.

 **(Remove All)**. Click to remove all rows from users text box.

Change Password

Depending on the *Domain Setting for User Login Settings > Password Strength* (on page 41) which controls the complexity of user passwords. Dialog will display the password strength required when modifying.

- **Password.** Enter a new password. Passwords are limited in length to 3 to 30 alphanumeric characters and cannot include asterisks.
- **Confirm Password.** Enter the user password a second time to confirm the password.

Related Tasks

- *Add User to Collaboration* (on page 147)
- *Specify Corresponding Collaboration User* (on page 147)



Note: After a user is added to Collaboration via the **Add User to Collaboration link**, this link changes to **Grant Access to a Public Folder.** However, if the new collaboration user's current e-mail address is not used in the **Account E-mail** text box, the user is not recognized as the same user and the **Add User to Collaboration link continues to display** for the user.

Save. Click to save changes.

Related Topics

Adding a IMail User (on page 143)

Deleting an IMail User (on page 148)

Adding Users Using Adduser.exe (on page 422)

Default User Settings (on page 98)

User Utilities (on page 136)

Configuring an NT/AD database

Use this page to configure your NT or Active Directory database. See also *Using the Windows NT/AD Database* (on page 65).

NT Database

- **NT Domain Name.** Enter the name of your NT Domain.
- **Machine name of Domain Controller.** Enter the machine name for your Domain Controller.

Active Directory Database



Important: To hide Active Directory users from the IMail Server, under user properties, add the word "built-in" in the front of the user description. *Example.* (on page 52)

- **Use Active Directory**. Select the check box to use Active Directory.
- **Naming Context.** If the Active Directory check box is selected, the naming context will be pulled from the Root DSE Directory Service Entry. If you choose to not use the default naming context, you can enter one of your choice.
- **Test.** Click to test the naming context. A successful test will tell you how many users are in that context.

- **OK.** Click to save your settings.
- **Cancel.** Click to cancel your settings and return to the Domain Properties page.

Related Topic

Example of Active Directory "built-in" (on page 52)

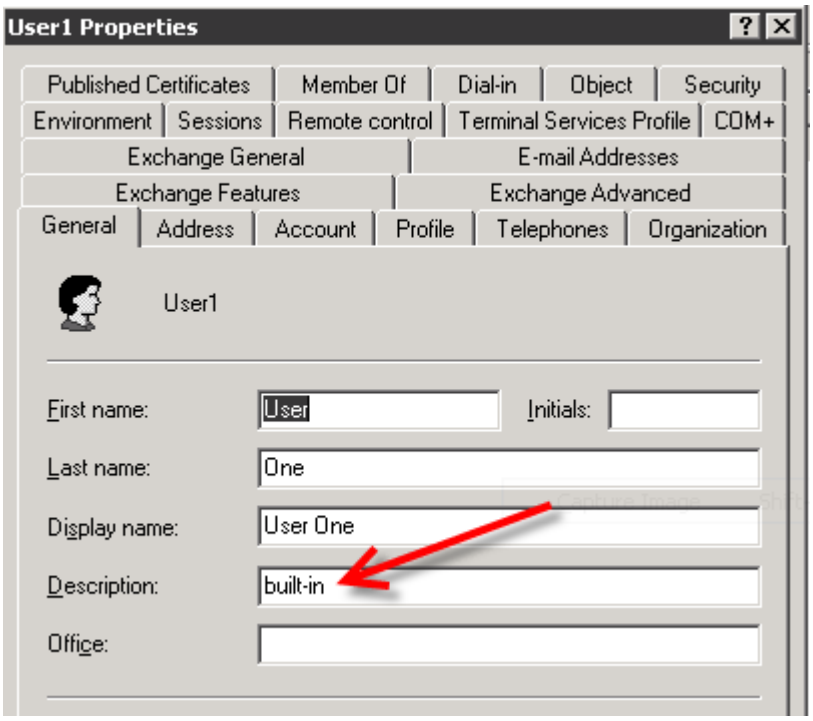
Example of Active Directory "built-in"

The example below will hide User1 from the IMail Server as a valid user.

1. Go to **Start > Control Panel > Administrative Tools > Active Directory (AD) Users and Computers**.
2. Select **AD** container with users.

3 Right click specified user that you would like to hide from the IMail Server, and select **Properties**.
4 Enter the word `"built-in"` into the **Description** field.
5 Click **"OK"**

Note: `"built-in"` must be at the front of the **description** text box. Trailing words are permitted.



Related Topics

Domain Properties (on page 41)

Configuring NT/AD Database (on page 52)

About Virtual Mail Domains (Hosts)

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

There are two types of virtual mail domains:

- *Virtual mail domains with IP addresses* (on page 123)
- *Virtual mail domains without IP addresses* (on page 123)

Note: Whether you use a virtual mail domain with an IP address or without an IP address, you must make DNS entries for your domain(s).

Related Topics

Adding a New IMail Domain (on page 47)

Setting Up a Virtual IMail Domain With an IP Address (on page 123)

Setting Up a Virtual IMail Domain Without an IP Address (on page 123)

LDAP Settings

How to get here

Use the LDAP Settings page to configure host options for OpenLDAP. This information is necessary for an LDAP client to edit the LDAP database. It is not necessary to enter an ID or password if you only want to view the OpenLDAP data.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

LDAP Settings

- **LDAP Admin ID.** Displays the LDAP administrator ID for the e-mail domain. This information is auto-populated. The administrator ID cannot be an IMail user ID.
- **Password.** Enter the LDAP administrator password.
- **Confirm Password.** Enter the password a second time to confirm the original password. The two password entries must match in order for the value to be saved.

Caution: Do not click **Initialize LDAP** unless you want to overwrite the database with the user IDs only that are stored in the Windows registry. First try synchronizing the LDAP database to resolve any problems.

Important: Because the password is randomly generated during installation and importation, we highly recommend that you change it as soon as possible after completing setting up LDAP.

Important: You can also use the *iLDAP.exe utility* (on page 382) to Init or Sync a specified LDAP domain or all the LDAP domains. This utility can be used in the case when the Web Administrator does not properly Init or Sync all the LDAP domains on a server. This issue sometimes occurs on servers running Microsoft Windows 2003 machines with over 30 domains.

LDAP Actions

- **Init LDAP (Initialize the LDAP database).** Click to Initialize the LDAP database created for the current e-mail domain by the *LDAP server* (on page 375).
- **Sync LDAP (Synchronize the LDAP database).** Click to synchronize the LDAP database. Synchronizing removes multiple database entries, deletes old accounts, and adds new accounts.

Save. Click to save settings. An "**Update Successful"** message and the time of the update appear.

Related Topics

About LDAP Server (on page 375)

About LDAP Data (on page 376)

LDAP Service Settings (on page 377)

LDAP User Information (on page 150)

Populating the LDAP Database Using Ldaper.exe (on page 381)

Init & Sync LDAP DB - iLDAP.exe utility (on page 382)

Bouncing Spam Messages using Rules

To bounce a message that is identified as spam, you must set up a delivery rule at the host level. Before you setup a rule, determine the reason you want to bounce spam messages and identify the corresponding X-IMAIL-SPAM header that is inserted into these types of messages (i.e. X-IMAIL-SPAM- DNSBL). If you want to bounce all spam messages regardless of the reason it was identified as spam, you need to create a rule or rules that search for the generic X-IMAIL- SPAM header. For more information, see *Spam X-Header Explanations* (on page 330).

Example:

The following example assumes that you want to bounce all messages that are identified as spam.

To bounce a message that is identified as spam:

1. Make sure that all of the antispam features are setup with the **Insert** X-Header action to be taken when e-mail is determined to be spam. For more information, see Getting to IMail Inbound Rules Options.
2. Click on an e-mail domain's **Inbound Rules** (on page 220) page, then click **Add**. Enter the following rule parameters:

Field: Header

Comparison: Contains

Search Text: X-IMAIL-SPAM

1. Click **Add**. The new rule is added to the list of rules.
2. Select the rule you just added.
3. On the **Action Type** list, select **Bounce**.
4. Click **Save**.

IMail Server Default Service Ports

Ports are used to facilitate communications between client and server programs, such as *IMail Administrator services* (on page 370). The following are the default service ports for IMail Server and can be configured.

TCP Ports:

- SMTP : Port 25
- SMTP Alternate Port : 587
- SMTP SSL : Port 465
- IMAP4 : Port 143
- IMAP4 SSL: Port 993
- LDAP : Port 389
- POP3 : Port 110
- POP3 SSL: 995
- CommTouch : 8088
- CommTouch IP Reputation : 8181
- WorkgroupShare : 8100 (Unsecure)
- WorkgroupShare : 8101 (Secured)
- WorkgroupShare Free/Busy : 8109
- Instant Messaging Server : 5177
- Instant Messaging Client : 5188 (Persistent connections not enabled)

Archiving

- MailArchiva SMTP : 8091
- MailArchiva : 8090
- MailArchiva - IMail Web Service : 8080

-OR-

- Sonian SMTP - 25

Setting up a Dial-up Internet Connection

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. 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 start the connection manually.

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

Receiving Mail from an Internet Service Provider

When you use a dial-up connection, your inbound mail from the Internet must be stored somewhere, usually with your ISP. Your ISP can store your mail in several ways. Three of the more popular ways are:

- **Method 1:** The ISP sets up individual mail accounts on the ISP computers. This method usually uses the POP3 mail protocol to read or retrieve mail. Each user dials up the ISP and either reads or downloads mail.
- **Method 2:** The ISP sets up individual mail accounts on the ISP computers, but the ISP forwards all mail for your users to your mail server when your dial-up connection is up. This method uses the ISP's Internet domain name. *Example.* (on page 59)
- **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 incoming mail and forwards it to your mail server when your dial-up connection is up. *Example.* (on page 60)

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 currently use Method 1, then you must 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.

Setting Up the Server for Dial-up Access

1. Setting up IMail Server using a dial-up connection is the same for both Methods 2 and 3, above. To do this, you need to create mail accounts for users on the IMail Server computer. For more information, see Administering IMail Users. If you use Method 2, user names must be the same on both the ISP's computer and your IMail Server computer.
2. Tell Windows about your e-mail domain name. When Windows looks up a domain name, it first searches the \winnt\system32\drivers\hosts file. If there is no match, it asks a Domain Name Server (DNS) for the IP address for the domain name.

This creates a problem, as your Windows computer has a different IP address than your ISP's computer. When IMail Server looks at the incoming mail, it looks up the domain name to which the email is addressed. If the domain name points to your ISP's computer (your ISP's IP address), then IMail Server sends 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 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 (Method 2, see *Example* (on page 59)), or your own (Method 3, see *Example* (on page 60)) on the **Add New Domain page**. See *Adding a New IMail Domain* (on page 47), *Setting Up a Virtual IMail Domain With an IP Address* (on page 123), or *Setting Up a Virtual IMail Domain Without an IP Address* (on page 123) for more information.

3 Unless you plan on maintaining a 24-hour, 7-day a week dial-up Internet connection, your ISP must spool all mail for your company. Then, have your ISP set up their computer to try to periodically send 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 computer?
- How often will your 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:

Queue Time	Minutes
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 Server Queue Time determines how often IMail Server tries to send mail to the ISP or Internet (this is set up on the *SMTP Options* (on page 392) page).

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 a Dial-up Connection* (on page 59).

Method 2 Example

If you are using Method 2, and the computers 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. Place each domain name in the hosts file, pointing to the IMail Server computer's IP address.

Related Topics

Setting Up a Dial-Up Internet Connection (on page 57)

Using ETRN to Retrieve Mail on a Dial-up Connection.

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 Tries before Return To Sender setting has elapsed. 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.

Related Topics

Setting Up a Dial-Up Internet Connection (on page 57)

Method 3 Example

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
```

Related Topics

Setting Up a Dial-Up Internet Connection (on page 57)

Changing the IP Address of a Host

Before changing the IP address of a domain, *back up your IMail registry* (on page 105).

To change the host IP address:

1. If you have not done so, bind the new IP address to the NIC (network interface card).
   - Navigate to Control Panel/Network Connections/LAN or High Speed Internet Connection.
   - Right-click on the Connection icon and select **Properties**. Scroll through the list under **This Connection Uses the following items** to (Internet Protocol) TCP /IP. Click the **Properties** button.

- The **General** tab appears. Enter the new IP address in the appropriate text box.

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, delete the old one. First, make sure that the "Official" value under the new IP address key shows the correct host name. If you only see a key for the old IP address you can rename that key to the new IP address.

4 Highlight the host name 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 *Stop and restart all services.* (on page 370)

Related Tasks

Back Up IMail Registry (on page 105)

Setting Up a Mail Gateway

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

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

- The other server must be running SMTP .
- 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 (\windows\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 number of **Tries Before Return to Sender** (set up on the SMTP Settings page) is exhausted.

- If you are using any of the Relay Mail for options on the SMTP Settings Page and want to relay outgoing mail for another mail server, the address of the other server must be added by clicking the Addresses button and adding the IP address on the Relay Mail for Addresses page. For further information, see *Setting IMail SMTP Options* (on page 392).

Example:

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: namedomain2.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 looks up a domain name, it first searches the \WINDOWS\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.



Note: You can use the ETRN command to manually retrieve mail from the ISP's mail server. See *Using ETRN to Retrieve Mail on a Dial-up Connection* (on page 59) for more information.

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 configure this, have the customer set his computer up to log into his ISP at intervals where he can catch the queue processing interval **(Times Before Return to Sender** setting on the SMTP Settings page) of your server. For example, if your retry 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 (\WINDOWS\system32\drivers\etc\hosts) which associates his IP address with his domain name. For example:

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

This way, IMail Server attempts to deliver mail it receives for that domain to his computer, bypassing the MX records in DNS, which points 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 to the *Access Control* (on page 400) page.

For example, if the remote host's DNS is set up to receive mail for a primary domain, such as 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 must specify its host name and IP address in the hosts file on your IMail Server host.

CHAPTER 4

User Mail Accounts

In This Chapter

Creating User Database 65
Working with Individual User Accounts 70

Creating User Database

In This Section

Creating NT/AD User Database (on page 65)

Using IMail Database (on page 68)

Creating External Database (on page 68)

Importing Windows NT Users (on page 66)

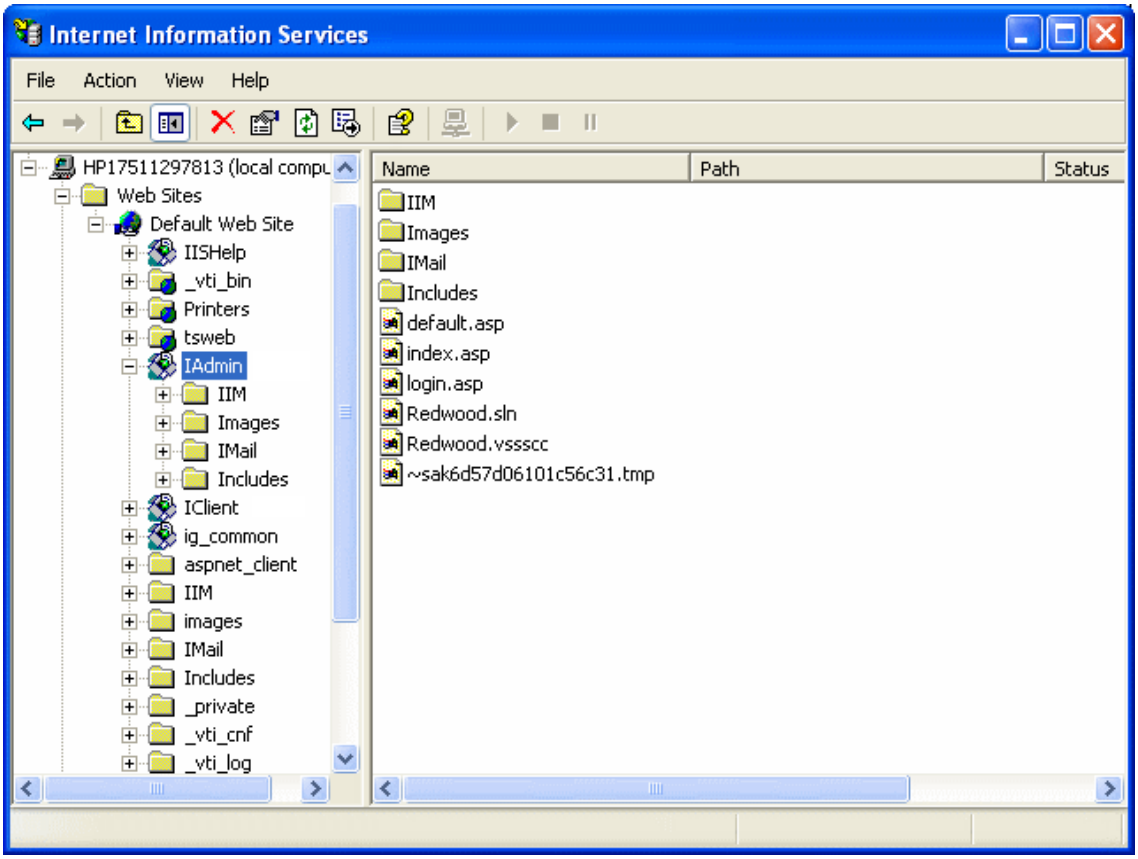
Using the Windows NT/Active Directory Database

If your IMail user database is a **Windows NT Database**, IMail Server creates a user mail account for each user listed in the Windows NT Database. The user mail accounts are created, as necessary, when the mail server receives a message addressed to the user or when a user accesses the IMail Server from a mail client . You cannot add or delete users using IMail Server Administrator; instead, you need to use the Windows NT User Manager. If you are using Active Directory, you need to set IIS to use a domain user.

To configure IMail Administrator virtual directory for anonymous access in IIS:

1. Click **Start** > **Programs** > **Administrative Tools** > **Internet Information Services**. The Internet Information Services Manager appears.
2. Click **+** next to **Web Sites**. The Web Sites folders expand.

3 Click **+** next to **Default Web Site**. The Web Sites folder expands.



4 Right-click **IAdmin,** select **Properties.** The **IAdmin Properties** dialog box appears.

5 Click the **Directory Security** tab, then click **Edit** in the **Anonymous access and authentication control** section. The **Authentication Methods** dialog box appears.

6 Click to clear the **Anonymous access** option.

7 Make sure that the **Integrated Windows authentication** option is selected.

8 Click **OK** to exit the dialog boxes.

9 Make sure that the IMail administrator has domain administrative privileges for the domain that the remote server is on.

Related Topics

Importing Windows NT Users (on page 66)

Importing Windows NT Users

How to get here

If a host uses the IMail Database for user mail accounts, you can import users from the NT Database and add them to the IMail database on the Import NT Users page.

Note: This differs from actually using the Windows NT Database, in that although the users keep their same user IDs, Administrators are required to set a default required password for importing these NT Users into the IMail database. Users can change the password after they have been imported.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Import NT User Options

- **Initial Password.** Use this text box to enter an initial password setting for users being imported.

Note: The password must be between 3 and 15 characters.

- **Confirm password.** Use this text box to confirm the password setting for users being imported.
- **Add as Collaboration User.** Select this check box to enable a User or Users selected from the Username list to access the Collaboration tools.
- **Add as Ipswitch Instant Messaging User.** Select this check box to enable a User or Users selected from the Username list to access Ipswitch Instant Messaging.

Existing Users on the NT Database

Search Box. Requires entering a minimum of two characters, and the search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

- **Username.** This column lists the usernames of all users imported from the NT database. You can click on the link under the username to access the user's User Properties.
- **Full Name.** This column lists the display names of the users.

Import. To add a user and password, select a user from the list by selecting the check box next to the Username, enter the initial password and the confirm password, and click **Import**.

Cancel. Click the **Cancel** button to return to the Utility page.

Related Topics

Using the Windows NT Database (on page 65)

Using the IMail Database

How to get here

If you select **IMail Database**, user IDs and passwords for mail accounts are stored in a database in the registry on the IMail Server system, separate from either the Windows NT database or any external database.

You can also import Windows NT users into an IMail database, without having them linked to the Windows NT database.

Creating External User Database for a Mail Domain

IMail Server can use an external database to register and authenticate users on a particular mail domain . Users that you add to and delete from an IMail Server host are also added to and deleted from the external database.

Important: Remember to restart the IMail Services, after creating external database.

Before you use an external database for a mail domain, 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 and database documentation for information on the System DSN .

Important: When you configure a DSN to an SQL data source in the Microsoft Windows ODBC Data Source Administrator, it may default to **Named Pipes** network library. Make sure that you set the connection type to **TCP/IP in order for the external database to work correctly.**

After you have verified the System DSN that points to the database you want to use, you can configure an external database.

Note: The external database can reside locally with the IMail Server.

Configuring an External User Database

The connection between IMail Server and an external user database is accomplished via a dynamic link library (DLL file). IMail Server includes a sample .dll file (ODBCUSER.DLL). This DLL uses the ODBC method, but can be modified to support other external database methods. The complete source code for this DLL is provided upon request from Ipswitch.

When you configure an external user database, IMail Server creates an ODBC database that holds tables configured with the correct fields. The fields are identified in the **Table Name** text box. After the database is created and the ODBC system data source name is established in the ODBC Source Administration tool (located in the Windows Control Panel), you can use the database to store user authentication

information and user properties. This information can be managed through IMail Administrator, including adding and deleting users.

Important: When using an external database, any IMail service you run (except the Log Server) must be set up from the Windows Control Panel Services application so the account that IMail Server runs under has access to the external database.

To create a mail domain that uses an external database:

1. In IMail Administrator, click **Domain** > **Domain Properties**.
2. In the **User Database** section, select **External Database** from the **User Database type** list box.
3. Click the **Configure** button. A domain options page appears.
   - **External Database Implementation DLL.** Enter the full path to the odbcuser.dll installed on your local server or the path of a .DLL that supports the functions: GetUserEntry, SetUserEntry, DeleteUserEntry, AuthorizeUser, GetFirstUserEntry, and GetNextUserEntry. (These are defined in the odbcuser.h file.)
   - **ODBC System Data Source Name (DSN).** Enter the source name for the database where the user information is stored. IMAILSECDB is the default name that the ODBC link uses.

Important: For users using SQL 7.0 or above, enter the following information after the ODBC System Data Source Name box: `DSN_NAME;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.

   - **Table Name**. Enter the table name within your ODBC database. Leaving **"[default]"** in this text box will use your domain name as the table name. All periods will be replaced with underscores.

Important: The table name cannot begin with a number.

Example:
If you use the Data Source Name IMAILSECDB and the username AUGUSTA and password GEORGIA, the correct format of the ODBC System Data Source Name box is: `IMAILSECDB;UID=AUGUSTA;PWD=GEORGIA`

   - **Table name**. Enter the database table name. If the field is blank or contains [default], the host name is used with dots replaced by underscores. The Table name cannot begin with a number.
   - **Enable Multiple Connections** to allow multiple connections from the external database to IMail Server.
   - **Maximum Number of Connections** to set the maximum number of connections from the external database to IMail Server

Save. Click this button to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

Related Topic

Domain Properties (on page 41)

Working with Individual User Accounts

In This Section

Vacation Message for Users (on page 70)

Customizing the Notification Message (on page 71)

Full Mailbox Notification Example (on page 71)

Vacation Message

How to get here

Note: Vacation Message can handle all foreign characters for display in the Web Admin.

You can create a vacation message for each e-mail user account. When the vacation message is enabled, IMail Server sends an automated vacation message to each email address the user receives mail from. The vacation message is stored in the vacation.ima file in the user's IMail Server home directory.

Note: **Vacation Message** can also be enabled and disabled within the user's Web Client.

Note: Disabling the vacation message will automatically clear the "vacation.snt"

Domain Name (OHN). The current domain name used to address mail to the users on the mail domain is displayed.

User ID. Displays the selected user ID (user name) for the e-mail account.

Enable Vacation. Check box to enable or disable the Vacation Message text box. Disabling the vacation message will clear the "vacation snt" file.

Vacation Message. Text box when enabled, allows a vacation message to respond to all new mail messages received. The vacation response will only be sent once to each unique e-mail address.

Save. Click this button to save your settings.

To create a vacation message:

1. Select **Enable Vacation**.
2. In the **Vacation Message** text box, enter the reply message you want to send while the user is away. The vacation message is sent one time to each e-mail address from whom the recipient receives mail. IMail Server saves the message sender's e-mail address in a file (vacation.snt). This file provides the user with a list of users that sent e-mail while away and also keeps track of the senders so the vacation message is only sent one time to each sender.
3. Click **Save**.

Customizing the Full Mailbox Notification Message

The notification e-mail message that is sent to a user is configurable. You can customize the text for this message in the `"Notify.txt"` file that is located in the `"...\IMail"` top directory.

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 above two tags will be replaced with the User ID and the domain .

Related Topics

Full Mailbox Notification Example (on page 71)

Full Mailbox Notify Example

Example:

If `"80"` is entered in the **Full Mailbox Notify** text box on the Domain properties page, a user will receive an e-mail when his/her mailbox is 80% full.

The user will receive a maximum of one message a day, for three days, as long as the mailbox is over 80%. The messages will stop when the mailbox size drops below 80% or it has sent 3 warning messages.



Note: The user will not receive this message if there is no mail activity.

Related Topics

Customizing the Full Mailbox Notification Message (on page 71)

CHAPTER 5

System Administration

System Settings handles the following menu options:

- *System Settings* (on page 73)
- *System Trailer* (on page 76)
- *System WebMail Message* (on page 78)
- *Exchange ActiveSync®* (on page 78)
- *DomainKeys / DKIM* (on page 82)
- *Server level DNS black lists* (on page 89)
- *Spool Directory* (on page 94)
- *System Default User Settings* (on page 98)
- *System Default Web Client Preferences* (on page 101)

Information on how to backup Registry data:

Registry Backup (on page 105)

In This Chapter

System Settings 73
System Trailer 76
System WebMail Message 78
Microsoft Exchange ActiveSync 78
DomainKeys / DKIM 82
DNS Black Lists (Server Level) 89
Spool Manager 94
System Default User Settings 98
System Default Web Mail Preferences 101
Registry Backup 105

System Settings

How to get here

The System Settings page allows you to configure the settings for the IMail domain.

- **Product Name (Display Only).** Ipswitch IMail Server Product Name.

- **Serial Number (Display Only).** Assigned at registration. Although not needed for installation of product, it is needed to receive Customer and Technical Support. It confirms current sales agreement and is also used to assist with upgrades/crossgrades.
- **Version Number (Display Only).** Version Number of IMail Server Product.
- **Licensed User Count (Display Only).** Licensed User Count of IMail Server Product.
- **Number of Active Users (Display Only)**. This count displays active users that are able to access their accounts. This does not count disabled users.
- **Domain Name (OHN).** Enter the Official Host Name (OHN) that will be used to address mail to the users on the domain.
- **Gate Host.** Enter the name of another host (IMail Serve) to send mail to when it cannot be delivered directly to the destination host. This can also be used in conjunction with the **Send All Remote Mail Through Gateway** option (on the **Services** tab, **SMTP Settings** page) to force mail delivery through the gateway host. Since IMail Server should be able to reach all hosts directly, this field should typically be left blank.
- **Default Host.** Enter the name of the host (IMail Server) that will accept messages when no mail domain is specified in the e-mail address.



Important: Restart Web Service after changing the value of the Default Host.

- **Top Directory.** The directory where IMail application files are installed. This is specified during installation. Use this text box to change the directory where the directories for users, lists, and web files for this host will be stored.
  - **Browse.** Use this button to browse to the directory where users, lists, and web files for this host will be stored. It is best to setup a folder within IMail Server directory. This can be done manually, or the following options to assist in creating the folder after clicking browse:

    Creating a New Folder:

    - The **Create New Folder** page appears.
    - Take note of the path at the top of the folder tree.
    - Click the  to move up the folder tree
    - Double click the displayed folder to move down the folder tree
    - Enter the new folder name in the text box, click **Create.**
    - Your new folder will automatically select, and appear as part of the path in the upper text box.
    - Click **OK.** The path to the new directory appears in the Log Directory text box.
- **Spool Directory.** This is the temporary directory where messages are spooled while awaiting processing and where log files are kept. Use this text box to change the directory that stores log and temp files, as well as mail messages, attachments, etc. that are waiting for delivery.

- **Browse.** Use this button to browse to the directory that stores log and temp files, as well as mail messages, attachments, etc. that are waiting for delivery. See above instructions to create a new folder.

- **Log Server.** Enter the IP address of the server to which IMail sends the log files.
- **Log Directory.** If you wish to separate log messages from spooled messages, use this text box to set up a separate directory.
  - **Browse.** Click this button to set up a separate directory to store log files. See above instructions to create a new folder.
- **Install Date.** Displays the date and time the IMail Server application was installed.

Archiving (If Installed)

Caution: Do not enable this feature unless archiving has been installed, as the Spool Manager will no longer function correctly.

Note: A utility exists to archive all current e-mail messages. This utility called **"archive.exe"** is located under \IMail directory, to archive existing messages that have never archived.

- *View Getting Started Guide* (http://docs.ipswitch.com/_Messaging/Archiving/GettingStarted/Archiving.pdf). PDF link to Archiving Getting Started Guide.
- **None.** (Default Setting)
- **SMTP-based.** This radio button should be checked to enable a third party archiving engine to use the SMTP-based transport mechanism.
  - **Server**. Location of third party archiving SMTP gateway server. Enter the valid IP address of the SMTP gateway server, or localhost.
  - **Port**. Port setting for your third party archiving server to listen on and communicate with your IMail Server.
  - **Recipient**. E-mail address of your third party archiving recipient.
  - **Archive Orphaned Messages**. Orphaned files, by default, will not be archived.
- **Mailbox-based.** This radio button should be checked to enable a third party archiving process to deliver e-mail to a specified recipient.
  - **Recipient**. Location of mailbox that will accept all archiving from your third party process. This recipient can be any valid user on the primary domain.
  - **Archive Orphaned Messages**. Orphaned files, by default, will not be archived.

Save. To save any changes made.

Related Topic

Configure DNS Black Lists (on page 89)

Spool Manager (on page 94)

System Trailer

How to get here

The System Trailer page allows the System Administrator to maintain a trailer message that will be appended to every outgoing message (This does not include locally sent messages within the server). This text file is named `"trailer.txt"` and can be located in the `"\IMail"` directory.

Note: "trailer.txt" is set to work for the entire IMail Server. Currently "**trailer.txt"** does not work on a per domain level.

- **Plain Text.** Set by default. Plain text will force your trailer to be sent using plain text.
- **HTML**. Setting this will allow the online HTML WYSIWYG editor to load.

Note: Switching from the HTML editor to the plain text editor will display all tags and text that were in place with the HTML editor. It will be up to the System Administrator to strip out what needs to remain.

- **Text**. Displays the trailer message that will be appended to every outgoing message that is not locally sent within the server.

Note: The online HTML WYSIWYG editor is the same editor used in the web client when creating new messages.

Save. Click to save your settings.

Related Topics

HTML Online Editor Help (on page 76)

HTML Online Editor

The System Trailer page allows the System Administrator to maintain a trailer message that will be appended to every outgoing message (This does not include locally sent messages within the server). This text file is named `"trailer.txt"` and can be located in the `"\IMail"` directory.

Text Styles and Formatting Toolbars

By selecting formatting styles, font types, sizes and colors from the list boxes, you can customize your messages. Individual help (known as Tool Tips) is available for each button by mousing over the button.

Mouse over the adjacent buttons to access information on the functions of the different tools.

The formatting list boxes let you choose:

- paragraph alignment
- font types
- font size
- zoom = To allow for easier viewing (25% - 400%) from original size

Much like a word processor there are familiar buttons along with some new icons as follows:

= New Document - Clears text box	= Print
= Print Preview	= Find & Replace
= Fit To Window - Enlarges text box. Click again return to original size.	= Cleanup HTML
= Undo Button	= Redo Button
= Insert Paragraph	= Insert Today's Date
= Insert Current Time	= Insert Anchor
= Special Characters	= Universal Keyboard
= Bold	= Italics
= Underline	
= Left Justify	= Right Justify
= Center Text	= Full Justify text
= Reset all text to Left Justify	
= Insert numbered list	= Insert bulleted list
= Direction Left to Right	= Direction Right to Left
= Insert Hyperlink	= Remove Hyperlink
= Strikethrough text	

System WebMail Message

How to get here

The System WebMail Message page allows the System Administrator to maintain a message that will display above the Web Client login page. Once enabled, this message is a system wide message and will display all users using the Web Client.

This text file is named `"webmailmsg.txt"` and can be located in the `"\IMail"` directory.



Note: "webmailmsg.txt" is set to work for the entire IMail Server, and does not work on a per domain level.

- **Enabled**. Check this box to activate the display for messages above web client login page.



Tip: This does not disable the Administrator from updating the text area. This allows the Administrator to update the message before displaying to the users.

- **Normal.** Set by default. By design the "webmailmsg.txt" is an html file. Copying and pasting a web page will automatically copy all the source to this page. Click on HTML to view the source.
- **HTML**. This will display the text as HTML source.



Note: Switching from the Normal text to HTML will display all tags and text that were in place with the Normal editor.

- **Preview**. Displays how the message that will appear on the web client page.

Save. Click to save your settings.

Microsoft Exchange ActiveSync

How to get here

The **Microsoft Exchange ActiveSync®** page allows the System Administrator to view of all users that are enabled for mobile synchronization with Microsoft Exchange ActiveSync®.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

Select to allow your users capability to use Microsoft Exchange ActiveSync® to synchronize mobile devices with their web client information for e-mail, contacts and calendars. Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

See **Synchronizing with Microsoft Exchange ActiveSync®** (on page 80) for more information on mobile device setup to use Microsoft Exchange ActiveSync®.

Microsoft Exchange ActiveSync® License Information

Displayed on this page is your Microsoft Exchange ActiveSync® user license limit, with the number of enabled users by domain. Selecting a domain will display all the enabled users first, followed by the disabled users, with the capability to enable / disable multiple users at a time.

Should your license for Microsoft Exchange ActiveSync® users go over the limit that you have purchased, a message will display at the top of the screen: `"You have reached your Microsoft Exchange ActiveSync® licensed user limit"`

Warning: Should your Microsoft Exchange ActiveSync® license be over the limit, new users will have Microsoft Exchange ActiveSync® disabled; and existing users can not be enabled until the limit is less than the Microsoft Exchange ActiveSync® licensed user limit.

Status. (Enabled by default) System wide setting for **Microsoft Exchange ActiveSync®**. This allows all enabled domains with enabled ActiveSync® users to synchronize their mobile devices with their web client information for e-mail, contacts and calendars.

- **Enable / Disable** button is a **system-wide setting** that will activate or de-activate Microsoft Exchange ActiveSync® for all users.

Warning: Disabling **Microsoft Exchange ActiveSync®** at the System level will disable all ActiveSync® users on all domains, overriding both Domain and User Properties.

Total Number of ActiveSync® Licenses. Total number of users authorized for ActiveSync® usage.

Total Number of ActiveSync® Licenses in Use. Total number of users with ActiveSync® enabled.

Days Remaining in ActiveSync® Licenses. Number of days remaining before license expires for Microsoft Exchange Activesync®.

Search Box. Typing will automatically begin narrowing the list. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

Note: Column Titles when clicked will sort the list for the current session only. Refreshing the page will reset the original sort.

Microsoft Exchange ActiveSync® Usage by Domain

- **Domain.** Domain name on the IMail Server.
- **ActiveSync Enabled**. (Yes / No) This is the Microsoft Exchange ActiveSync® in the domain properties setting.
- **ActiveSync User Count**. Total active users for the selected domain with Microsoft Exchange ActiveSync® enabled. This count is totaling all users in the domain with Microsoft Exchange ActiveSync® enabled at the user level.

Note: Domains that have Microsoft Exchange ActiveSync® disabled will always display a **zero** for **ActiveSync® User Count**, ignoring the actual user settings.

Enable. Select a domain and click **Enable** to allow Microsoft Exchange ActiveSync® access for the domain.

Disable. Select a domain and click **Disable** to turn off Microsoft Exchange ActiveSync® access for the domain.

Related Topics

Synchronizing with Microsoft Exchange ActiveSync® (on page 80)

Microsoft Exchange ActiveSync® Users (on page 136)

Synchronizing With Microsoft Exchange ActiveSync

Mobile Device Synchronization with Microsoft Exchange ActiveSync®

Note: See the *Mobile Client White Paper* (http://docs.ipswitch.com/_Messaging/IMailServer/v11/Mobile/MobileSync.pdf) for more detail information on mobile device setup.

IMail Server now supports Microsoft Exchange ActiveSync® for the synchronization of data between a user's mobile device and your IMail Server. Once configuration of your

mobile device is complete, synchronization will allow access to your e-mail messages, calendar appointments and contact information.

IMail Server currently supports the following mobile devices:

- Windows Mobile® 5
- Windows Mobile® 6
- Windows Mobile® 6.1
- IPhone™

Mobile Client Requirements

Two requirements are essential for mobile device synchronization:

1. Windows Mobile® 5.0 and later are the only devices that IMail currently supports for synchronizing data to your mobile device.
2. Data Access for synchronization by either:
   - A data plan provided by your cellular provider or
   - A wireless connection with internet data access

Mobile Device Synchronization

To correctly allow users to set up their mobile devices to synchronize with your IMail Server, Microsoft Exchange ActiveSync® must be configured to run on their mobile device. Microsoft Exchange ActiveSync® compares the information on your device with the information on your IMail Server and updates all locations with the most recent information. Microsoft Exchange ActiveSync® will synchronize with your IMail Server information from your E-mail, Contacts and Calendar through your Web Client.

Outlook Synchronization

For Outlook synchronization, the WorkgroupShare Client must be installed. The WorkgroupShare Client is located under your `...IMail\WorkgroupShare\ClientSetup\` folder and the application name is `"ClientInternationalSetup.exe"`.

Once installed Outlook will synchronize E-mail, Contacts, Calendar and Tasks with the IMail Server. For more detail information see both the *WorkgroupShare Server Guide* (http://docs.ipswitch.com/_Messaging/WorkgroupShare/WGS2.3/WGSServer.pdf) and the *WorkgroupShare Client Guide* （http://docs.ipswitch.com/_Messaging/WorkgroupShare/WGSClient.pdf）.

Web Client Synchronization

Your web client has direct access to E-mail, Contacts and Calendar data, and does not require synchronization. Once the WorkgroupShare Client and Microsoft Exchange ActiveSync® are correctly configured, information updated using the Web Client will synchronize with both your user's mobile devices and Outlook.

Sync Log. This log defaults to the spool directory will only exist when errors are generated. Errors that occur with mobile synchronization will log to `"syncmmddyyyy.log"`.

Related Topics

Mobile Client White Paper
(http://docs.ipswitch.com/_Messaging/IMailServer/v11/Mobile/MobileSync.pdf)

WorkgroupShare Server Guide
(http://docs.ipswitch.com/_Messaging/WorkgroupShare/WGS2.3/WGSServer.pdf)

WorkgroupShare Client Guide
(http://docs.ipswitch.com/_Messaging/WorkgroupShare/WGSClient.pdf)

Microsoft Exchange ActiveSync® License Summary (on page 78)

DomainKeys / DKIM

DomainKeys and **DomainKeys Identified Mail (DKIM)** are e-mail authentication methodologies designed to verify digitally signed e-mail on a per-domain basis. Both methods were designed for protection of e-mail identity and have assisted in the control of "spam" and "phishing". DomainKeys and DKIM use asymmetric key cryptography to sign messages with a private key and use DNS to distribute the public key for signature verification.

DomainKeys (*RFC4870* (http://tools.ietf.org/html/rfc4870)) is a precursor to DKIM (*RFC4871* (http://tools.ietf.org/html/rfc4871)), though both are currently in use, DomainKeys is considered deprecated by DKIM.

See the following PDF for help in *Getting Started with DomainKeys / DKIM* (http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/PDF/DomainKeysGSG.pdf).

DomainKeys

DomainKeys is a domain-level e-mail authentication standard that uses public/private key encryption and DNS to prove the legitimacy and contents of an e-mail message, and also verifies that the domain used in the "from" or "sender" header of a message has not been modified while in transit.

Public Key / Private Key

A public key/private key-pair is created for the sending domain. The private key is stored securely on the mail server and is used to sign all outgoing messages. The public key is stored and published in DNS as a TXT record of the domain.

When an e-mail is sent, the mail server will use the private key to digitally sign it, which is part of the message header. When the e-mail message is received, the DomainKeys signature can be verified against the public key on the domain's DNS.

For detail specifications on **DomainKeys** see *RFC4870* (http://tools.ietf.org/html/rfc4870).

DKIM

DKIM is very similar in functionality to DomainKeys, with an enhanced standard that provides more flexibility and security. Although DKIM does not filter or identify spam, widespread use of DKIM can prevent spammers from forging the source address of their messages. If spammers are forced to show a correct source domain, then the other spam filtering techniques will work more effectively.

Some of the improvements provided by DKIM are as follows:

- Multiple hashing algorithms (as opposed to just one available with DomainKeys).
- Capability for one DNS text record to handle multiple domains.
- Improved option for canonicalization that validates header and body separately.
- Capability to delegate signing to third parties.
- Capability to self-sign additional headers.
- More advanced options for customization using DKIM. (e.g. Hash Algorithms, Body Settings, Expiration)

For detail specifications on **DKIM** see *RFC4871* (http://tools.ietf.org/html/rfc4871).

Related Topics

System Signing List (Selectors) (on page 83)

Domain Signing List (Selectors) (on page 164)

System Selector List (Signatures)

How to get here

Selectors allow a domain to have one DomainKeys selector and one DKIM selector enabled at one time. Multiple selectors are allowed in a domain to give the IMail Administrator capability to easily change from one public-key in DNS to another.

Important: Only **one DomainKey selector** and **one DKIM selector** can be enabled at **one time for a domain**. **Example:** A DKIM selector "selector1" is enabled for domain1.com. The IMail Administrator decides to enable "selector2" for domain1.com. "selector1" will automatically be disabled for domain1.com.

Important: After updating or creating a selector be sure to restart your **SMTP and Queue Manager services**.

System Signatures (Selectors)

Status. (Disabled by default) A system-wide status setting for **DomainKeys / DKIM**.

- **Enable / Disable** button is a **system-wide setting** that will activate / de-activate DomainKeys / DKIM for all domains.

Search Box. Typing will automatically begin narrowing the list. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

Note: Column Titles when clicked will sort the list for the current session only. Refreshing the page will reset the original sort.

Selector List

- **Name**. Name used to identify selector.
- **DNS Text Record**. Name used to identify the selector in DNS. This text name allows any text string that is a legal DNS domain name.

Example: DNS Text Record set to MyDNSName will be named `"MyDNSName_domainkey.domainname.com"`

- **Domains**. Domain names that are assigned to selector.
- **Type**. E-mail authentication type to verify the DNS domain of an E-mail sender and the message integrity.
  - **DomainKeys**. DomainKeys uses the Message Algorithm as the specified canonicalization method.
  - **DKIM**. (DomainKeys Identified Mail) is an enhanced protocol of DomainKeys, using public-key cryptography and key server technology to verify the source and contents of e-mail. DKIM uses the Header and Body Algorithm as the specified canonicalization method.

Add (on page 85). Click to add a new selector. This will give the following two options

- **Wizard** (on page 179). Run this option for Administrators that are new to DomainKeys.
- **Advanced** (on page 85). Click this option for Administrators that are familiar with all DomainKeys options.

Delete. Click this after selecting item(s) from the list to delete.

Related Topics

System Selector Add / Edit (on page 85)

System Selector Add / Edit

How to get here

Important: After updating or creating a selector be sure to **restart** your **SMTP and Queue Manager services**.

Selector Signing Properties

- **Type**.
  - **DomainKeys**. Uses Message Algorithm for Preparation Signing.
  - **DKIM**. Uses Header and Body Algorithm for Preparation Signing.
- **Name**. Value used to identify the selector in the IMail Administrator.
- **DNS Text Record**. Name that will associate the selector in DNS. This text name allows any text string that is a legal DNS domain name.

Example: DNS Text Record set to MyDNSName will be named `"MyDNSName_domainkey.domainname.com"`

- **Status**. (On by default) Click "Off" to disable the selector.
- **Description**. Free format text box limited to 1024 characters.
- **Header Algorithm (DKIM only)**. DKIM uses both the Header and Body Algorithm as the specified canonicalization method.
  - **Simple**. This algorithm is designed to be the least tolerant. Each header is unfolded per RFC2822 and is converted to lowercase.
  - **Relaxed**. (Set by default) This algorithm tolerates common modifications such as white-space replacement and header line re-wrapping.
- **Body Algorithm (DKIM only)**.
  - **Simple**. This algorithm is designed to be the least tolerant.
  - **Relaxed**. (Set by default) This algorithm tolerates common modifications such as white-space replacement and header line re-wrapping.
- **Message Algorithm (DomainKeys only).** DomainKeys uses the Message Algorithm as the specified canonicalization method.
  - **Simple**. Allows toleration of almost no modification.
  - **No Folding Whitespace (nofws)**. (Set by Default) Allows common modifications such as white-space replacement and header line re-wrapping.
- **Public Key**. The public key which is automatically generated is what must be stored and published in DNS as a TXT record of the associated domain.



Tip: Remember to check for the "p=" in front of the key

Advanced Properties

DomainKeys and DKIM Option

Private Key. Text box displaying text string of Private Key. The private key is stored securely on the mail server and is used to sign all outgoing messages.

- **Generate New Key**. (Default is 1024 Kb) Clicking this button will generate a new **Private Key**, with a pop-up option for the private key length (512, 768, 1024, 1536, 2048).

DKIM Advanced Options Only

Hash Algorithm. SHA (Secure Hash Algorithm) hash functions are a set of cryptographic hash functions designed by the NSA and published by the NIST as a US Federal Information Processing Standard.

- **SHA-256**. (Set by default) Is an improved hash function in the SHA-2 family, computed with 32-bit words.
- **SHA-1**. The best established of the existing SHA hash functions, and is employed in several widely used security applications and protocols.

Body Settings. Options for body length limits when signing.

- **Sign Entire Body**. (Set by default)
- **Sign Entire Body and Include Length Tag**. Including the length tag allows message trailers to be better tolerated after the message is sent.
- **Specify Max Body Length for Signing**. Textbox for max amount of bytes to sign.

Expiration. When both the Timestamp and Expiration Tag are set, then a validation check will be done to verify that the Expiration Tag is greater than the Timestamp when the signature is verified.

- **Include Timestamp**. (Set by Default) This tag tells the verifying server when the signature was generated.
- **Include Expiration Tag**. (Optional) When used, this tag tells the verifying server to ignore this signature after the time specified.
  - **Time in Which to Expire**. Time is counted by minutes, hours or days. The expiration time will be calculated based on the time when the signature is generated.

Authoritative Domain.

- **Use the Domain's Auth Name**. (Set by default) This option requires a DNS text record for each domain signature selector.
- **Use the Sending User's Domain Name**. This option requires a DNS text record for each domain signature selector.

- **Use the Following Auth Name**. (Set by default for DKIM Wizard) This option allows the administrator to create one DNS text record to handle many domains.

Assigning Domains

Domains can easily be assigned to a selector, allowing the domain to use as a signature.

Available Domains not Assigned

The left box displays all available domains that do not have the selector assigned.

- **Domain Name**. Domain name that currently does not have the current selector assigned.

   **(Add Domain to Selector)**. Select an available domain and click to add to the current selector.

   **(Remove Domain from Selector)**. Select a domain from the domains currently assigned and click to remove the current selector.

   **(Add All Domains to Selector)**. Click to add all available domains to the current selector.

   **(Remove All Domains From Selector)**. Click to remove all domains from the current selector.

Assigned Domains for Current Selector

- **Domain Name**. Domain name that has the current selected assigned.
- **Enabled.** Check this box to activate and allow the domain to use the selector.

Enable All. Click this button to activate all the assigned selectors.

Disable All. Click this button to deactivate all the assigned selectors. The selector will be assigned to all the domains, but the selector will be disabled for use as a domain signature.

Test DNS Setup. Click this button to test the current selector against your current DNS setup. The DNS Test button will display **"successful"** for each domain. A link to assist with DNS problems will display for domains that **"failed".**

- See the following KB for DNS help **-** *http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=727* (http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=727)

Headers List

- **Sign All Headers**. (**Not** set by default) See all Headers.

 **Sign All Headers** when setting Prevent Adding for a signature will be unchecked, unless the header list is specified otherwise.

Warning: Disabling the default set of headers to be signed opens the possibility of header modifications and spoofing depending on the headers that are being signed.

DomainKeys / DKIM Headers

By default (RFC minimum recommendation) the following headers are set for signing:

- CC
- Content-Description
- Content-ID
- Content-Transfer-Encoding
- Content-Type, Date
- From, In-Reply-To
- List-Archive
- List-Help
- List-ID
- List-Owner
- List-Post
- List-Subscribe
- List-Unsubscribe
- Message-ID
- MIME-Version
- References
- Reply-To
- Resent-CC
- Resent-Date
- Resent-From
- Resent-Message-ID
- Resent-Sender
- Resent-To
- Sender, Subject
- To

TIP: The default headers are recommended as the **minimum** headers necessary for maintaining secure header signing.

DomainKeys Header List

- **Name**. Header name selected to be signed.

DKIM Header List

- **Name**. Header name selected to be signed.
- **Maximum Number To Sign**. (Default set to 1) Maximum number of same headers allowed to be signed.
- **Sign All**. (True by Default) Signatures will sign all headers with the same headers for the domain.



Tip: **Max Number to Sign** and **Sign All** are not available for update when the **"Sign All"** check box is set.

- **Prevent Adding**. (False by Default) A signature will not tolerate headers with the same header name to be added.

Add Header. Click the **Add** button to create a custom header or select a header from the drop down for a list of all headers.

Edit Header. (DKIM functionality only) Select a header and click the Edit button to update the header options.

Delete Header. Select a header and click the Delete button to remove.



Note: To maintain a secure header signing, it is not recommended to remove a default header.

Related Topics

About DomainKeys / DKIM (on page 82)

System Selector List (Signatures) (on page 83)

DNS Black Lists (Server Level)

How to get here

Server level DNS black lists are spam databases that store information about IP addresses that are known to send spam. IP addresses that have open mail relays (relays mail for anyone) are also commonly listed in black lists, because those servers have the potential to be easily hijacked by spammers. Each black list compares the IP addresses from which an e-mail is sent against the spam database to look for a match. If a domain's IP address is listed in one of the black lists, mail from that domain should be suspected of being spam.

All black lists must be configured and enabled at the server level before an IMail e-mail domain can use them. This lets a system administrator decide which black lists to allow an e-mail domain to use. Only black lists that are enabled on the DNS Black Lists page are available for use in domain (host) level configurations.

Use DNS Black Lists Options to add, edit and delete server black lists. All black lists that are currently configured for the server are displayed in the DNS black list. The DNS black list information is stored in the `"spamblkm.txt"` file located in the `"...\IMail"` top directory.



Note: DNS black lists must be enabled at the server level before they are made available for use at the email domain level. DNS black lists are then used at the domain level (when bound to an IP address), where administrators can choose which black lists to enable for the host on the *Connection Checks* (on page 274) page.

- **Add.** Click this button to *Add to DNS Black List* (on page 92) page.
- **Edit.** Select the DNS to edit and click this button to *Edit the DNS Black List* (on page 92) to the DNS Black List.
- **Delete.** Select an item on the DNS Black List to delete and click the **Delete** button.



Important: Updates made to the DNS Black List will not successfully update until the "Save" button has been clicked, and the message "Your changes have been saved" is displayed at the top.

Save. Click to save your settings. An "Update Successful" message and the time of the update appear.

Related Topics

Server Level Antispam Options (Black Lists) (on page 270)

Understanding DNS Black Lists (on page 90)

How Black Lists Work (on page 91)

Adding a DNS Black List (on page 92)

Setting Connection Checks Options (on page 274)

Understanding DNS Black Lists

What is a DNS Black List?

DNS black lists are databases of known spammers. These databases contain IP addresses that are known to send spam. They also contain IP addresses that have open mail relays, because a spammer can easily use these systems to send out spam.

How IMail Server Uses DNS Black Lists

IMail Server uses DNS black lists during connection filtering. In order to fully understand how antispam and connection filtering work, it is necessary to understand DNS black lists. Connection filtering compares each message against the configured DNS black lists to see if the IP address of the connecting server is listed. If the result is positive, the message is either deleted or an X-Header is inserted into the message.

"Standard" and "Trusted" DNS Black Lists

You can separate DNS black lists into two categories: standard DNS Black Lists and trusted DNS Black Lists.

A trusted DNS black list is one that you know is updated frequently, and is more likely to be accurate. You may also identify a black list as trusted because you find that for your uses it produces the least number of false positives.

Warning: If a message makes a match on the **Trusted Black List**, it is automatically **deleted**.

A standard DNS black list is a black list of which you are uncertain about its accuracy. If a message matches one of these lists, an X-Header is inserted into the message, indicating which black list it matched.

Configurable for Each Host

DNS black lists are configurable for the entire server, which enables a system administrator to decide which DNS black lists are available to each domain. Each domain administrator is then responsible for enabling the configured black list for the domain. A domain cannot use a black list that is not configured and enabled for the server.

Related Topics

Server Level Antispam Options (Black Lists) (on page 270)

How Black Lists Work (on page 91)

Server Level DNS Black Lists (on page 89)

Trusted Black Lists (on page 277)

Add/Edit the DNS Black List (on page 92)

How Black Lists Work

DNS black list databases contain a list of IP addresses that are known to send spam. They also contain IP addresses that have open mail relays, because a spammer can easily hijack these systems to send out spam. Each black list has different reasons for why an IP address is blacklisted. Among the more common reasons are: dialups, bulk mailers, spammers and open relays.

Categorizing IP Addresses in Separate Domains

Just as black lists have different criteria for including IP addresses, they also have different ways of categorizing the IP addresses. Some black lists use different domains (called query domains) to separate IP addresses based on the reason they are

blacklisted. One domain will contain only IP addresses for dialup accounts, another domain will contain only IP addresses for bulk mailers. This type of categorization allows you to select the reasons for which you do not want to accept black listed mail, and use the domain that contains IP addresses for that reason.

Categorizing IP Addresses by a Reason Code/IP Address

Other black lists return a reason code/IP address (i.e. 127.0.0.3) as to why an IP address is black listed. Although all IP addresses are listed in one domain, each will contain a reason code that explains why it is included. For example, a code of 127.0.0.3 may represent a dial-up account, and a code of 127.0.0.4 might represent a bulk mailer. The Fiveten black list is an example of one of these black lists.

How to Determine Which Method a Black List Uses

Unfortunately, there is no standard across black lists. One black list may use separate query domains, and another may use reason/IP codes. Likewise, there is no standard across the reason/IP codes that are returned. For one black list, 127.0.0.3 may represent dial-ups, and on another black list this code may represent bulk mailers. The best resources for finding out this information are the black lists themselves. By going to their web sites, you can learn how each black list classifies the listed IP addresses.

Related Topics

Server Level Antispam Options (Black Lists) (on page 270)

Understanding DNS Black Lists (on page 90)

Server Level DNS Black Lists (on page 89)

Trusted Black Lists (on page 277)

Add/Edit the DNS Black List (on page 92)

Add/Edit DNS Black List

How to get here

This pop-up enables you to either edit an existing DNS black list or configure a new DNS black list.



Important: Fields cannot be left blank or contain spaces.

- **Name.** Enter a name in the text box to identify a new black list. This can be any name that you want, and will be used in log lines to identify the black list entry.

- **Server.** In the text box, enter the domain name or IP address of the DNS server to contact for black list queries. This field contains an asterisk (*) by default, which indicates that the default IMail Server DNS is used for black list queries, where it relays the DNS query to the DNS server for the black list. Using the asterisk eliminates the need to enter the IP address or domain.
- **Query Domain.** In the text box, enter the domain to query in the zone file. This name usually matches the server domain name. However, sometimes a black list will contain multiple zones to query on the same server. When this happens, the server name and the query domain will be different. The only way to know this is to read the documentation for the black list being used.
- **Type.** Select the type of lookup that the black list performs from the list box.
  - **ADDR (ADDRESS).** This type of black list uses a message's "FROM" address to determine whether the message is spam.
  - **DNS.** This type of black list checks the IP address of the connecting SMTP server against spam databases to determine whether the message is spam. If the IP address is listed in one of the black list's databases, the message is identified as spam.
  - **HELO.** This type of black list checks the domain supplied in the HELO or EHLO command to determine whether to accept the message. The domain name that is given in the HELO/EHLO command must match the IP address.
  - **RHS (RIGHT-HAND SIDE).** This type of black list checks the information following the @ symbol supplied in the "MAIL FROM" command to determine whether the message is spam.
- **Enable.** Select the check box to enable the black list.
- **TCP/IP First.** Some black lists, especially ones that supply .txt records, have packets that are too large to transmit via the UDP protocol. These lists disable UDP access and require TCP to query the black list. Select this check box to allow the administrator to flag a list as one of these types.

OK. Click this button to add to DNS black list. The new black list appears on the DNS Black Lists page, but will not be permanent until the **"Save"** button is clicked.

Cancel. Click this button to cancel adding a new black list. No new information should appear on the DNS Black Lists page.

Related Topics

Understanding DNS Black Lists (on page 90)

How Black Lists Work (on page 91)

Setting DNS Black Lists Options (on page 277)

Setting Connection Checks Options (on page 274)

Spool Manager

How to get here

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. The Spool directory is also where the IMail Server *log files* (on page 411) are stored.

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.

To view the files in the queue, see *Managing Messages in the Spool* (on page 95).

Files in the Queue

Files in the queue are on the way in or out. The **Number of Tries** column shows the number of times IMail has attempted to deliver a message. When this number reaches the number of **Tries Before Return to Sender**, which is set on the *IMail SMTP Services* (on page 392) page, the message is returned to the sender as "undeliverable."

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* (on page 97) and by the *file extension* (on page 96).

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 any time required to transmit large files over slow links. For example, the time-out 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.

Attachments

Attached files also appear in the queue. For multiple attachments, the Windows Explorer naming convention is used. For example, 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 run the Spool Cleaner utility to delete old files. For more information, see *Cleaning the Spool Directory* (on page 96).

Related Topics

About Log Files (on page 411)

Beginning Character of Files in the Spool (on page 97)

File Extensions of Files in the Spool (on page 96)

Troubleshooting the Spool Directory (on page 391)

Cleaning the Spool Directory (on page 96)

Managing Spool Manager

How to get here

The mail queue, also known as the spool, is a directory that stores mail messages that are waiting for delivery. Files in the queue include incoming messages, outgoing messages, attachments, and error messages. The queue releases messages one at a time in the order that they were received. The Spool Manager provides status information about the IMail queue.

- **File Name**. File names determine what stage a message is in. see *Beginning Character of Files in the Spool* (on page 97) and *File Extensions of Files in the Spool* (on page 96).
- **Status**. Current status of files in the queue. Click **Refresh List** to update.
- **Date Created**. Creation date of the file.
- **Tries**. Number of times IMail has attempted to deliver a message. When this number reaches the number of **Tries Before Return to Sender**, which is set on the *IMail SMTP Services* (on page 392) page, the message is returned to the sender as "undeliverable."
- **From**. Displays e-mail address from whom the message was created.
- **Recipients**. Displays e-mail address of all recipients.
- **Delete File.** Click **Delete File** to delete selected file(s) from the spool directory.
- **Send Now.** Click **Send Now** to attempt delivery of only the selected messages in the spool list.
- **Refresh List.** Refresh page to display the most current files in the spool.
- **Start Queue Run**. Click **Start Queue Run** to attempt to force delivery of all of the messages in the queue.

Related Topics

About the Spool Directory (Queue) (on page 94)

About Log Files (on page 411)

Beginning Character of Files in the Spool (on page 97)

File Extensions of Files in the Spool (on page 96)

Troubleshooting the Spool Directory (on page 391)

Cleaning the Spool Directory (Isplcln.exe)

Isplcln.exe is a command utility that 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: 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 deletes all log files that are thirty days old or older.

Command	Function
-x	The number of days old a file must be before it is deleted.
-y	The number od days old a log file must be before it is deleted.

File Extensions of Files in the Spool

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.
- .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**.**

Related Topics

About the Spool Manager (Queue) (on page 94)

About Log Files (on page 411)

Beginning Character of Files in the Spool (on page 97)

Troubleshooting the Spool Manager (on page 391)

Beginning Character of Files in the Spool

Files in the spool are mail messages on the way in or out of the spool. You can determine what stage a message is in by looking at the first character in the file name and by looking at the file extension.

When an e-mail message is in the spool, it is a "data file" with a file name that begins with D. Data files have matching T, Q, and A files as they get processed.

First Character in Filename	Explanation
A	A data file undergoing connection filtering and SPF testing; deleted when message is delivered.
D	A file that matches the data file while the message is inbound; when the message is fully received; the T file is renamed to a Q.
T	A file that matches the data file while the IMail Server attempts to deliver the message.
A	A locked file that is being processed. These files also have a tilde (~) in the file extension. (If three characters of the filename are nex, the file is being processed via (??web messaging or the

	IMail Web Client) or imail1.exe).
*~??	A locked file that is being processed. These files also have a tilde (~) in the file extension. (If three characters of the filename are nex, the file is being processed by (??web messaging or the IMail Web Client) or imail1.exe).
F	A Mail to Fax file.

Normally, messages are processed in a few seconds or minutes. However, if there is message delivery problem, the associated files may stay in the spool longer.

IMail does not delete the data file when a message is not deliverable; therefore, no message is ever truly lost.

If you reboot your system while a message is being received, IMail may leave behind the T and D files. You can use the *Spool Cleaner utility* (on page 96) to clean up these files.

Related Topics

About the Spool Directory (Queue) (on page 94)

About Log Files (on page 411)

File Extensions of Files in the Spool (on page 96)

Troubleshooting the Spool Manager (on page 391)

System Default User Settings

How to get here

The System Default User Settings are default values when creating new user accounts.

- **Maximum Mailbox Size.** (**Unlimited** is default value) In the list box, click select **Specify size** and enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account or select **Unlimited** mailbox size for each user.

  The following will occur when a users mailbox is over the **Max Mailbox Size**:

  - All new incoming mail will no longer be received, they will get bounced.
  - New messages can still be sent.

- Other users sending messages to a users full mailbox will receive a postmaster message stating the user's mailbox is exceeding the allowed limit.
- When users mailbox is below the **Max Mailbox Size**, it will begin receiving mail again.

Important: If you set a size limit for mailboxes, then by default the Disk Space Indicator will be displayed when users log into the Web client. To turn it off, see *Managing the Client Disk Space Indicator* (on page 148).

Note: When the Maximum Mailbox Size value is set to a value other than Unlimited in the user settings, it will override the e-mail domain's default settings. In this case, the unlimited value is no longer unlimited for the domain default settings. For more information, see *Adding a New IMail User* (on page 143).

- **Maximum Mailbox Messages.** (**Unlimited** is default value) Enter the default maximum number of messages allowed in each user's mailbox.

Note. When the Maximum Mailbox Messages value is set to a value other than Unlimited in the user settings, it will override the e-mail domain's default settings. In this case, the unlimited value is no longer unlimited for the domain default settings. For more information, see *Adding a New IMail User* (on page 143).

- **Encoding**. Default message encoding used for sending messages. Default setting is Unicode (UTF-8).
  - **Unicode (UTF-8).** Choose this character set for multi-language mail. In IMail, this includes English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish.
  - **English (US-ASCII).** For composing e-mail for English-speaking readers, based on the English alphabet.
  - **Western European (ISO-8859-15).** For composing e-mail in French, Italian, German, or Spanish.
  - **Chinese Traditional (BIG5).** For composing e-mail in traditional Chinese.
  - **Chinese Simplified (GB2312).** For composing e-mail in simplified Chinese.
  - **Japanese (ISO-2022-JP).** For composing e-mail in Japanese.
- **Add as Collaboration User** (selected by default). Select to create a collaboration user for Workgroupshare to allow synchronization with Outlook.
- **Allow Password Change** (selected by default). Select to let the user change his/her password in Web Messaging.
- **Account Enabled** (selected by default). Select to let the user use the e-mail account remotely through POP3 or IMAP4. You can clear this option to disable the account without changing the user's password or removing him/her from the domain.
- **Access Information Services** (selected by default). Select to make the user's LDAP information available in the LDAP database.

Caution: Clearing the **Access Information Services** check box permanently deletes the user's information from the LDAP database and prevents distribution of user information via the IMail LDAP service. There is currently no method available to hide information within an OpenLDAP database, except to use this option to clear user information. If you want to show LDAP information for this user after clearing this option, you must add the LDAP information back into the user information.

- **Access LDAP Attributes** (selected by default). Select to let the user modify his/her LDAP attributes (name, address, organization, etc.).
- **Allow Web Calendaring.** Select to let a user access IMail Web Calendaring.
- **Allow Use of Ipswitch Instant Messaging** (not selected by default). Select this check box to allow the user access to Instant Messaging.
- **Add as Ipswitch Instant Messaging User** (selected by default, if IMail User DB is in use). Select this check box if the user should also be added to the Instant Messaging DB. If Instant Messaging is set to use the IMail User Database the check box will be automatically set and grayed.
- **Allow Web Access.** Select to let a user access his/her IMail Web Messaging client and IMail Web Calendaring.
- **Allow Microsoft Exchange ActiveSync®**. (Not set by default) Enables a user with a mobile device to synchronize using ActiveSync® to their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

  Disabling this feature at the User Property level will disable synchronization for only the specified user.

  See the **Mobile Synchronization Setup** (on page 80) for more client help.

Note: Disabling Exchange ActiveSync® at the User Property Level will disable mobile synchronization for only the specified user.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

Note: Disabling Exchange ActiveSync® at the System Default User Setting level only affects new domains being created. A new domain will have the Domain Default User settings with Exchange ActiveSync® disabled, which will disable all new users on the new domain from using ActiveSync®.

- **List Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete any list server mailing list on the mail domain(s) he or she has list administrator permissions to.

- **Domain Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete users and aliases (except program aliases) on the mail domain (host) he or she has domain administrator permission to. Domain administrators also have List administrator permissions.
- **System Administrator Permissions** (cleared by default). Select to let a user have full administration capabilities with all IMail features and options. System administrators have Domain administrator and List administrator permissions.

Save. Click to save your settings.

System Default Web Mail Preferences

How to get here

The IMail Administrator has the capability to globally set default web client preferences for all new users, to include Viewing, Composing, and Forwarding, Replying & Deleting preferences.

Viewing Web Client Preferences

The following items only apply to the standard version of Web Messaging.

- **Upon login go to:** This drop down box gives two alternate selections for login.
  - **INBOX** - Initial login will open the INBOX message folder.
  - **Default Page** - Initial login will open the mail folders page, displaying all message folders and sizes. This can be manually accessed by clicking on **E-mail** in the folder tree.
- **Show Message Preview Pane.** Checked by default. This feature will split your message list window, and allow user to preview the selected message below the message list.

  When preview pane is off, the message list window will display more messages, but will required a double click to view a message.



Note: This control is not used with the low bandwidth template, as it is set to automatically open a message when clicked on.

- **Display selection check boxes in grids**. Checked by default for new users. This feature allows selection of a message by use of a check box. Unchecked will remove the check boxes and revert to usage of message highlighting with usage of the shift+ key for blocks of messages, or the ctrl+ for multiple random messages on a page.



Note: For existing users before who have a saved user preferences file, the check box option will be turned off. For existing users that have never saved their preferences, they will be treated as a new user with the check box option turned on.

Important: "Check All" will only apply to the currently displayed page for the standard web client.

- **Enable Usage Bar**. Checked by default for new users. Controls only the display of the Maximum Mailbox Size bar in the web client. Turning this feature off will still adhere to the Maximum Mailbox Size, which is set at the Domain Properties, and/or User Properties.

The following preferences only apply to the low bandwidth template (Web Messaging Lite)

- **Upon login go to:** This drop down box gives three alternate selections for login.

  1 **Default Page** - By default the initial login page displays a message showing the number of unread messages. This message is also a link to the user's **INBOX** if there are new unread messages. This check box will skip this page and go to **View Mail Folders**.

  2 **Mail Folders Page** - Initial login will open the mail folders page, displaying all message folders.

  3 **INBOX** - Initial login will open the INBOX message folder.

- **Message Click Action**. Use the drop down menu for the following two options:
  - View Message in Existing Window
  - View Message in New Window
- **Number of items to show per page.** Default set to 10. Allows flexibility for users customize page display. If the number is larger than the screen will hold, a scroll bar will appear. When there are more messages to display than the setting, then linked page numbers will display at the bottom of the message folder. The highlighted page will tell you what page you are on.

  If your messages per page is set to a number that higher than what will fit in your web browser window, a scroll bar will appear.
- **Maximum To/From characters to display**. Default set to 50. To/From is the address displayed in a mailbox folder list. The number set will control the maximum number of characters that will display in the mailbox folder before it truncates the display. This control allows flexibility for users with wide monitors or large font.

  For example, for a user with a wide monitor can set this field to 70 to allow more characters to display. Should the screen display not be wide enough the displayed line will wrap within the text box.
- **Maximum Subject characters to display**. Default set to 50. Subject is the message subject displayed in a mailbox folder list. The number set will control the maximum number of characters that will display in the mailbox before it truncates the display. This control allows flexibility for users with wide monitors or large font.

For example, for a user with large font can set this field to 30 to allow fewer characters to display. Should the screen display not be wide enough the displayed line will wrap within the text box.

- **"Check All" will check all items across all pages in a mail folder.** Unchecked by default. This feature controls check boxes on a current page or check boxes for all messages in the mailbox folder.

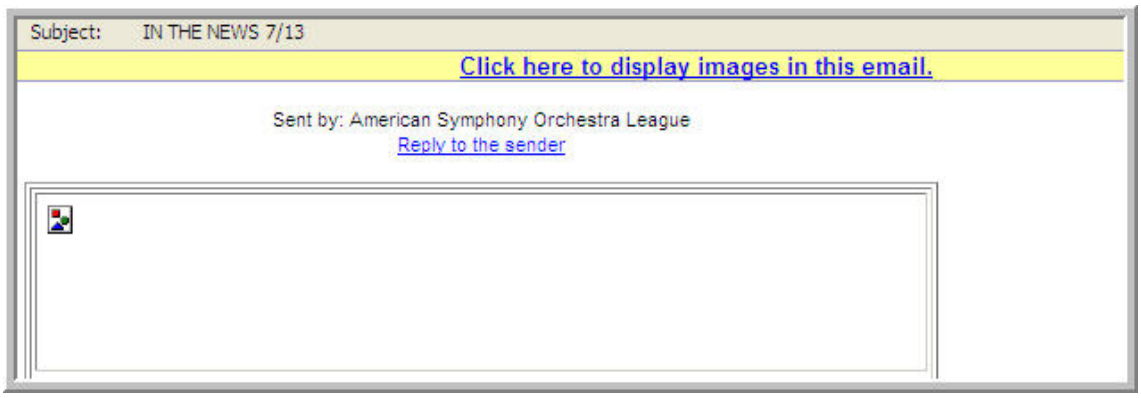
  When this feature is checked, the "Check All" will mark all messages in the mailbox folder.

  When this feature is unchecked, the "Check All" will check only the messages on the current page.

The following preferences apply to both versions of Web Messaging

- **Enable image suppression for e-mail messages**. Checked by default. This feature will suppress images for all messages. Once the link has been clicked, the images will always display when the message is selected.

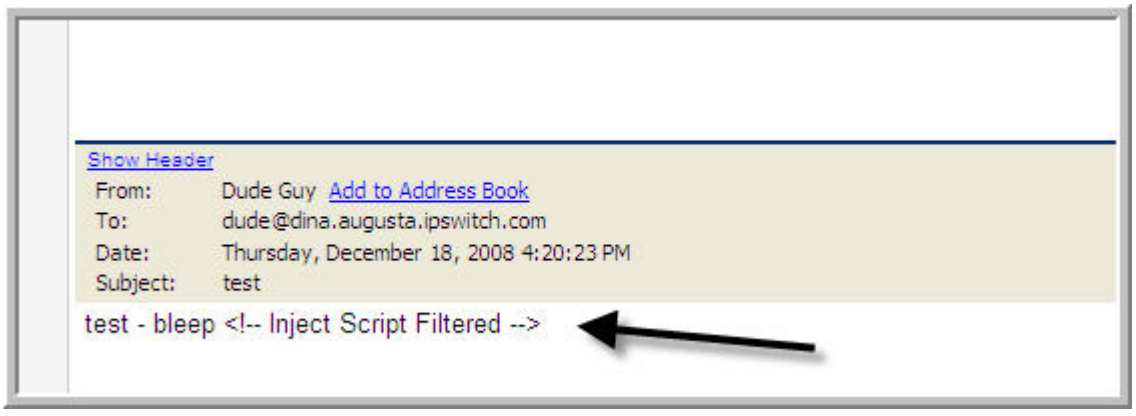
  A link will appear as seen below:



Note: Once this link is clicked, the images will always display when the message is selected.

- **Enable javascript removal for e-mail messages**. Checked by default. This feature when checked will search all messages and disable any javascript encountered.

  Example showing that a script was removed:



Composing

Following are User **Preferences** settings for composing new messages:

- **Default New Message Style.**
  - **HTML.** Select this option if you wish to compose your message using features such as bold, italic, underlining, multiple fonts, multiple colors, bullets, numbering, etc.
  - **Plain Text.** Select this option if you wish to compose your message using no formatting.
- **Open Compose In:**
  - **Same Window.** This option lets you compose your message in a new message window that replaces the message list.
  - **New Window.** This option lets you compose your message in a new message window separate from the message list.
- **Save Copy of Outgoing Messages in Sent folder.** Choose this option if you wish to keep copies of your messages in the **Sent** folder.
- **Save Recipients by Default.** Choose this option if you wish to automatically add recipients to your Contacts when sending new messages.
- **Enable Autosuggest for contacts (Web Messaging Standard Only).** Choose this option to automatically suggests message recipient names as you type them in the To text box. If the recipient exists in your contacts, a drop down containing the complete name appears.



Note: This feature is not available in the low bandwidth template, due to the large bandwidth requirement.

Forwarding

- **Include original message.** Checked by default. This check box will include the original message when it is forwarded.
- **Include attachments.** Checked by default. This check box will include the original attachments when it is forwarded.

Replying

- **Include original message.** Checked by default. This check box will include the original message in your reply.



Note: Reply To does not include attachments. Use **Forward** to include attachments when sending a message.

Deleting

- **Deleted Folder / Purge.** Radio button selection.
  - **Move message to deleted folder.** Set by default. Select this option to move deleted messages to the Deleted folder. These messages remain in the folder

until you purge them by selecting one or more messages and clicking the **Delete** button.

- **Purge Message.** Select this option to completely remove deleted messages. Purged messages are deleted from the server and cannot be recovered.

- **Confirm Before Delete.** Set by default. Select this check box to have IMail ask you to confirm the request before deleting the selected message(s).

Save. To save any changes made.

Registry Backup

In This Section

Back Up IMail Registry (on page 105)

Restoring IMail Registry (on page 106)

Backing Up System Files (on page 107)

Backing Up User Mailboxes (on page 107)

Back Up IMail Registry

There are two methods of saving the IMail registry keys. Select one that is fits best.



Important: This will only backup user data for domains that use the IMail User Database.

Backing Up Registry with Command Line

To backup the registry keys for IMail using **command line** use the following steps.

1. Click **Start > Run > "cmd"**. This will open a DOS window.
2. At the DOS prompt enter the following command all on one line:

```
regedit /e c:\imail\imail.reg
HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail
```

3. Entering a different path or file name is up to the administrator.

This will copy the complete IMail registry "hive" to the c:\imail directory folder.

Backing up Up Registry Manually

To backup the registry keys **manually** using export with the following steps:

1. Click on **Start > Run >** type "**regedit**" and click OK.
2. Go to the path: `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`
3. Select "IMail" Registry key
4. Right click and select "Export".
5. Select the desired path, and name the file.
6. The "selected branch" field should show the following:
7. `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`
8. Click **Save**.

This will save all domain data, user names and user passwords for all domains that use the IMail user database.

Related Topics

Restoring IMail Registry (on page 106)

Backing Up IMail Server System Files (on page 107)

Backing Up User Mail (on page 107)

Restoring IMail Registry

There are two methods of restoring the IMail registry keys. Select one that is fits best.

Restoring using Windows Explorer

1. Go to Windows Explorer and double click on the exported .reg file
2. A prompt asking if you are sure that you want to add the information in "path name".reg file to the registry. Click "Yes" if the path name looks correct.
3. A prompt telling you it was successfully entered into the registry.

Restoring using "regedit"

1. Make sure a copy of the registry file is on the server.
2. Click on **Start > Run >** type "**regedit**" and click OK.
3. Click File > Import

4 Browse to the copy of the registry file on the server.

The current IMail registry keys will be overwritten with the selected file.

Related Topics

Back Up IMail Registry (on page 105)

Backing Up IMail Server System Files (on page 107)

Backing Up User Mail (on page 107)

Backing Up IMail Server System Files

IMail Server stores its system files in the \IMail directory, unless you have given it a different name. You can make a backup copy of the IMail Server directory tree.

Related Topics

Back Up IMail Registry (on page 105)

Restoring IMail Registry (on page 106)

Backing Up User Mail (on page 107)

Backing Up User Mail

Users' mail is stored in directories below `\IMail`, usually under `IMail\users`, but each domain may have mail stored, under `\IMail\domain\users`, if default paths were selected.

Daily backups should include these directories.

Related Topics

Back Up IMail Registry (on page 105)

Restoring IMail Registry (on page 106)

Backing Up IMail Server System Files (on page 107)

CHAPTER 6

Domain Administration

In This Chapter

System Administrator 109
Domain (Host) Administrator 110
Domains 110
User Administration 124
DomainKeys / DKIM 162
Spam Filtering (Domain Level) 182
Alias Administration 183
List Administration 192
LDAP Settings 217
InBound / Outbound Rules 218
White List Administration 242
Peer List 244

System Administrator

A System Administrator has full administrative control over all IMail permissions and options.

A System Administrator can create other System Administrator accounts, with full permissions. A System Administrator has full administration capabilities for all IMail permissions and options. System Administrators have Domain Admin and List Admin permissions.

System Administrator permissions is set at **User Administration > User Properties.**

Related Topics

Domain Management (on page 110)

User Administration (on page 124)

User Properties (on page 126)

Domain (Host) Administrator

A Domain Administrator can add, modify, or delete users or aliases (except program aliases) on the mail domain (host) he or she has domain administrator permissions to.

Domain Administrators cannot delete System Administrator accounts, permissions, or change other System Administrator settings. Domain Administrators will also not display System Administrator rules or file directory information. Domain Administrators have List Administrator permissions.

Domain Administrator permissions is set at **User Administration > User Properties.**

Related Topics

Domain Management (on page 110)

User Administration (on page 124)

User Properties (on page 126)

Domains

How to get here

Domain Properties, add new mail domains, and delete existing mail domains.

Search box. Enter a domain name or part of a domain name that you want to search for in the list of available domains, then click **Search**.

Domain List

- **Name** list. Click a domain name to modify the Domain Properties.
- **Top Directory**. Displays top directory path of the associated domain.
- **IP Address**. Displays the IP address of the associated domain. Will display "$virtualX" if there is no associated IP address.

Add. Click **Add** to create a new domain on IMail Server . For more information, see *Adding a New IMail Domain* (on page 47).

Edit. Select a domain to modify, then click **Edit**.

Delete. Select a domain that you want to delete from the Domains list, then click **Delete** to delete the domain.

Related Topics

Setting Domain Properties (on page 41)

User Administration (on page 124)

Alias Administration (on page 183)

List Administration (on page 192)

LDAP Settings (on page 54)

Attachment Blocking (on page 227)

InBound / Outbound Rules (on page 218)

White List Administration (on page 242)

Peer List (on page 244)

Domain Properties

How to get here

Use the Domain Properties to add a new mail domain, add or update a domain alias, enable virus scanning, and set other message and mailbox properties.

General Domain Settings

- **Domain Name (Official Host Name or OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **TCP /IP Address**. Select **Select an IP Address** to use an IP address (domain) for the mail domain or select **Virtual** (*virtual IP address* (on page 53)) to use a non-IP-ed domain.



Note: If you change a primary domain to a virtual domain, you must restart ALL services. See *Changing the IP Address of a Host* (on page 60) for more information.

- **Top Directory.** Enter the name or **Browse** to the directory where users, lists, and web files for this mail domain are stored.
- **Domain Aliases**. Specify alternate domain names for which you want the mail domain to accept mail. Multiple aliases are separated by a space. This field is limited to 255 characters.



Note: If the Domain Alias name is changed, stop and restart all services via the *Service Administration* (on page 367) page in order for the change to take effect correctly.

Example: If the mail domain 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 fred@domain2.com.

Note: Host Alias requires also that the proper updates to DNS must be made to work correctly.

Domain Options

- **Enable Microsoft Exchange ActiveSync®**. (Enabled by default) Allows all enabled users for the specified domain to use ActiveSync® for synchronizing mobile devices with their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. Once installed Outlook will synchronize e-mail, contacts, calendars, notes, and tasks with their mobile devices.

  See the **Mobile Synchronization Setup** (on page 80) for more information.

Warning: Disabling ActiveSync® at the domain level will disable all ActiveSync® users on the specified domain, overriding the User Property setting.

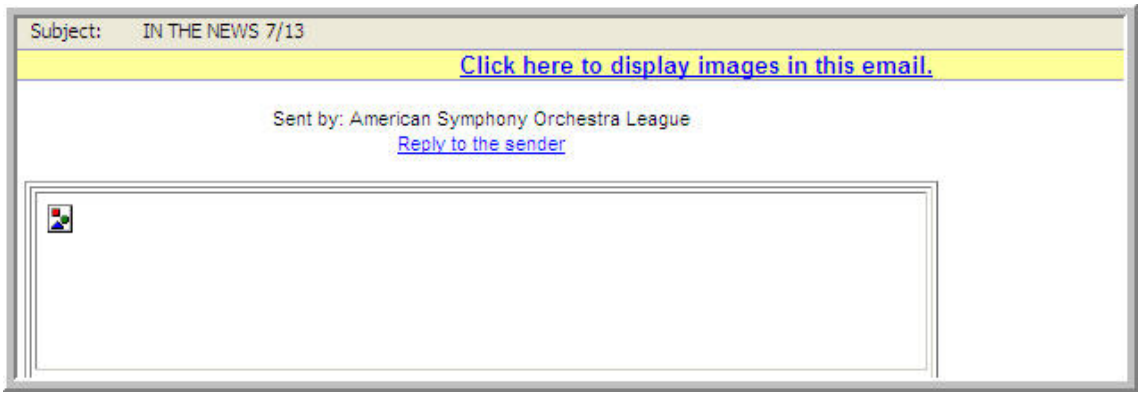
Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

- **Enable Web Calendar.** Specify whether the current mail domain allows access to the Web Calendaring Service (if available in software version).
- **Enable Ipswitch Instant Messaging** (selected by default if available in software version). Specify whether the current mail domain will allow access to the Ipswitch Instant Messaging service.

Note: If Enable Ipswitch Instant Messaging and/or Enable Web Calendaring is selected at the mail domain level, it can be selected or cleared for each user of the mail domain on the *User Properties* (on page 126) page.

- **Enable Virus Scanning** (selected by default if available in software version).
  - If this option is selected, virus scanning is performed for:
    - the primary domain
    - any virtual domain (IP-less) that is bound to the primary domain
  - If this option is cleared, virus scanning is performed for:
    - any virtual domain (IP-less) that is bound to the primary domain and has the anti-virus option selected at the virtual domain level.
- **Enable image suppression for e-mail messages**. Checked by default. This feature will suppress images for all messages. Once the link has been clicked, the images will always display when the message is selected.

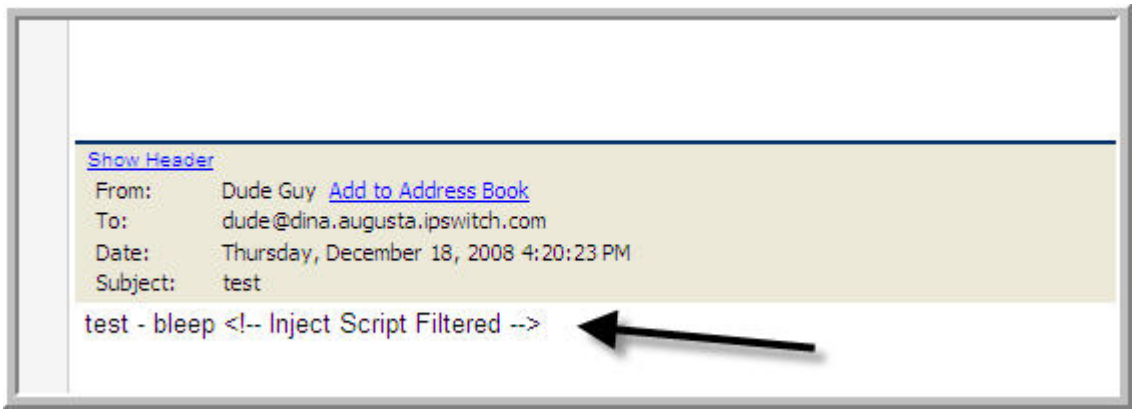
A link will appear as seen below:



Note: Once this link is clicked, the images will always display when the message is selected.

- **Enable javascript removal for e-mail messages**. Checked by default. This feature when checked will search all messages and disable any javascript encountered.

  Example showing that a script was removed:



- **Enable content filtering for authenticated users.** Select this option to enable content filtering for all messages that are received from authenticated users.

Note: Even if the **Enable content filtering for authenticated users** option is selected, content filtering is not performed on messages that are sent from system and host administrators. This prevents mail from being filtered twice in cases where a message is misidentified as spam and the administrator then forwards it on to its intended recipient.

Note: The primary domain is identified in the **Domain Name** box.

Message and Mailbox Options

- **Default Maximum Mailbox Size.** (0 is default value). Enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account. Enter zero for an unlimited mailbox size for each user.
- **Max. Outbound Message Size.** (0 is default value). Enter the maximum size (in bytes, KB, MB, or GB) of an outbound message. Any message that is larger than the size entered will be bounced. Enter 0 for an unlimited maximum outbound message size. For more information, see *File Attachment Settings.* (on page 26)
- **Single Message Maximum Size.** (0 is default value). Enter the maximum size (in bytes, KB, MB, or GB) of a single message. Messages that exceed this size are returned to the sender. Enter 0 for an unlimited single message maximum size. For more information, see *File Attachment Settings.* (on page 26)
- **Full Mailbox Notify (percentage).** (0 is default value). Enter a percentage that users will be notified when their mailbox is within a specified percentage of being full. Enter 0 for no full mailbox notification. *Example* (on page 71). See also *customizing the notification message* (on page 71).
- **Full Mailbox Notify Address.** Enter 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 administrator's address.
- **Default Maximum Messages.** (0 is default value) Enter the default maximum number of messages allowed in each user's mailbox. Enter 0 for an unlimited number of messages.
- **Maximum User Count.** (0 is default value) Enter the maximum number of users that can be registered for this mail domain. Enter 0 for an unlimited number of users.
  - **Domain Administrators** will not be able to add users once the Max User Count has been met. A message on the User Administration page will also display: "The User Limit for the domain has been reached".
  - **System Administrators** will still be allowed to add users, but a message on the User Administration page will still display: "The User Limit for the domain has been reached".



Tip: The user count configured on the Domain Properties page **DOES NOT** include Root.

- **Current User Count**. Displays the current number of users registered for this mail domain.
- **Sub- mailbox Creation.** Select how to handle a message when it arrives for a user and is addressed to a sub-mailbox that does not exist. Select one of the following actions:
  - **Create.** (Default setting) Creates the sub-mailbox and delivers the message.
  - **Send to Inbox.** Does not create the sub-mailbox. Instead the message is delivered to the "main" mailbox.
  - **Bounce.** Bounces the mail back to the sender as an invalid e-mail address.
- **Minimum POP Frequency (minutes).** Enter the number of minutes delay between POP logins for each user. The default is 0 (or unlimited) logins.

Caution: If you enter any number of minutes for Minimum POP frequency, you are limiting popping to one mailbox per user per domain. If you create more than one mailbox for a user, that mailbox will receive mail, but the user will be unable to access it unless the POP frequency is set at 0 (zero). An error message is sent to the client and logging in is denied, Different e-mail clients may handle this error differently.

Example: Outlook and Outlook Express display the userid/password dialog box continuously. If you click **Cancel,** the error message the POP server returns is: "-ERR login frequency exceeded - try again later" User Database Setting.

User Login Settings

Tip: To reset a suspended account, go to User Properties page and uncheck "Account Suspended" check box. This will reset the user's failed login attempts to zero.

Tip: A successful login will also reset failed login attempts to zero.

- **Allowed Login Attempts Before Account Lockout** (Default Setting = 3). Allows the user "X" login attempts before displaying:

  "You have exceeded the maximum number of allowed login attempts. Please try again later."

Note: Setting **Allowed Login Attempts for Account Lockout to zero (0)** will disable this feature.

- **Allowed Lockouts Before Account Suspension**. (Default Setting = 3). Allows the user "X" of the above message before being suspended and requiring an Administrator intervention, with the message:

  "Due to multiple failed login attempts, your account access has been suspended."

Note: Setting **Allowed Login Attempts for Account Suspension to zero (0)** will disable the feature.

Drop down text box contains the following password complexity settings:

- **0 - Weak** (Default Setting). Requires password to be:
  - Must be at least 3 characters in length
  - And not to exceed 30 characters
  - White space characters are not allowed
- **1 - Simple.** Requires password to be:
  - Must be at least 6 characters in length

- And not to exceed 30 characters
- Must contain at least 1 letter (regardless of case)
- Must contain at least 1 number or special character
- White space characters are not allowed

- **2 - Moderate.** Requires password to be:
  - Must be at least 6 characters in length
  - And not to exceed 30 characters
  - Must contain at least 1 letter (lower case)
  - Must contain at least 1 number
  - Must contain at least 1 special character or 1 capital letter
  - White space characters are not allowed
- **3 - Strong.** Requires password to be:
  - Must be at least 8 characters in length
  - And not to exceed 30 characters
  - Must contain at least 1 lower case letter
  - Must contain at least 1 capital letter
  - Must contain at least 1 number
  - Must contain at least 1 special character
  - White space characters are not allowed
- **4 - Extreme.** Requires password to be:
  - Must be at least 8 characters in length
  - And not to exceed 30 characters
  - Must contain at least 2 lower case letters
  - Must contain at least 2 capital letters
  - Must contain at least 2 numbers
  - Must contain at least 2 special characters
  - White space characters are not allowed



Note: Valid special characters `[! @ # $ % ^ & * ( ) _ + } { " : ' ? / > . < ; , ]`

User Database Setting

- **User Database Type** area, select one of the following:
  - *IMail Database* (on page 68)
  - *NT/AD Database* (on page 65)

- **Configure.** Click to *Configure your NT or Active Directory database* (on page 52).

- *External Database* (on page 68)
  - **Configure.** Click to *Configure an external database.* (on page 68)

Save. Click **Save** to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Related Topics

Adding a New IMail Domain (on page 47)

Adding a New IMail User (on page 143)

Creating an E-mail Alias (on page 185)

Changing the IP Address of a Host (on page 60)

Virtual mail domains with IP addresses (on page 123)

Virtual mail domains without IP addresses (on page 123)

Creating External User Database for a Mail Domain

IMail Server can use an external database to register and authenticate users on a particular mail domain . Users that you add to and delete from an IMail Server host are also added to and deleted from the external database.

Important: Remember to restart the IMail Services, after creating external database.

Before you use an external database for a mail domain, 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 and database documentation for information on the System DSN .

Important: When you configure a DSN to an SQL data source in the Microsoft Windows ODBC Data Source Administrator, it may default to **Named Pipes** network library. Make sure that you set the connection type to **TCP/IP in order for the external database to work correctly.**

After you have verified the System DSN that points to the database you want to use, you can configure an external database.

Note: The external database can reside locally with the IMail Server.

Configuring an External User Database

The connection between IMail Server and an external user database is accomplished via a dynamic link library (DLL file). IMail Server includes a sample .dll file (ODBCUSER.DLL). This DLL uses the ODBC method, but can be modified to support other external database methods. The complete source code for this DLL is provided upon request from Ipswitch.

When you configure an external user database, IMail Server creates an ODBC database that holds tables configured with the correct fields. The fields are identified in the **Table Name** text box. After the database is created and the ODBC system data source name is established in the ODBC Source Administration tool (located in the Windows Control Panel), you can use the database to store user authentication information and user properties. This information can be managed through IMail Administrator, including adding and deleting users.

Important: When using an external database, any IMail service you run (except the Log Server) must be set up from the Windows Control Panel Services application so the account that IMail Server runs under has access to the external database.

To create a mail domain that uses an external database:

1. In IMail Administrator, click **Domain** > **Domain Properties**.
2. In the **User Database** section, select **External Database** from the **User Database type** list box.
3. Click the **Configure** button. A domain options page appears.
   - **External Database Implementation DLL.** Enter the full path to the odbcuser.dll installed on your local server or the path of a .DLL that supports the functions: GetUserEntry, SetUserEntry, DeleteUserEntry, AuthorizeUser, GetFirstUserEntry, and GetNextUserEntry. (These are defined in the odbcuser.h file.)
   - **ODBC System Data Source Name (DSN).** Enter the source name for the database where the user information is stored. IMAILSECDB is the default name that the ODBC link uses.

Important: For users using SQL 7.0 or above, enter the following information after the ODBC System Data Source Name box: `DSN_NAME;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.

   - **Table Name**. Enter the table name within your ODBC database. Leaving **"[default]"** in this text box will use your domain name as the table name. All periods will be replaced with underscores.

Important: The table name cannot begin with a number.

Example:
If you use the Data Source Name IMAILSECDB and the username AUGUSTA and password GEORGIA, the correct format of the ODBC System Data Source Name box is: `IMAILSECDB;UID=AUGUSTA;PWD=GEORGIA`

- **Table name**. Enter the database table name. If the field is blank or contains [default], the host name is used with dots replaced by underscores. The Table name cannot begin with a number.
- **Enable Multiple Connections** to allow multiple connections from the external database to IMail Server.
- **Maximum Number of Connections** to set the maximum number of connections from the external database to IMail Server

Save. Click this button to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

Related Topic

Domain Properties (on page 41)

Configuring an NT/AD database

Use this page to configure your NT or Active Directory database. See also *Using the Windows NT/AD Database* (on page 65).

NT/AD Domain Name. Enter the name of your NT or Active Directory domain name.

NT Database.

- **Machine name of Domain Controller.** Enter the machine name for your Domain Controller.

Active Directory Database

Important: To hide Active Directory users from the IMail Server, under user properties, add the word "built-in" in the front of the user description. *Example.* (on page 52)

- **Use Active Directory**. Select the check box to use Active Directory.
- **Naming Context.** If the Active Directory check box is selected, the naming context will be pulled from the Root DSE Directory Service Entry. If you choose to not use the default naming context, you can enter one of your choice.
- **Save.** Click to save your settings.
- **Cancel.** Click to cancel your settings and return to the Domain Properties page.

Related Topic

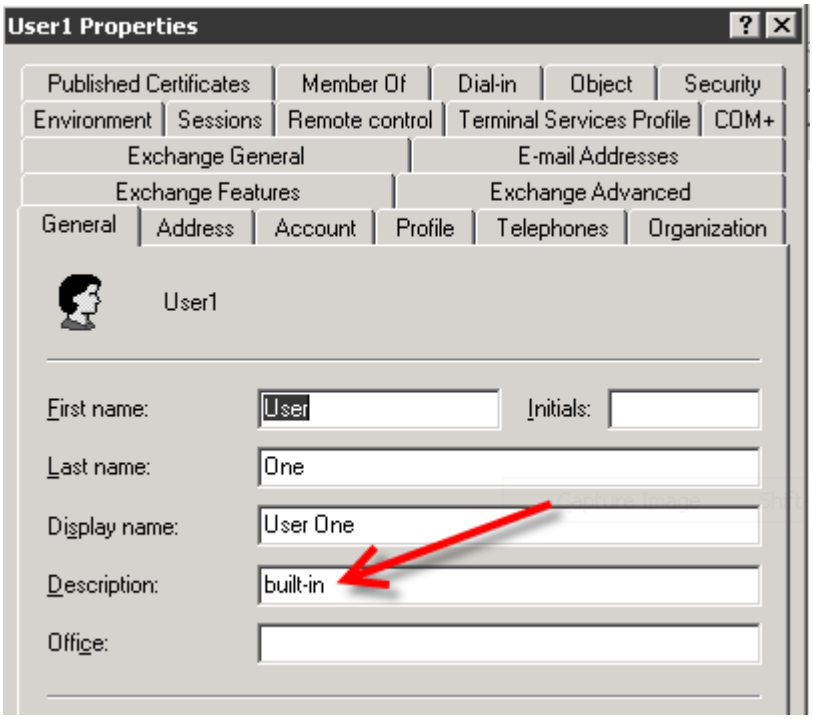
Example of Active Directory "built-in" (on page 52)

Example of Active Directory "built-in"

The example below will hide User1 from the IMail Server as a valid user.

1. Go to **Start > Control Panel > Administrative Tools > Active Directory (AD) Users and Computers**.
2. Select **AD** container with users.
3. Right click specified user that you would like to hide from the IMail Server, and select **Properties**.
4. Enter the word `"built-in"` into the **Description** field.
5. Click **"OK"**

Note: `"built-in"` must be at the front of the **description** text box. Trailing words are permitted.



Related Topics

Domain Properties (on page 41)

Configuring NT/AD Database (on page 52)

Deleting an IMail Domain

How to get here

Use the domain options to delete a mail domain.

- **Search** box. Enter a domain name or part of a domain name that you want to search for in the list of available domains, then click **Search**.
- **Clear.** Click **Clear** to reset the domain search results list to display all available domains.
- **Name** list. Click a domain name or multiple domain names to delete the domain(s).
- **Add.** Click **Add** to create a new domain on IMail Server. For more information, see *Adding a New IMail Domain* (on page 47).
- **Delete.** Select a domain or multiple domains that you want to delete from the Domains list, then click **Delete** to delete the domain(s).

Related Topics

Domain Properties (on page 41)

Adding a Virtual Host (adddomain.exe)

AddDomain.exe is a utility for adding virtual domains. It can be used to simply add a single domain, but is especially useful in a batch file to add multiple domains.

Basic Command Syntax and Example

Usage:

```
adddomain -h Hostname -i IPAddress -t TopDir

[-a Aliases -u IM | NT | External -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -m

[-t TopDir -a Aliases -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -i IPAddress -t TopDir -u External

[-e DLLFilename -o ODBC_DSN -n TableName]

adddomain -h Hostname -delete

adddomain -f Filename
```

Examples:

1 In the following example, since the -e, -o,or -n options are not specified, the external database relies on the default “values %“Imail_top dir”%odbcuser.dll , IMAILSECDB, and [default] accordingly:

```
adddomain -h newhost1 -i virtual -u external
```

2 The following command populates an external database with settings of C:\mydll.dll, IMAILSECDB, and [default]:

adddomain -h newhost2 -i virtual -u external -e C:\mydll.dll

3 The following example changes an existing host (notice the -m for modify) to use an ODBC Data Source Name (DSN) of MyNewDSN. If the other fields of -e and -n were previously set, they will be preserved. If the other fields of -e and -n were not previously set, they will be set with the default values:

adddomain -h ExistingHost -m -u external -o MyNewDSN



Note: The -e, -o, and -n commands must be used in conjunction with -u EXTERNAL.

4 If you need to specify a DSN other than 'IMailSecDB,' or you need to specify a userID and password (required when setting up a DSN to connect to an SQL database), use the -o switch :

adddomain -h ExistingHost -m -u external -o IMailSecDB;UID=MyUser;

PWD=MyPassword

5 The following example shows how to add a new virtual host (or virtual host with an IP) using an external database:

adddomain -u external -t C:\IMail\newdomain_com -i virtual

-o IMailSecDB;UID=sqluser;PWD=sqlpassword -n table_name

6 Adddomain.exe supports the following command line options:

Command	Function
-h	Fully qualified host name; must match the IMail official host name
-i	IP address or virtual IP address for an IP-less host
-t	Path (full or relative) to the top directory for the domain
-m	Command to modify existing settings instead of creating new ones
-a	Alias list for a host
-u	User data base to use (IMail, NT, or external)
-e	Path to external database implementation DLL
-o	External database ODBC system Data Source Name (DSN)
-n	External database table name
-x	Default max mailbox size (in kbytes).
-s	Default max number of messages for mailbox.
-f	Path to the file containing the settings to modify
-r	Maximum number of users allowed on this host.
-delete	Removes the virtual host.

Note: AddDomain.exe does not warn when assigning already claimed IP addresses to new hosts. Assigning an already used IP address to another host will orphan the original host without warning.

Setting the IP Address for a Virtual Host

If you use a virtual IMail domain with an IP Address , all capabilities of regular IMail Server mail domains are available to virtual domains with IP addresses. The only limitations of virtual IMail domains with IP addresses are:

- Each virtual domain requires its own unique IP address.

In Microsoft Windows, this requires the extra step of adding an IP address in the Windows NT TCP/IP configuration in the Control Panel (**Network Connections** > **Local Area Connections > Properties** > **TCP/IP Protocol** > **Advanced**).

Note: With Microsoft Windows 2000, you can add up to five IP addresses in the Network applet. If you need to add more than five IP addresses, refer to the operating system documentation for more information.

Important: Whether you use a real IP address or a virtual IP address, you need to make the proper DNS entries for your mail domain(s). If you use a virtual IP address, the MX record (in DNS) for the mail domain must point to a real IP address.

Setting Up a Virtual Host Without an IP Address

If you use a virtual IMail domain without an IP Address, IMail Server assigns the virtual IP address. This method lets you have a virtual mail domain without an IP address. After you set up a virtual IMail domain, use an MX record in your DNS to point the virtual mail domain to a real IP address.

Important: Whether you use a real IP address or a virtual IP address, you need to make the proper DNS entries for your mail mail domain(s). If you use a virtual IP address, the MX record (in DNS) for the mail domain must point to a real IP address.

There are several limitations to a virtual IMail domain without an IP address:

- Users must log in to mail accounts on the mail domain by specifying their User ID as userid@virtualhost, where `userid` is the User ID and virtualhost is the host name. This associates the IMail Server with the correct virtual IMail domain.
- LDAP server does not work with virtual IMail domains that do not use an IP address.

When to use IP-less Virtual IMail Domains

Virtual IMail domains 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.

Example:

Your primary domain is called abracadabra.com. You want all mail that is sent to merlin.com to be forwarded to info@abracadabra.com. To accomplish this:

1. Set up a virtual IMail domain without an IP address for merlin.com and do not create any users for merlin.com.
2. Set up a *nobody alias* (on page 187) for merlin.com pointing to a user ID on abracadabra.com. All mail to any user at merlin.com is sent to the specified user at abracadabra.com (in this case, info@abracadabra.com).

User Administration

How to get here

Use the Users Administration properties to search for users in the selected domain, access and edit user properties, add new users, or delete existing users. Columns can be sorted allowing Admins, or Disabled Users to sort to the top. Two utilities have been added to this page to allow **Renaming a Username** and **Resetting a users password** without going to User Properties.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Search Box. Requires entering a minimum of two characters, and the search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered. Search target includes both the "Username" and "Full Name" columns as criteria for search selection.



Caution: Search requires a minimum of two characters for the search process to begin.



Note: Column Titles when clicked will sort the user list for the current session only. Refreshing the page will reset to Username sorting. **Example.** Clicking on the "Disabled" column heading twice will sort all the disabled users to the top of the page.

User Image Icons.

-  Displays for users with System Administrator permissions.
-  Displays for users with Domain Administrator permissions.
-  Displays for users with List Administrator permissions.
-  Displays for all normal users, with no Administrative permissions.
-  Displays for disabled users.

User List

- **Username** list. Click a username to modify the User Properties.
- **Full Name.** Full name as entered in User Properties page.

- **System Admin.** This column displays whether or not the specific user is set up as a System Administrator on the User Properties page.
- **Domain Admin.** This column displays whether or not the specific user is set up as a Domain Administrator on the User Properties page. A domain administrator
- **List Admin.** This column displays whether or not the specific user is set up as a List Administrator on the User Properties page.
- **Enabled.** This column displays whether or not the user's account is active or disabled, as set up on the User Properties page.
- Rename Username Utility. Utility link to allow renaming a Username.
- Change Password Utility. Utility link to allow changing a users password.

Tip: The user count configured on the Domain Properties page **DOES NOT** include Root.

Add. Click **Add** to create a new user to the current domain. If the maximum number of users is reached, the button will be grayed out. For more information, see *Adding a New IMail User* (on page 143). The maximum number of users is configured on the Domain Properties page.

Edit. Select and highlight a user, then click **Edit** to update an existing user.

Delete. Select a user that you want to delete from the current domain, then click **Delete** to delete the user.

Related Topics

Adding an IMail User (on page 143)

Deleting an IMail User (on page 148)

Adding Users Using Adduser.exe (on page 422)

Default User Settings (on page 98)

User Utilities (on page 136)

Creating Config_CommonAddrBook.cgi (on page 445)

Change Password

How to get here (on page 125)

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed.

- **User ID.** Displays the selected user ID (user name) for the email account.
- **Password.** Enter a new password. Passwords are limited in length to 3 to 30 alphanumeric characters and cannot include asterisks.
- **Confirm Password.** Enter the user password a second time to confirm the password.

Save. Click to validate and save new password.

Cancel. Click to not change password.

Related Topics

User Properties (on page 126)

User Properties

How to get here

Use the User Properties to change a user's settings, such as: user password, user ID, maximum mailbox size and maximum number of mailbox messages, add user to Collaboration, and change other user mailbox properties.

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **Domain Name(OHN)**. This clickable link displays only for existing users. This link will take you to the **Domain Properties** page.
- **Username.** Enter a unique user ID (user name) for the e-mail account. User IDs are limited in length to 1 to 30 characters and must be created from alphanumeric characters. The User ID cannot include spaces and must be a unique name within the domain you are adding the user to.
- **Full name.** Enter the user's First Name and Last Name.
- **Reply To Address.** Enter an e-mail address that you want to have IMail Server automatically use as your Reply To mail address. You can leave this text box empty to let recipients of this user's messages reply to the User ID you entered. You can also enter an e-mail address that omits the domain 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 Stephanie@mail.ipswitch.com, you can enter Stephanie@ipswitch.com.
- **Forwarding Address.** Enter an e-mail address that you want to have IMail Server automatically forward a user's mail to.



Example 1: To forward messages to another mailbox besides INBOX by entering the forwarding address as `"yourUserID-othermailbox@domainname.com".`



Example 2: To forward e-mail to another mailbox and also keep a copy in the original mailbox by preceding the e-mail address with `"."` allowing no spaces in between. `".,userid@domainname.com"`

- **Maximum Mailbox Size.** (0 is default value) Enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account. If the user's Maximum Mailbox Size is zero, the defaults for the e-mail domain are applied to the user. If the domain's default is also zero, the Maximum Mailbox Size for the user is unlimited. If a new message will cause the total size of all mailboxes in a user's account to exceed the Maximum Mailbox Size value, the mail is returned to the sender.



Note: Currently the maximum allowed mailbox size is 2 GB.

When the Maximum Mailbox Size value is non-zero, it will override the e-mail domain's default settings. In this case, the 0 value is no longer unlimited for the domain default settings.

The following will occur when a users mailbox is over the **Max Mailbox Size**:

- All new incoming mail will no longer be received, they will get bounced.
- New messages can still be sent.
- Other users sending messages to a users full mailbox will receive a postmaster message stating the user's mailbox is exceeding the allowed limit.
- When users mailbox is below the **Max Mailbox Size**, it will begin receiving mail again.

- **Maximum Mailbox Messages.** (0 is default value) Enter the default maximum number of messages allowed in each user account. If the user's Maximum Mailbox Messages is zero, the defaults for the e-mail domain are applied to the user. If the domain's default is also zero, the Maximum Mailbox Messages for the user is unlimited.

  When the Maximum Mailbox Messages value is non- zero, it will override the e-mail domain's default settings. In this case, the 0 value is no longer unlimited for the domain default settings.



Note: If the **Max Mailbox Messages** option is set to 5, and the user's main mailbox already has five messages stored, then the next message sent to the user's main mailbox is bounced. However, if the next message is sent to a sub-mailbox instead, the message is delivered as long as there are less than five messages currently stored in the sub-mailbox.

- **Encoding**. Default message encoding used for sending messages. Default setting is Unicode (UTF-8).
  - **Unicode (UTF-8).** Choose this character set for multi-language mail. In IMail, this includes English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish.
  - **English (US-ASCII).** For composing e-mail for English-speaking readers, based on the English alphabet.
  - **Western European (ISO-8859-15).** For composing e-mail in French, Italian, German, or Spanish.
  - **Chinese Traditional (BIG5).** For composing e-mail in traditional Chinese.

- **Chinese Simplified (GB2312).** For composing e-mail in simplified Chinese.
- **Japanese (ISO-2022-JP).** For composing e-mail in Japanese.

- **Allow Password Change** (selected by default). Select to let the user change his/her password in Web Messaging.
- **Account Enabled** (selected by default). Select to let the user use the e-mail account remotely through POP3 or IMAP4. You can clear this option to disable the account without changing the user's password or removing him/her from the domain.
- **Access Information Services** (selected by default). Select to make the user's LDAP information available in the LDAP database.



Caution: Clearing the **Access Information Services** check box permanently deletes the user's information from the LDAP database and prevents distribution of user information via the IMail LDAP service. There is currently no method available to hide information within an OpenLDAP database, except to use this option to clear user information. If you want to show LDAP information for this user after clearing this option, you must add the LDAP information back into the user information.

- **Access LDAP Attributes** (selected by default). Select to let the user modify his/her LDAP attributes (name, address, organization, etc.).
- **Allow Web Calendaring.** Select to let a user access IMail Web Calendaring.
- **Allow Use of Ipswitch Instant Messaging.** (Only present if Ipswitch Instant Messaging is installed). Select to let the user have access to Instant Messaging. Clear the check box to disable the user's access.
- **Allow Web Access.** Select to let a user access his/her IMail Web Messaging client.
- **Account Suspended.** Automatically becomes enabled if a user's web access becomes suspended from the settings set in the **Domain Properties > User Login Settings.** To re-enable web access web access for the user Account Suspended must be manually unchecked.



Note: This feature is controlled on a per domain basis in *Domain Properties* (on page 41) under **User Login Settings**.

- **Allow Microsoft Exchange ActiveSync®**. (Not set by default) Enables a user with a mobile device to synchronize using ActiveSync® to their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

  Disabling this feature at the User Property level will disable synchronization for only the specified user.

  See the **Mobile Synchronization Setup** (on page 80) for more client help.



Note: Disabling Exchange ActiveSync® at the User Property Level will disable mobile synchronization for only the specified user.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

- **List Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete any list server mailing list on the mail domain(s) he or she has List Administrator permissions to.
- **Domain Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete users and aliases (except program aliases) on the mail domain (host) he or she has domain administrator permission to.
- **System Administrator Permissions** (cleared by default). Select to let a user have full administration capabilities with all IMail features and options. System Administrators have Domain Administrator and List Administrator permissions.

Lists and Groups Aliases

- **Lists**. Select the available domain's list(s) from the list box to which the user wants to subscribe.
- **Group Aliases.** Select the available domain's group alias(es) from the list box to which the user wants to belong.

 **(Add to)**. Select row and click to add.

 **(Remove from)**. Select row from user text box and click to remove.

 **(Add All)**. Click to add all rows to users text box.

 **(Remove All)**. Click to remove all rows from users text box.

Change Password

Depending on the *Domain Setting for User Login Settings > Password Strength* (on page 41) which controls the complexity of user passwords. Dialog will display the password strength required when modifying.

- **Password.** Enter a new password. Passwords are limited in length to 3 to 30 alphanumeric characters and cannot include asterisks.
- **Confirm Password.** Enter the user password a second time to confirm the password.

Related Tasks

- *Add User to Collaboration* (on page 147)
- *Specify Corresponding Collaboration User* (on page 147)

Note: After a user is added to Collaboration via the **Add User to Collaboration link**, this link changes to **Grant Access to a Public Folder.** However, if the new collaboration user's current e-mail address is not used in the **Account E-mail** text box, the user is not recognized as the same user and the **Add User to Collaboration link continues to display** for the user.

Save. Click to save changes.

Related Topics

Adding a IMail User (on page 143)

Deleting an IMail User (on page 148)

Adding Users Using Adduser.exe (on page 422)

Default User Settings (on page 98)

User Utilities (on page 136)

Domain Default User Settings

How to get here

The Domain Default User Settings are default values when creating new user accounts.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **Maximum Mailbox Size.** (**Unlimited** is default value) In the list box, click select **Specify size** and enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account or select **Unlimited** mailbox size for each user.

  The following will occur when a users mailbox is over the **Max Mailbox Size**:

  - All new incoming mail will no longer be received, they will get bounced.
  - New messages can still be sent.
  - Other users sending messages to a users full mailbox will receive a postmaster message stating the user's mailbox is exceeding the allowed limit.
  - When users mailbox is below the **Max Mailbox Size**, it will begin receiving mail again.

Important: If you set a size limit for mailboxes, then by default the Disk Space Indicator will be displayed when users log into the Web client. To turn it off, *see Managing the Client Disk Space Indicator* (on page 148).

Note: When the Maximum Mailbox Size value is set to a value other than Unlimited in the user settings, it will override the e-mail domain's default settings. In this case, the unlimited value is no longer unlimited for the domain default settings. For more information, see *Adding a New IMail User* (on page 143).

- **Maximum Mailbox Messages.** (**Unlimited** is default value) Enter the default maximum number of messages allowed in each user's mailbox.

Note. When the Maximum Mailbox Messages value is set to a value other than Unlimited in the user settings, it will override the e-mail domain's default settings. In this case, the unlimited value is no longer unlimited for the domain default settings. For more information, see *Adding a New IMail User* (on page 143).

- **Encoding**. Default message encoding used for sending messages. Default setting is Unicode (UTF-8).
  - **Unicode (UTF-8).** Choose this character set for multi-language mail. In IMail, this includes English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish.
  - **English (US-ASCII).** For composing e-mail for English-speaking readers, based on the English alphabet.
  - **Western European (ISO-8859-15).** For composing e-mail in French, Italian, German, or Spanish.
  - **Chinese Traditional (BIG5).** For composing e-mail in traditional Chinese.
  - **Chinese Simplified (GB2312).** For composing e-mail in simplified Chinese.
  - **Japanese (ISO-2022-JP).** For composing e-mail in Japanese.
- **Add as Collaboration User** (selected by default). Select to create a collaboration user for Workgroupshare to allow synchronization with Outlook.
- **Allow Password Change** (selected by default). Select to let the user change his/her password in Web Messaging.
- **Account Enabled** (selected by default). Select to let the user use the e-mail account remotely through POP3 or IMAP4. You can clear this option to disable the account without changing the user's password or removing him/her from the domain.
- **Access Information Services** (selected by default). Select to make the user's LDAP information available in the LDAP database.

Caution: Clearing the **Access Information Services** check box permanently deletes the user's information from the LDAP database and prevents distribution of user information via the IMail LDAP service. There is currently no method available to hide information within an OpenLDAP database, except to use this option to clear user information. If you want to show LDAP information for this user after clearing this option, you must add the LDAP information back into the user information.

- **Access LDAP Attributes** (selected by default). Select to let the user modify his/her LDAP attributes (name, address, organization, etc.).

- **Allow Web Calendaring.** Select to let a user access IMail Web Calendaring.
- **Allow Use of Ipswitch Instant Messaging** (not selected by default). Select this check box to allow the user access to Instant Messaging.
- **Add as Ipswitch Instant Messaging User** (selected by default, if IMail User DB is in use). Select this check box if the user should also be added to the Instant Messaging DB. If Instant Messaging is set to use the IMail User Database the check box will be automatically set and grayed.
- **Allow Web Access.** Select to let a user access his/her IMail Web Messaging client and IMail Web Calendaring.
- **Allow Microsoft Exchange ActiveSync®**. (Not set by default) Enables a user with a mobile device to synchronize using ActiveSync® to their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

  Disabling this feature at the User Property level will disable synchronization for only the specified user.

  See the **Mobile Synchronization Setup** (on page 80) for more client help.



Note: Disabling Exchange ActiveSync® at the User Property Level will disable mobile synchronization for only the specified user.



Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.



Note: Disabling Exchange ActiveSync® at the Domain Default User Setting level will disable ActiveSync® for new users being created for the domain.

- **List Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete any list server mailing list on the mail domain(s) he or she has list admin permissions to.
- **Domain Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete users and aliases (except program aliases) on the mail domain (host) he or she has domain administrator permission to. Domain admins also have List admin permissions.
- **System Administrator Permissions** (cleared by default). Select to let a user have full administration capabilities with all IMail features and options. System admins have Domain admin and List admin permissions.

Save. Click to save your settings.

Domain Default Web Preferences

How to get here

The IMail Administrator has the capability to set domain level default web client preferences for all new users, to include Viewing, Composing, and Forwarding, Replying & Deleting preferences.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Viewing Web Client Preferences

The following items only apply to the standard version of Web Messaging.

- **Upon login go to:** This drop down box gives two alternate selections for login.
  - **INBOX** - Initial login will open the INBOX message folder.
  - **Default Page** - Initial login will open the mail folders page, displaying all message folders and sizes. This can be manually accessed by clicking on **E-mail** in the folder tree.
- **Show Message Preview Pane.** Checked by default. This feature will split your message list window, and allow user to preview the selected message below the message list.

  When preview pane is off, the message list window will display more messages, but will required a double click to view a message.



Note: This control is not used with the low bandwidth template, as it is set to automatically open a message when clicked on.

- **Display selection check boxes in grids**. Checked by default for new users. This feature allows selection of a message by use of a check box. Unchecked will remove the check boxes and revert to usage of message highlighting with usage of the shift+ key for blocks of messages, or the ctrl+ for multiple random messages on a page.



Note: For existing users before who have a saved user preferences file, the check box option will be turned off. For existing users that have never saved their preferences, they will be treated as a new user with the check box option turned on.



Important: "Check All" will only apply to the currently displayed page for the standard web client.

- **Enable Usage Bar**. Checked by default for new users. This feature controls the display of the maximum disk space usage bar in the web client. Disabling the display will still maintain the Maximum Disk Space Usage rules.

The following preferences only apply to the low bandwidth template (Web Messaging Lite).

- **Upon login go to:** This drop down box gives three alternate selections for login.

1. **Default Page** - By default the initial login page displays a message showing the number of unread messages. This message is also a link to the user's **INBOX** if there are new unread messages. This check box will skip this page and go to **View Mail Folders**.

2. **Mail Folders Page** - Initial login will open the mail folders page, displaying all message folders.

3. **INBOX** - Initial login will open the INBOX message folder.

- **Message Click Action**. Use the drop down menu for the following two options:
  - View Message in Existing Window
  - View Message in New Window
- **Number of items to show per page.** Default set to 10. Allows flexibility for users customize page display. If the number is larger than the screen will hold, a scroll bar will appear. When there are more messages to display than the setting, then linked page numbers will display at the bottom of the message folder. The highlighted page will tell you what page you are on.

  If your messages per page is set to a number that higher than what will fit in your web browser window, a scroll bar will appear.
- **Maximum To/From characters to display**. Default set to 50. To/From is the address displayed in a mailbox folder list. The number set will control the maximum number of characters that will display in the mailbox folder before it truncates the display. This control allows flexibility for users with wide monitors or large font.

  For example, for a user with a wide monitor can set this field to 70 to allow more characters to display. Should the screen display not be wide enough the displayed line will wrap within the text box.
- **Maximum Subject characters to display**. Default set to 50. Subject is the message subject displayed in a mailbox folder list. The number set will control the maximum number of characters that will display in the mailbox before it truncates the display. This control allows flexibility for users with wide monitors or large font.

  For example, for a user with large font can set this field to 30 to allow fewer characters to display. Should the screen display not be wide enough the displayed line will wrap within the text box.
- **"Check All" will check all items across all pages in a mail folder.** Unchecked by default. This feature controls check boxes on a current page or check boxes for all messages in the mailbox folder.

  When this feature is checked, the "Check All" will mark all messages in the mailbox folder.

  When this feature is unchecked, the "Check All" will check only the messages on the current page.

Composing Web Client Preferences

Composing

Following are User **Preferences** settings for composing new messages:

- **Default New Message Style.**
  - **HTML.** Select this option if you wish to compose your message using features such as bold, italic, underlining, multiple fonts, multiple colors, bullets, numbering, etc.
  - **Plain Text.** Select this option if you wish to compose your message using no formatting.
- **Open Compose In:**
  - **Same Window.** This option lets you compose your message in a new message window that replaces the message list.
  - **New Window.** This option lets you compose your message in a new message window separate from the message list.
- **Save Copy of Outgoing Messages in Sent folder.** Choose this option if you wish to keep copies of your messages in the **Sent** folder.
- **Save Recipients by Default.** Choose this option if you wish to automatically add recipients to your Contacts when sending new messages.
- **Enable Autosuggest for contacts (Web Messaging Standard Only).** Choose this option to automatically suggests message recipient names as you type them in the To text box. If the recipient exists in your contacts, a drop down containing the complete name appears.



Note: This feature is not available in the low bandwidth template, due to the large bandwidth requirement.

Forwarding

- **Include original message.** Checked by default. This check box will include the original message when it is forwarded.
- **Include attachments.** Checked by default. This check box will include the original attachments when it is forwarded.

Replying

- **Include original message.** Checked by default. This check box will include the original message in your reply.



Note: Reply To does not include attachments. Use **Forward** to include attachments when sending a message.

Deleting

- **Deleted Folder / Purge.** Radio button selection.
  - **Move message to deleted folder.** Select this option to move deleted messages to the Deleted folder. These messages remain in the folder until you purge them by selecting one or more messages and clicking the **Delete** button.

- **Purge Message.** Selected by default. Select this option to completely remove deleted messages. Purged messages are deleted from the server and cannot be recovered.

- **Confirm Before Delete.** Checked by default. Select this check box to have IMail ask you to confirm the request before deleting the selected message(s).

Save. To save any changes made.

Microsoft Exchange ActiveSync Users

How to get here

Microsoft Exchange ActiveSync® Users by Domain

To allow the IMail Administrator capability to enable / disable multiple ActiveSync® users at a time, this domain **User List** is sorted by users with enabled ActiveSync® users listed first, followed by the disabled users.

- **Name**. The unique User ID (user name) of the users e-mail account.
- **ActiveSync® Enabled**. (Yes / No) User properties check box for allowing usage of ActiveSync® for a single user.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

Enable. Select a user(s) and click **Enable** to allow ActiveSync® usage for a user.

Disable. Select a user(s) and click **Disable** to turn off ActiveSync® usage for a user.

Related Topics

Microsoft Exchange ActiveSync® (on page 78)

User Utilities

How to get here

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

The User Utilities page gives you access to:

- Use *Domain User Changes* (on page 137) to set global settings for all of the current domains user accounts.

- *Import NT Users* (on page 66) from the NT Database to add them to the IMail Database, if a domain uses the IMail Database for user mail accounts.
- Using *Find Orphans* (on page 140) to locate an orphan directory in the IMail Users directory.
- *Set Default "Reply To"* (on page 141) to set the domain portion of the Reply To address to be the same for all users on the current domain.
- *Delete Messages by Date* (on page 141) to delete messages for all users by a specified date.

Related Topics

Deleting Old Messages (immsgexp.exe) (on page 141)

Sending Mail to All Users (mailall.exe) (on page 143)

Creating Config_CommonAddrBook.cgi (on page 445)

Exporting Users to File (on page 140)

v10.5 Domain User Changes

How to get here

You can use Domain User Changes to set or unset specific settings for all user accounts for the current domain.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **Maximum Mailbox Size.** Choose from the following three options:
  - **No change.** Select this option to indicate no change from the settings indicated on the **Standard User Settings** page.
  - **Use the default setting for the domain.** Select this option to use the domain's default setting.
  - **Specify size.** If you select this option, enter the numerical amount in the text box and select either bytes, KB, MB, or GB from the list box.
- **Maximum Mailbox Messages.** Choose from the following three options:
  - **No change.** Select this option to indicate no change from the settings indicated on the **Standard User Settings** page.
  - **Use the default setting for the domain.** Select this option to use the domain's default setting.
  - **Specify size.** If you select this option, enter the numerical amount in the text box and select either bytes, KB, MB, or GB from the list box.
- **Encoding**. Default message encoding used for sending messages. Default setting is Unicode (UTF-8).

- **Unicode (UTF-8).** Choose this character set for multi-language mail. In IMail, this includes English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish.
- **English (US-ASCII).** For composing e-mail for English-speaking readers, based on the English alphabet.
- **Western European (ISO-8859-15).** For composing e-mail in French, Italian, German, or Spanish.
- **Chinese Traditional (BIG5).** For composing e-mail in traditional Chinese.
- **Chinese Simplified (GB2312).** For composing e-mail in simplified Chinese.
- **Japanese (ISO-2022-JP).** For composing e-mail in Japanese.

- **Allow Password Change.** Options are **No Change**, **Yes**, and **No**. Select **No Change** if you want the settings to remain the same as noted in the **Allow Password Change** option on the User Properties page. Select **Yes** to allow users to change passwords remotely. Select **No** to prevent all users from changing their passwords remotely.
- **Grant Account Access.** Options are **No Change**, **Yes**, and **No**. **No Change** indicates users keep the existing settings as noted in the **Grant Account Access** option on the Standard User Settings page. Select **Yes** to let users access their e-mail accounts remotely through POP3 or IMAP4 . Select **No** to prohibit users from accessing their accounts remotely through POP3. This allows you disable accounts without changing users' passwords or removing them from the system
- **Access Information Services.** Options are **No Change**, **Yes**, and **No**. Select **No Change** if you want the settings to remain the same as noted in the **Access Information Services** option on the Standard User Settings page. Select **Yes** if you want to globally provide user information provided in LDAP settings. Select **No** to prevent the distribution of any information about users through LDAP, if you have the LDAP server running.
- **Allow Web Access.** Options are **No Change**, **Yes**, and **No**. Select **No Change** if you want the settings to remain the same as those specified in the **Allow Web Access** option on the Standard User Settings page. Select **Yes** to let users access their IMail Web Messaging client and IMail Web Calendaring. Select **No** to prevent users access to their accounts remotely via the Web.
- **Allow Web Calendaring.** Options are **No Change**, **Yes**, and **No**. Select **No Change** if you want the settings to remain the same as those specified in the **Allow Web Calendaring** option on the Standard User Settings page. Select **Yes** to let users access their IMail Web Calendaring through the Web Client. Select **No** to prevent users access.

Save. Click **Save** to run utility.

Cancel. Click **Cancel** to exit without running utility.

Importing Windows NT Users

How to get here

If a host uses the IMail Database for user mail accounts, you can import users from the NT Database and add them to the IMail database on the Import NT Users page.

Note: This differs from actually using the Windows NT Database, in that although the users keep their same user IDs, Administrators are required to set a default required password for importing these NT Users into the IMail database. Users can change the password after they have been imported.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Import NT User Options

- **Initial Password.** Use this text box to enter an initial password setting for users being imported.

Note: The password must be between 3 and 15 characters.

- **Confirm password.** Use this text box to confirm the password setting for users being imported.
- **Add as Collaboration User.** Select this check box to enable a User or Users selected from the Username list to access the Collaboration tools.
- **Add as Ipswitch Instant Messaging User.** Select this check box to enable a User or Users selected from the Username list to access Ipswitch Instant Messaging.

Existing Users on the NT Database

Search Box. Requires entering a minimum of two characters, and the search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

- **Username.** This column lists the usernames of all users imported from the NT database. You can click on the link under the username to access the user's User Properties.
- **Full Name.** This column lists the display names of the users.

Import. To add a user and password, select a user from the list by selecting the check box next to the Username, enter the initial password and the confirm password, and click **Import**.

Cancel. Click the **Cancel** button to return to the Utility page.

Related Topics

Using the Windows NT Database (on page 65)

Exporting Domain Users to File

The **"Export Users to File"** utility can be accessed using the **IMail Console Administration** under **Utilities**.

Related Topics

User Utilities (on page 136)

Finding Orphan Mail Accounts

How to get here

Use this page to find and delete any mail account that has a directory in the IMail Users directory whose user has been deleted from the user list.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Orphan Mail Options

- **User Directory.** Displays the directory in which the mail accounts reside.
- **Initial Password.** Use this text box to enter an initial password setting for users being imported.



Note: The password must be between 3 and 15 characters.

- **Confirm password.** Use this text box to confirm the password setting for users being imported.
- **Add as Collaboration User.** Select this check box to enable a User or Users selected from the Username list to access the Collaboration tools.
- **Add as Ipswitch Instant Messaging User.** Select this check box to enable a User or Users selected from the Username list to access Ipswitch Instant Messaging.

Orphan mail accounts on the domain.

Search Box. Requires entering a minimum of two characters, and the search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered.



Caution: Search requires a minimum of two characters for the search process to begin.

- **Username.** This column lists IMail User folders that no longer exist in User Administration list.

Delete. Deletes selected Username(s) that still have existing user folders.

Import. Click this button to import orphaned accounts back into your user database.

Cancel. Click this button to return back to Utility page without running utility.

Set "Reply To" Address

How to get here

You can use this page to set the domain portion of the **Reply To** address to be the same for all users on the current domain.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **Reply To Address.** Use the text box to enter the domain portion of the Reply To address for all users on the current domain.



Warning: This utility will not only set the domain name, but will also reset the **Username** to its User Account name.

Save. Click this button to run the utility to change all **"Reply To"** addresses.

Cancel. Click this button to cancel and return to **User Utility** page.

Deleting Messages by Date

How to get here

Use this page to delete messages for all users by a specified date.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

You can choose one of two options to choose the age of messages to delete:

- **Number of Days.** Select this option and enter the number of days that a message can exist before being deleted. For example, if you enter 14, all messages that are more than 14 days old will be deleted.
- **Date.** Select this option and enter a specific date (or choose the date from the calendar), after which all existing messages older than this date will be deleted.

Delete. Click this button to run utility and delete the selected messages.

Cancel. Click this button to return to Utility page without running utility.



Caution: Deletion affects **ALL** users mailboxes not just the **INBOX**.

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
      -m specific_mailbox
      -f fully_qualified_path_to_mailbox (cannot be used with -t and -m)
```

The "startdirectory" will be scanned search only "specific_mailbox" and any message older than "#of_days_to_save" will be deleted.

Option -f gives capability to delete "#of_days_to_save" from a "fully_qualified_path_to_mailbox".

Warning: -t option can not be used with the -f option.

Warning: -m option will be ignored if used with the -f option.

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).

Examples:

The following command deletes all messages in the "C:\Program Files\Ipswitch\IMail" directory that are more than 60 days old.

```
immsgexp -t"C:\Program Files\Ipswitch\IMail" -d60
```

The following command deletes all messages in the "spam" mailbox located in the c:imail directory that are more than 60 days old.

```
immsgexp -t"C:\Program Files\Ipswitch\IMail" -mspam.mbx -d60
```

The following command deletes messages in the "sent" mailbox of the User "jdoe" that are more than 90 days old.

```
immsgexp -d90 -f"C:\Program Files\Ipswitch\IMail\jdoe\sent.mbx"
```

immsgexp.exe command line options

Command	Function
-t	The directory containing the mailboxes from which messages will be deleted.
-d	The number of days that a message will remain on the server before it is deleted.
-m	The name of the mailbox from which messages will be deleted.
-f	Full path to the specific mailbox.

	Warning - Can not be used with the -t option. **Warning** - The -m option will be ignored when using this option.

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 system.

Basic Command Syntax

mailall -h hostname|ALL> -f sender -d [-s Subject] <FullPathToMessageFile>

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. When an e-mail is sent to the program alias, the executable program is invoked and the entire contents of the message is passed as the text for the "mailall.exe" message.

Command	Function
-h hostname	The -h parameter is required. Use it to enter the hostname.
-h ALL	The -h parameter is required. Use this command to specify all hosts on the IMail system.
-f sender	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	This is an optional parameter that specifies the content of the Subject field.
-d	Optional. Use -d to delete the source files when mailing is complete.
FullPathToMessageFile	This parameter is required.

Adding an IMail User

How to get here

Use the User Administration properties to add a new user, user password, set maximum mailbox size and maximum number of mailbox messages, and set other user mailbox properties.

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **Username.** Enter a unique user ID (user name) for the e-mail account. User IDs are limited in length to 1 to 30 characters and must be created from alphanumeric characters. The User ID cannot include spaces and must be a unique name within the domain to which you are adding the user.
- **Full name.** Enter the user's First Name and Last Name.
- **Password.** Enter a user password. Passwords are limited in length to 3 to 30 alphanumeric characters and cannot include asterisks.
- **Confirm Password.** Enter the user password a second time to confirm the password.
- **Maximum Mailbox Size.** (**Unlimited** is default value) Enter the default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account. If the user's Maximum Mailbox Size is unlimited, the defaults for the e-mail domain are applied to the user. If the domain's default is also unlimited, the Maximum Mailbox Size for the user is unlimited. If a new message will cause the total size of all mailboxes in a user's account to exceed the Maximum Mailbox Size value, the mail is returned to the sender.
  When the Maximum Mailbox Size value is a value other than Unlimited, it will override the e-mail domain's default settings. In this case, the unlimited value is no longer unlimited for the domain default settings.
- **Maximum Mailbox Messages.** (**Unlimited** is default value) Enter the default maximum number of messages allowed in each user account. If the user's Maximum Mailbox Messages is unlimited, the defaults for the e-mail domain are applied to the user. If the domain's default is also unlimited, the Maximum Mailbox Messages for the user is unlimited.
  When the Maximum Mailbox Messages value is a value other than Unlimited, it will override the e-mail domain's default settings. In this case, the unlimited value is no longer unlimited for the domain default settings.



Note: If the Max Mailbox Messages option is set to 5, and the user's main mailbox already has five messages stored, then the next message sent to the user's main mailbox is bounced. However, if the next message is sent to a sub-mailbox instead, the message is delivered as long as there are less than five messages currently stored in the sub-mailbox.

- **Encoding**. Default message encoding used for sending messages. Default setting is Unicode (UTF-8).
  - **Unicode (UTF-8).** Choose this character set for multi-language mail. In IMail, this includes English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish.
  - **English (US-ASCII).** For composing e-mail for English-speaking readers, based on the English alphabet.

- **Western European (ISO-8859-15).** For composing e-mail in French, Italian, German, or Spanish.
- **Chinese Traditional (BIG5).** For composing e-mail in traditional Chinese.
- **Chinese Simplified (GB2312).** For composing e-mail in simplified Chinese.
- **Japanese (ISO-2022-JP).** For composing e-mail in Japanese.

User Options

- **Add as Collaboration User.** Select to add the user to the collaboration tools that let users share contact lists, calendars, task lists, notes, and free/busy scheduling information.
- **Allow Password Change** (selected by default). Select to let the user change his/her password in Web Messaging.
- **Account Enabled** (selected by default). Select to let the user use the e-mail account remotely through POP3 or IMAP4. You can clear this option to disable the account without changing the user's password or removing them from the domain.
- **Access Information Services.** (selected by default). Select to let the user modify his/her LDAP attributes (name, address, organization, etc.).



Caution: Clearing the **Access Information Services** check box permanently deletes the user's information from the LDAP database and prevents distribution of user information via the IMail LDAP service. There is currently no method available to hide information within an OpenLDAP database, except to use this option to clear user information. If you want to show LDAP information for this user after clearing this option, you must add the LDAP information back into the user information.

- **Access LDAP Attributes.** Select to allow user to update LDAP user information (name, address, organization, etc.).
- **Allow Web Calendaring.** Controls access to Web Calendaring when using Web Client. Unchecking this will turn off the Web Calendaring link in the Web Client folder tree.
- **Allow Use of Ipswitch Instant Messaging.** (Only present if Ipswitch Instant Messaging is installed). Select to let the user have access to Instant Messaging. Clear the check box to disable the user's access.
- **Add as Ipswitch Instant Messaging User** (selected by default). Select to give the user access to Ipswitch Instant Messaging. This option is only available if Ipswitch Instant Messaging Server is installed and the Enable Instant Messaging option is selected in the Domain Properties. For more information, see *Setting Domain Properties* (on page 41).
- **Allow Web Access.** Select to let a user access his/her IMail Web Messaging client and IMail Web Calendaring.
- **Allow Microsoft Exchange ActiveSync®**. (Not set by default) Enables a user with a mobile device to synchronize using ActiveSync® to their web client information for e-mail, contacts and calendars.

Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

Disabling this feature at the User Property level will disable synchronization for only the specified user.

See the **Mobile Synchronization Setup** (on page 80) for more client help.

Note: Disabling Exchange ActiveSync® at the User Property Level will disable mobile synchronization for only the specified user.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

- **List Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete any list server mailing list on the mail domain(s) he or she has list admin permissions to.
- **Domain Administrator Permissions** (cleared by default). Select to let a user add, modify, or delete users and aliases (except program aliases) on the mail domain (host) he or she has domain administrator permission to. Domain administrators also have List administrator permissions.
- **System Administrator Permissions** (cleared by default). Select to let a user have full administration capabilities with all IMail features and options. System admins have Domain admin and List admin permissions.

Lists and Group Aliases

Adding to Lists and Groups

- **Subscribe to Lists**. Select the domain's list(s) from the list box to which the user wants to subscribe.
- **Add to Group Aliases.** Select the domain's group alias(es) from the list box to which the user wants to belong.

Save. Click **Save** to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Related Topics

Creating Public Mailboxes (on page 374)

Managing Mailboxes (on page 375)

Adding Users Using Adduser.exe (on page 422)

Full Mailbox Notification (on page 71)

Customizing the Notification Message (on page 71)

Add User to Collaboration

How to get here

Add User to Collaboration. This link will only appear if there is no corresponding Collaboration user.

Account Details. Enter the following information, to create an associated WorkgroupShare Collaboration user.

- **Account Name.** Enter the user's account name in the text box.
- **Account E-mail.** Enter the user's E-mail account in the text box.
- **Login Name.** Enter the name with which the user logs into the system.
- **Password.** Enter a password for this collaboration user into the text box.
- **Confirm Password.** Re-enter the password for collaboration this user into the text box.

Save. Click to save settings.

Cancel. Click to cancel any modifications.

Related Topics

User Properties (on page 126)

Specify Corresponding Collaboration User

How to get here

Specify Corresponding Collaboration User. Click to open the link. Displays only when a collaboration user exists for specified user.

- **Use Default Collaboration Login Name**. Displays the current Collaboration Login Name.
- **Specify Collaboration Login Name**. Select this radio button to specify a different Collaboration Login Name than the default.
- **Save.** Click to save your settings.
- **Cancel**. Click to cancel any modifications.

Related Topics

User Properties (on page 126)

Deleting an IMail User

How to get here

Use the User Administration properties page to delete a user. Select the associated check box and click **Delete**.

- **Search box.** Enter a domain name or part of a domain name to search for in the list of available domains, then click Search.
- **Clear.** Click Clear to reset the domain search results list to display all available domains.
- **Username list.** Check the associated check box of a user name or multiple user names to delete the user(s).



Note: Deleting a user will prompt giving the option to delete any associated Lists and/or Aliases.

Deleting an IMail User from Aliases/Lists

Use the Deletion Options page to remove a user from all related aliases and/or all related lists.

- **Remove corresponding user(s) from all related aliases.** Select the check box to remove the user's aliases from IMail.
- **Remove corresponding user(s) from all related lists.** Select the check box to remove the user from all related IMail lists.

Delete. Click to remove the user.

Cancel. Click to cancel your changes and return to the **User Administration** page.

Managing the Client Disk Space Indicator

To turn the disk space indicator off for all users.

1. Locate the iClient.config file in the webclient root directory.
2. In that file, locate the sections that look as follows: `<add key="UsageBarOnOrOff" value="on" />`
3. Change the word “on” to “off” and save the changes.
4. The disk space indicator will be hidden from all users.

To turn the disk space indicator off for specific users.

1. Locate the preferences.config file for the particular user for whom you wish to turn off the indicator. This file will be located in the IMail user's directory, along with his or her mailboxes.
   - New users will not have a preferences.config file until the user saves the preferences.

- If this is a new user, the preferences.config node will initially appear as <enable_usagebar/>. This will need to be replaced with `<enable_usagebar>false</enable_usagebar>`

2 If the preferences.config file is not present,it is possible that it may not be there if the user has not updated their preferences since the latest version of the Web client was installed. If it is not there, simply add the following text. If it is there, then change that node so that it appears as follows:
`<enable_usagebar>false</enable_usagebar>`



Note: If the above node is not present, it must be added at any ending node: e.g. </node>, but do not add at the beginning or the end, as this will cause XML errors.

3 Save the changes to the file and the indicator will no longer appear for this particular user.

ActiveSync Domain Level Checkbox

- **Enable Microsoft Exchange ActiveSync®**. (Enabled by default) Allows all enabled users for the specified domain to use ActiveSync® for synchronizing mobile devices with their web client information for e-mail, contacts and calendars.

  Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. Once installed Outlook will synchronize e-mail, contacts, calendars, notes, and tasks with their mobile devices.

  See the **Mobile Synchronization Setup** (on page 80) for more information.



Warning: Disabling ActiveSync® at the domain level will disable all ActiveSync® users on the specified domain, overriding the User Property setting.



Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

ActiveSync -User Level Checkbox

- **Allow Microsoft Exchange ActiveSync®**. (Not set by default) Enables a user with a mobile device to synchronize using ActiveSync® to their web client information for e-mail, contacts and calendars.

Outlook synchronization is also capable, but requires installing the WorkgroupShare Client. This enables synchronizing e-mail, contacts, calendars, notes, and tasks with mobile devices.

Disabling this feature at the User Property level will disable synchronization for only the specified user.

See the **Mobile Synchronization Setup** (on page 80) for more client help.

Note: Disabling Exchange ActiveSync® at the User Property Level will disable mobile synchronization for only the specified user.

Tip: For a single user to begin using Microsoft Exchange ActiveSync® there are 3 levels that require Microsoft Exchange ActiveSync® to be enabled: **1) System level, 2) Domain level (see Domain Properties) and 3) the User level (See User Properties)**.

Rename User ID

How to get here

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed.
- **Current User ID.** Displays the selected user ID (user name) for the e-mail account.
- **New User ID.** Enter a **New User ID** in the box,
- **Rename Corresponding IIM User.** Displays only if Instant Messaging ID exists for this user.
- **Rename Corresponding Collaboration User.** Displays only if a collaboration user exists for the specified user.

Save. Click to validate and save new User ID.

Cancel. Click to not rename User ID.

Related Topics

User Properties (on page 126)

LDAP Information

How to get here

- Enter user information on the LDAP Information page. LDAP user information is published on the server and the information is made available to LDAP-enabled clients.
- **Domain Name (OHN)**. Displays the name of the specified user's domain.
- **Userid.** Displays the ID of the specified user.

The following information can be updated to the LDAP database for the specified user:

- **Full name**
- **Organization**
- **Department**
- **Address**
- **City**
- **State**
- **Postal Code**
- **Country**
- **Telephone**

Related Topics

LDAP Settings (on page 54)

About LDAP Server (on page 375)

About LDAP Data (on page 376)

Setting IMail LDAP Options (on page 377)

Populating the LDAP Database Using Ldaper.exe (on page 381)

File Directory

How to get here

Use the User Administration properties to add a new user, user password, set maximum mailbox size and maximum number of mailbox messages, and set other mailbox user properties.

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **User ID.** The unique user ID (user name) for the e-mail account.
- **Full name.** The user’s First Name and Last Name.
- **Maximum Mailbox Size.** The default maximum size (in bytes, KB, MB, or GB) of all the mailboxes in each user account. If the user's Maximum Mailbox Size is zero, the defaults for the e-mail domain are applied to the user. If the domain's default is also zero, the Maximum Mailbox Size for the user is unlimited. If a new message will cause the total size of all mailboxes in a user's account to exceed the Maximum Mailbox Size value, the mail is returned to the sender.

  When the Maximum Mailbox Size value is non-zero, it will override the e-mail domain's default settings. In this case, the 0 value is no longer unlimited for the domain default settings.

- **Maximum Mailbox Messages.** The default maximum number of messages allowed in each user mailbox. If the user's Maximum Mailbox Messages is zero, the defaults for the e-mail domain are applied to the user. If the domain's default is also zero, the Maximum Mailbox Messages for the user is unlimited.

  When the Maximum Mailbox Messages value is non- zero, it will override the e-mail domain's default settings. In this case, the 0 value is no longer unlimited for the domain default settings.
- **Directory.** Displays the directory where the selected user's mailbox files are saved.
- **File Name list.** Displays all mailboxes (.mbx) in the user's directory. Other files may also display in the list.
- **Size.** Displays the current total size of the all mailboxes in the user's account.
- **Created.** Displays the date the mailbox file was created.
- **Last Accessed.** Displays the date the mailbox file was last accessed.
- **Last Modified.** Displays the date the mailbox file was last modified.
- **Delete File.** Select a filename(s) in the list, then click **Delete** to delete a mailbox file.

To rename a user's mailbox (.mbx), user ID (.uid), last login (.in) file, vacation (.ima), or other data file:

1. Click associated link of the file (.mbx), (.uid), (.in), (.ima), or other data file in the File Name list, a pop-up window with the User file name appears.
2. Click **Change**. After changing the file name in the text box.
3. Click **Cancel**. To return to File Directory page.

To delete mailbox messages by date:

1. Click a mailbox (.mbx) file in the File Name list, the User File page appears.
2. Click **Delete Messages by Date**. The Delete Messages By Date page appears.
3. Set options to delete messages:
   - **Number of Days box.** Messages are deleted automatically when they reach the specified number of days old.
   - **Date box.** Messages are deleted automatically when they reach the specified date.



Note: There are also two IMail Server utilities available to delete old messages. For more information, see *Cleaning the Spool Directory (isplcln.exe)* (on page 96) or *Deleting Old Messages (immsgexp.exe)* (on page 141).

Deleting Messages by Date for User

How to get here

Use this page to delete messages for a selected user for all or a specific mailbox with a date parameter.

- **Domain Name (OHN).** Displays the official host name (OHN) of the user's domain.
- **Username**. Selected User.

- **Mailbox**. Default is set for all Mailboxes. Drop down text box displaying all mailboxes for selected user.

You can choose one of two options, either by date or by number of days.

- **Number of Days.** Select this option and enter the number of days that a message can exist before being deleted. For example, if you enter 14, all messages that are more than 14 days old will be deleted.
- **Date.** Select this option and enter a specific date (or choose the date from the calendar), after which all existing messages older than this date will be deleted.

Delete. Click this button to delete the selected messages.

Related Topics

Inbound Delivery Rules for Users

How to get here

Use Inbound delivery rules to sort incoming mail messages for each user.

Use the Inbound Rules page to add new inbound rules, edit and delete inbound rules, move inbound rule evaluation priority up or down, add rules, and set actions to take on a message that matches the rule criteria.

The Inbound Rules list displays information about each of the active inbound rules for the selected user. The inbound delivery rules for a user are stored in the `"rules.ima"` file, located in `"...\IMail\users\username"`.

Inbound Rules

- **Name** list. Click a rule name to modify the Rule Settings.
- **Action.** Displays the action to take on a message that matches the rule condition criteria.
- **Condition.** Displays the inbound rule condition associated with a rule.
- **Destination.** Displays the mailbox or forwarding e-mail address that matches the rule condition criteria. A Destination is only available when **Move to Mailbox** or **Forward** are selected in the *Action Type list* (on page 223).

Add. Click **Add** to create a new user rule. For more information, see *Adding Inbound Rule Conditions for Users* (on page 154).

Edit. Select a rule and click **Edit** to modify rule conditions.

Move Up. Select a rule and click **Move Up** to move the rule processing order to a higher priority for e-mail filtering. Rules are processed in the order in which they appear in the Rules list.

Move Down. Select a rule and click **Move Down** to move the rule processing order to a lower priority for e-mail filtering. Rules are processed in the order in which they appear in the Rules list.

Delete. Select a rule that you want to delete from the Inbound Rules list, then click **Delete** to delete the rule.

To Edit an Inbound Rule:

1 From the Rules list, select a rule and click Edit. The Rule Settings page appears.
2 Make the desired changes to the conditions, then click **Save**.

Related Topics

Overview of Mail Delivery Rules (on page 218)

Adding an Inbound Rule Condition (on page 156)

Creating an Outbound Rule for a Domain (on page 222)

How Delivery Rules are stored and processed (on page 219)

Rules Syntax (on page 232)

Adding Multiple Conditions to Rules (on page 157)

Adding Rule for Users

How to get here

Use the Rule Settings page to add new rule conditions, edit rule conditions, delete conditions, move rule condition evaluation priority up or down, add rule conditions, and set actions to take on a message that matches the rule condition criteria.

After you create a rule condition, the new Rule is placed at the bottom of the Rules list. Rules are identified in the list by their sequence in the list, for example (Rule 1, Rule 2; etc.).

Rule Name

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **Rule Name**. Enter the name for the rule.

Conditions

- **Field.** Select the message field to be filtered: **From Address**, **To**, **Subject**, **Sender**, **Body**, or **Header.**
- **Comparison.** Displays **Contains** when the delivery rule filter messages contain the search text. Displays **Does Not Contain** when the delivery rule filter message does not contain the search text.
- **Search Text.** Displays the search criteria that is used in the rule condition.

- **Match Case.** Displays **Yes** or **No** to indicate whether the search text must match the text case used in the Search Text condition.
- **Add Condition...** Click *Adding a Rule Condition* (on page 156).

  To add more than one condition to a rule, create the first condition, then click:

  - **Add AND/OR...** to create the second condition as you did the first. For more information, see *Adding Multiple Conditions to Rules* (on page 157).



Note: The Add Condition button will only display on a new rule with no conditions, and after an AND/OR has been created.



NOTE: Be aware, that a rule can not be saved when an AND/OR exists without a condition.

- **Edit**. Select a condition and click **Edit** or double click to modify a condition.
- **Delete.** Select a condition that you want to delete from the Conditions list, then click **Delete** to delete the condition.
- **Move Up**. Select a condition and click **Move Up** to move the condition processing order to a higher priority for e-mail filtering. Conditions are processed in the order in which they appear in the Conditions list.
- **Move Down.** Select a condition and click **Move Down** to move the condition processing order to a lower priority for e-mail filtering. Conditions are processed in the order in which they appear in the Conditions list.

Action

- **Action Type.** Select an action to take if a rule traps a message that meets the rule criteria:
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the **Target** box. If the mailbox does not exist, it is created. The default mailbox is "bulk". A POP3 user will see this mailbox only if he logs on to this mailbox using the format `userid- mailbox`. By default, if nothing is entered into the text box, messages meeting the rule criteria will be sent to the user's Main mailbox.
  - **Forward to Address.** Forwards the message to an e-mail address. Enter an e-mail address to forward mail to in the **Target** box. You must enter the full e-mail address, such as Mary@domain1.com.
  - **Delete.** Immediately deletes the message.
  - **Copy.** Delivers the message to its intended recipient as well as copies it to an additional address that you specify in the **Target** box.
  - **Bounce.** Sends the message back to the sender without being processed.
- **Target. Enter the name of the user's mailbox or e-mail address to** forward the message to which matches the rule condition criteria. If you enter a mailbox that does not exist, one is created. A POP3 user will see this mailbox only if he logs on to this mailbox using the format userid-mailbox. By default, if nothing is entered in the text box, messages meeting the rule criteria are sent to the user's Main mailbox.
- **Add.** Click **Add** to save changes.

- **Cancel.** Click **Cancel** to exit without saving changes.

Related Topics

Overview of Mail Delivery Rules (on page 218)

Adding a Rule Condition (on page 156)

Creating an Outbound Rule for a Domain (on page 222)

How Delivery Rules are stored and processed (on page 219)

Delivery Rule Syntax (on page 232)

Adding Multiple Conditions to Rules (on page 157)

Adding a Rule Condition

Use this pop-up dialog to create a rule condition.

Define Condition

- **Where.** Select the message field that you want to filter: **From**, **To**, **Subject**, **Sender**, **Body**, or **Header.**
- **Comparison.**
  - **Contains.** Select to have the delivery rule filter messages that have this search text.
  - **Does Not Contain.** Select to have the delivery rule filter messages that do **not** have the search text.
- **Search Text.** Enter search text that contains the text you want to search. 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", enter: jazz
  - Type search expressions and quantifiers as shown in *text patterns* (on page 235).
  - 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.
- **Match Case.** Select to search for text that matches the case of the search text. To ignore the text case, clear **Match Case.**
- **Save.** Click **Save** to add condition.
- **Cancel.** Click **Cancel** to exit without saving changes.

Related Topics

Inbound Rules for Domains (on page 220)

Overview of Mail Delivery Rules (on page 218)

Delivery Rule Syntax (on page 232)

How Delivery Rules are Stored and Processed (on page 219)

Adding Multiple Conditions for Users

You can create multiple conditions for both inbound and outbound rules. By using multiple conditions, you can often combine multiple rules into one, thus, saving time and creating a more compact rules file. Sometimes a rule with only one condition is adequate to fulfill rule filtering requirements. However, when you need to create more complex rules, you may want to use multiple conditions. For example, see *Rule with Multiple Conditions Example* (on page 226).

To add a rule with multiple conditions:

1. Follow the instructions to create a rule as described in *Setting Inbound Rules for Users* (on page 153). After adding the first rule condition, select the new rule condition.
2. Click **Add AND/OR...** This will bring a pop-up window allowing either
   - selection of the **"AND"** button, meaning **"ALL"** the rule conditions must be met for the message to be trapped.
   - or selection of the **"OR"** button, meaning **"ANY"** one of the conditions must be met for the message to be trapped.
3. Create the second condition as you did the first. Continue adding conditions until you are satisfied with the rule.
4. Follow the instructions to set the rule actions as described in the **Actions** section of *Setting Inbound Rules for Users* (on page 153). When you are finished creating the rule, click **Add** to save your changes.

Vacation Message

How to get here

Note: Vacation Message can handle all foreign characters for display in the Web Admin.

You can create a vacation message for each e-mail user account. When the vacation message is enabled, IMail Server sends an automated vacation message to each email address the user receives mail from. The vacation message is stored in the vacation.ima file in the user's IMail Server home directory.

Note: **Vacation Message** can also be enabled and disabled within the user's Web Client.

Note: Disabling the vacation message will automatically clear the "vacation.snt"

Domain Name (OHN). The current domain name used to address mail to the users on the mail domain is displayed.

User ID. Displays the selected user ID (user name) for the e-mail account.

Enable Vacation. Check box to enable or disable the Vacation Message text box. Disabling the vacation message will clear the "vacation snt" file.

Vacation Message. Text box when enabled, allows a vacation message to respond to all new mail messages received. The vacation response will only be sent once to each unique e-mail address.

Save. Click this button to save your settings.

To create a vacation message:

1. Select **Enable Vacation**.
2. In the **Vacation Message** text box, enter the reply message you want to send while the user is away. The vacation message is sent one time to each e-mail address from whom the recipient receives mail. IMail Server saves the message sender's e-mail address in a file (vacation.snt). This file provides the user with a list of users that sent e-mail while away and also keeps track of the senders so the vacation message is only sent one time to each sender.
3. Click **Save**.

Viewing Vacation Message Recipients

How to get here

The Vacation Recipients page provides a list of the e-mail addresses for those who have been sent a vacation message for the selected user. The addresses are tracked and listed under the **Email Addresses** list. The messages are tracked to prevent the vacation message from being sent multiple times to the same recipient.

Clear all. Click to clear the "vacation.snt file for those who have been sent a vacation message.

Note: Disabling the vacation message will also automatically clear the "vacation.snt"

Related Topics

Vacation Message for IMail User (on page 70)

User Properties (on page 126)

Auto Responder

How to get here

Note: Previously called **Information Manager**, was changed to match the Web Client title of Auto Responder for clarity.

The Auto Responder can automatically handle routine e-mail inquiries for common information about your company. For example, you might want to respond to general inquiries with an acknowledgment that the inquiry was received plus a promise to follow up.

Using the Auto Responder for a Single Automated Response

To use the Auto Responder, you first need to set up a special user account whose user ID is Info. This mail account does not belong to a specific user, but accepts mail addressed to `Info@yourcompany.com`. When someone sends mail to the Info account, she receives a prepared response such as:

"This is an automated response from General Sales. You will receive a personal response by e-mail from one of our staff within two business days."

Subdividing the Auto Responder Account

You can subdivide an Auto Responder account into more specific sub-areas that can automatically send more detailed information in response to inquiries.

Example:

You can have an automated response that lists products, prices, and ordering information; another automated response that describes the classes you offer the general public; and a third automated response that sends out company news.

To divide the Auto Responder account into more specialized responses, you create sub-areas of 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 account, IMail Server returns a prepared response that describes the Auto Responder account sub-areas such as:

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

The sender could then send a message to Info-sales@ipswitch.com and receive a special message related to sales or the sender could send a message to Info-classes@ipswitch.com and receive a message about classes.

There is no limit to the number of sub-areas you can use with the Auto Responder. Sub-areas take up no disk space since messages addressed to them merely activate an automated response. In other words, mail addressed to sub-areas is not stored anywhere, unless you specify that it be saved.

Related Topics

Creating an Auto Responder Account (on page 160)

Creating Auto Responses to Sub-Mailboxes (on page 161)

Viewing Auto Responder Message Recipients (on page 161)

Auto Responder Variables (on page 162)

Sending Mail to All Users Using Mailall.exe (on page 143)

Add / Edit Auto Responder Account

How to get here

Before you define the automated response on the Auto Responder page, you need to first create an Auto Responder account.

To create an Auto Responder account:

1. *Select a domain* (on page 110) and user to associate the Auto Responder settings with.
2. On the User Auto Responder page, click **Add** or click link to **Edit**.
3. In the **Mailbox** text box, enter a mailbox (inbox, sent, or joe).
4. Check **Enable Auto Responder**.
5. In the **Forwarding Address** text box, enter the e-mail address you want e-mail inquiries forwarded to after the automatic response is sent. Leave blank if forwarding is not required, this will leave all requests in the associated mailboxes.

   Should you want the message to be deleted without any forwarding. Enter as follows: "user-NUL@hostname.com.



Important:Virtual e-mail domains without IP addresses must enter the full address, as it will authenticate against the primary domain with the full domain address.

6. In the **Auto Response Message** box, enter the response message to send to mail addressed to this account. The first 80 characters entered in the Message box are used as the subject of the message, and are displayed in the subject field.
7. When mail is sent to an Auto Responder account, the sender's mail address is listed in a file with the extension .snt in the user's File Directory. To view this file, click the **Recipients List** link next to the Enable Auto Responder check box.



Note: The automatic response message is saved in a file with an .inf extension in the folder of the user's account. If you want to set up the same Auto Responder information for multiple accounts, copy the .inf file from one account directory to the directories of other accounts.

Related Topic

Creating Responses for Sub-Mailboxes (on page 161)

Auto Responder Variables (on page 162)

Viewing Auto Responder Message Recipients (on page 161)

Add Auto Responder Sub-Mailbox Responses

How to get here

After creating an Auto Responder account, sub-mailbox folders can be created to define different automated responses as described in the automated response from the "main" response.

To create responses using sub-mailboxes:

1. Select the user to associate the sub-mailboxes with in Auto Responder.
2. On the User Auto Responder page, click **Add**.
3. In the **Sub- area** text box, enter a folder name (`e.g. prod1`).

> **Note:** Enter **only** the sub-mailbox name, the sub-mail box **will not work** if the userid-submailbox (`e.g. "info-prod1")` is used.

4. Click **Enable Auto Responder**. This will enable access to the other text boxes.

   In the **Forwarding Address** text box, enter the e-mail address you want e-mail inquiries forwarded to after the automatic response is sent. Leave blank if forwarding is not required, this will leave all requests in the associated mailboxes. Should you want the message to be deleted without any forwarding. Enter as follows: "user-NUL@hostname.com.

> **Important:** Virtual e-mail domains without IP addresses must enter the full address, as it will authenticate against the primary domain with the full domain address.

5. In the **Auto Response Message** box, enter the appropriate response message for the sub-mailbox on this account. The first 80 characters entered in the Message box are used as the subject of the message, and are displayed in the subject field.
6. When mail is sent to an Auto Responder account, the sender's mail address is listed in a file with the extension .snt in the user's File Directory. To view this file, click the **Recipients List** link next to the Enable Auto Responder check box.

> **Note:** The automatic response message is saved in a file with an .inf extension in the folder of the user's account. If you want to set up the same Auto Response information for multiple accounts, copy the .inf file from one account directory to the directories of other accounts.

Viewing Auto Responder Message Recipients

How to get here

Use the Auto Responder Message Recipients page to view the e-mail addresses of those who have been sent an automated response message.

The Auto Responder message is sent one time to each e-mail address that the recipient receives mail from. IMail Server saves the message sender's e-mail address in a file with the .snt extension in the account's directory. This file provides the user with a list of users that sent e-mail and also keeps track of the senders so the message is only sent one time to each sender.

Auto Responder Variables

The Auto-response message can include parts of the sender's message.

Note: Variables in the subject of your auto-response message can not be substituted. The first line of the auto-response text is also the subject of auto-response message.

Variables are as follows:

%s	"Subject" of the infobot file (first line)
%t	Include "To:" from the header of the sender's message
%m	Include sender's message
%h	Include header of the sender's message
%b	Include body of the sender's message

Note: If delivery rules are used to filter the body of messages, with usage of %m or %b in the auto-response message could create a mail loop.

DomainKeys / DKIM

How to get here

Domain Signing Options (Selectors) (on page 164)

DomainKeys/DKIM Verification Settings (on page 171)

Add Selector Wizard (on page 179)

DomainKeys and **DomainKeys Identified Mail (DKIM)** are e-mail authentication methodologies designed to verify digitally signed e-mail on a per-domain basis. Both methods were designed for protection of e-mail identity and have assisted in the control of "spam" and "phishing". DomainKeys and DKIM use asymmetric key cryptography to

sign messages with a private key and use DNS to distribute the public key for signature verification.

DomainKeys (*RFC4870* (http://tools.ietf.org/html/rfc4870)) is a precursor to DKIM (*RFC4871* (http://tools.ietf.org/html/rfc4871)), though both are currently in use, DomainKeys is considered deprecated by DKIM.

See the following PDF for help in *Getting Started with DomainKeys / DKIM* (http://docs.ipswitch.com/_Messaging/IMailServer/v11.01/PDF/DomainKeysGSG.pdf).

DomainKeys

DomainKeys is a domain-level e-mail authentication standard that uses public/private key encryption and DNS to prove the legitimacy and contents of an e-mail message, and also verifies that the domain used in the "from" or "sender" header of a message has not been modified while in transit.

Public Key / Private Key

A public key/private key-pair is created for the sending domain. The private key is stored securely on the mail server and is used to sign all outgoing messages. The public key is stored and published in DNS as a TXT record of the domain.

When an e-mail is sent, the mail server will use the private key to digitally sign it, which is part of the message header. When the e-mail message is received, the DomainKeys signature can be verified against the public key on the domain's DNS.

For detail specifications on **DomainKeys** see *RFC4870* (http://tools.ietf.org/html/rfc4870).

DKIM

DKIM is very similar in functionality to DomainKeys, with an enhanced standard that provides more flexibility and security. Although DKIM does not filter or identify spam, widespread use of DKIM can prevent spammers from forging the source address of their messages. If spammers are forced to show a correct source domain, then the other spam filtering techniques will work more effectively.

Some of the improvements provided by DKIM are as follows:

- Multiple hashing algorithms (as opposed to just one available with DomainKeys).
- Capability for one DNS text record to handle multiple domains.
- Improved option for canonicalization that validates header and body separately.
- Capability to delegate signing to third parties.
- Capability to self-sign additional headers.
- More advanced options for customization using DKIM. (e.g. Hash Algorithms, Body Settings, Expiration)

For detail specifications on **DKIM** see *RFC4871* (http://tools.ietf.org/html/rfc4871).

Related Topics

System Signing Options (Selectors) (on page 83)

Domain Selector List (Signatures)

How to get here

Selectors allow a domain to have one DomainKeys selector and one DKIM selector enabled at one time. Multiple selectors are allowed in a domain to give the IMail Administrator capability to easily change from one public-key in DNS to another.

Important: Only **one DomainKey selector** and **one DKIM selector** can be enabled at **one time for a domain**. **Example:** A DKIM selector "selector1" is enabled for domain1.com. The IMail Administrator decides to enable "selector2" for domain1.com. "selector1" will automatically be disabled for domain1.com.

Important: After updating or creating a selector be sure to restart your **SMTP and Queue Manager services**.

Domain Signatures (Selector)

Search Box. Typing will automatically begin narrowing the list. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

Note: Column Titles when clicked will sort the list for the current session only. Refreshing the page will reset the original sort.

- **Default Selector**. Hyperlink that allows the IMail Administrator to designate the default selector to be used for signing, should there be one selector set on a domain.

Note: Only one **DomainKeys selector** and one **DKIM selector** can be set as default at one time.

Selector List

- **Name**. Name used to identify selector.
- **DNS Text Record**. Name used to identify the selector in DNS. This text name allows any text string that is a legal DNS domain name.

Example: DNS Text Record set to MyDNSName will be named "MyDNSName_domainkey.domainname.com"

- **Status**. Selector status indicating active and on, or off.
- **Type**. E-mail authentication type to verify the DNS domain of an E-mail sender and the message integrity.
  - **DomainKeys**. DomainKeys uses the Message Algorithm as the specified canonicalization method.
  - **DKIM**. (DomainKeys Identified Mail) is an enhanced protocol of DomainKeys, using public-key cryptography and key server technology to verify the source and contents of e-mail. DKIM uses the Header and Body Algorithm as the specified canonicalization method.
- **Enabled**. Displays the selectors that are active for the selected domain. Click to "activate / de-activate" the selector domain status.

Note: Only one DomainKey and one DKIM selector can be enabled per domain.

Add New (on page 165). Click to add a new selector. This will give the following two options

- **Wizard**. Run this option for Administrators that are new to DomainKeys.
- **Advanced** (on page 165). Click this option for Administrators that are familiar with all DomainKey options.

Add Existing (on page 170). Click to add a **System Selector** to the domain.

Remove. Click this after selecting item(s) from the list to remove from the Domain Selector List.

Note: This will not delete from the **System Selector List**.

Related Topics

System Signing Options (Selectors) (on page 83)

Domain Selector Add / Edit (on page 165)

Domain Selector Add / Edit

How to get here

Important: After updating or creating a selector be sure to **restart** your **SMTP and Queue Manager services**.

Selector Signing Properties

- **Type**.
  - **DomainKeys**. Uses Message Algorithm for Preparation Signing.
  - **DKIM**. Uses Header and Body Algorithm for Preparation Signing.
- **Name**. Value used to identify the selector in the IMail Administrator.
- **DNS Text Record**. Name that will associate the selector in DNS. This text name allows any text string that is a legal DNS domain name.

Example: DNS Text Record set to MyDNSName will be named `"MyDNSName_domainkey.domainname.com"`

- **Status**. (On by default) Click "Off" to disable the selector.
- **Description**. Free format text box limited to 1024 characters.
- **Header Algorithm (DKIM only)**. DKIM uses both the Header and Body Algorithm as the specified canonicalization method.
  - **Simple**. This algorithm is designed to be the least tolerant. Each header is unfolded per RFC2822 and is converted to lowercase.
  - **Relaxed**. (Set by default) This algorithm tolerates common modifications such as white-space replacement and header line re-wrapping.
- **Body Algorithm (DKIM only)**.
  - **Simple**. This algorithm is designed to be the least tolerant.
  - **Relaxed**. (Set by default) This algorithm tolerates common modifications such as white-space replacement and header line re-wrapping.
- **Message Algorithm (DomainKeys only).** DomainKeys uses the Message Algorithm as the specified canonicalization method.
  - **Simple**. Allows toleration of almost no modification.
  - **No Folding Whitespace (nofws)**. (Set by Default) Allows common modifications such as white-space replacement and header line re-wrapping.
- **Public Key**. The public key which is automatically generated is what must be stored and published in DNS as a TXT record of the associated domain.

Tip: Remember to check for the "p=" in front of the key

Advanced Properties

DomainKeys and DKIM Option

Private Key. Text box displaying text string of Private Key. The private key is stored securely on the mail server and is used to sign all outgoing messages.

- **Generate New Key**. (Default is 1024 Kb) Clicking this button will generate a new **Private Key**, with a pop-up option for the private key length (512, 768, 1024, 1536, 2048).

DKIM Advanced Options Only

Hash Algorithm. SHA (Secure Hash Algorithm) hash functions are a set of cryptographic hash functions designed by the NSA and published by the NIST as a US Federal Information Processing Standard.

- **SHA-256**. (Set by default) Is an improved hash function in the SHA-2 family, computed with 32-bit words.
- **SHA-1**. The best established of the existing SHA hash functions, and is employed in several widely used security applications and protocols.

Body Settings. Options for body length limits when signing.

- **Sign Entire Body**. (Set by default)
- **Sign Entire Body and Include Length Tag**. Including the length tag allows message trailers to be better tolerated after the message is sent.
- **Specify Max Body Length for Signing**. Textbox for max amount of bytes to sign.

Expiration. When both the Timestamp and Expiration Tag are set, then a validation check will be done to verify that the Expiration Tag is greater than the Timestamp when the signature is verified.

- **Include Timestamp**. (Set by Default) This tag tells the verifying server when the signature was generated.
- **Include Expiration Tag**. (Optional) When used, this tag tells the verifying server to ignore this signature after the time specified.
  - **Time in Which to Expire**. Time is counted by minutes, hours or days. The expiration time will be calculated based on the time when the signature is generated.

Authoritative Domain.

- **Use the Domain's Auth Name**. (Set by default) This option requires a DNS text record for each domain signature selector.
- **Use the Sending User's Domain Name**. This option requires a DNS text record for each domain signature selector.
- **Use the Following Auth Name**. (Set by default for DKIM Wizard) This option allows the administrator to create one DNS text record to handle many domains.

Assigning Domains

Domains can easily be assigned to a selector, allowing the domain to use as a signature.

Available Domains not Assigned

The left box displays all available domains that do not have the selector assigned.

- **Domain Name**. Domain name that currently does not have the current selector assigned.

   **(Add Domain to Selector)**. Select an available domain and click to add to the current selector.

   **(Remove Domain from Selector)**. Select a domain from the domains currently assigned and click to remove the current selector.

   **(Add All Domains to Selector)**. Click to add all available domains to the current selector.

   **(Remove All Domains From Selector)**. Click to remove all domains from the current selector.

Assigned Domains for Current Selector

- **Domain Name**. Domain name that has the current selected assigned.
- **Enabled.** Check this box to activate and allow the domain to use the selector.

Enable All. Click this button to activate all the assigned selectors.

Disable All. Click this button to deactivate all the assigned selectors. The selector will be assigned to all the domains, but the selector will be disabled for use as a domain signature.

Test DNS Setup. Click this button to test the current selector against your current DNS setup. The DNS Test button will display **"successful"** for each domain. A link to assist with DNS problems will display for domains that **"failed".**

- See the following KB for DNS help **-** *http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=727* (http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=727)

Headers List

- **Sign All Headers**. (**Not** set by default) See all Headers.

 **Sign All Headers** when setting Prevent Adding for a signature will be unchecked, unless the header list is specified otherwise.

 **Warning**: Disabling the default set of headers to be signed opens the possibility of header modifications and spoofing depending on the headers that are being signed.

DomainKeys / DKIM Headers

By default (RFC minimum recommendation) the following headers are set for signing:

- CC
- Content-Description
- Content-ID
- Content-Transfer-Encoding
- Content-Type, Date
- From, In-Reply-To
- List-Archive
- List-Help
- List-ID
- List-Owner
- List-Post
- List-Subscribe
- List-Unsubscribe
- Message-ID
- MIME-Version
- References
- Reply-To
- Resent-CC
- Resent-Date
- Resent-From
- Resent-Message-ID
- Resent-Sender
- Resent-To
- Sender, Subject
- To



TIP: The default headers are recommended as the **minimum** headers necessary for maintaining secure header signing.

DomainKeys Header List

- **Name**. Header name selected to be signed.

DKIM Header List

- **Name**. Header name selected to be signed.
- **Maximum Number To Sign**. (Default set to 1) Maximum number of same headers allowed to be signed.

- **Sign All**. (True by Default) Signatures will sign all headers with the same headers for the domain.



Tip: **Max Number to Sign** and **Sign All** are not available for update when the **"Sign All"** check box is set.

- **Prevent Adding**. (False by Default) A signature will not tolerate headers with the same header name to be added.

Add Header. Click the **Add** button to create a custom header or select a header from the drop down for a list of all headers.

Edit Header. (DKIM functionality only) Select a header and click the Edit button to update the header options.

Delete Header. Select a header and click the Delete button to remove.



Note: To maintain a secure header signing, it is not recommended to remove a default header.

Add. Click **Add** to for a new Header.

Edit. Select a Header and click **Edit** to update.

Delete. Select a Header then click **Delete** to remove.

Related Topics

About DomainKeys / DKIM (on page 82)

System Selector List (Signatures) (on page 83)

Domain Selector List (Signatures) (on page 164)

Existing System Selectors

How to get here

Existing System Signing Options (Selectors) will display all the current System Selectors that exist. This list can also be viewable in the IMail Administration at **System > DomainKeys / DKIM**.



Important: After updating or creating a selector be sure to **restart** your **SMTP and Queue Manager services**.

Search Box. Typing will automatically begin narrowing the list. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

Note: Column Titles when clicked will sort the list for the current session only. Refreshing the page will reset the original sort.

Selector List

- **Name**. Name used to identify selector.
- **DNS Text Record**. Name used to identify the selector in DNS. This text name allows any text string that is a legal DNS domain name.

Example: DNS Text Record set to MyDNSName will be named `"MyDNSName_domainkey.domainname.com"`

- **Domains**. Domain names that are assigned to selector.
- **Type**. E-mail authentication type to verify the DNS domain of an E-mail sender and the message integrity.
  - **DomainKeys**. DomainKeys uses the Message Algorithm as the specified canonicalization method.
  - **DKIM**. (DomainKeys Identified Mail) is an enhanced protocol of DomainKeys, using public-key cryptography and key server technology to verify the source and contents of e-mail. DKIM uses the Header and Body Algorithm as the specified canonicalization method.

Add. Select and click **Add** to copy the existing system selector to the domain.

Cancel. Click **Cancel** to exit without adding.

Related Topics

About DomainKeys / DKIM (on page 82)

System Signing Options (Selectors) (on page 83)

Domain Selector List (Signatures) (on page 164)

DomainKeys / DKIM Verification Settings

How to get here

The **DomainKeys Verification Settings** page provides administrators increased capability to stop incoming e-mail identified as spam by signature errors. Use the DomainKeys Verification settings to configure how to process e-mail that is identified as

spoofed e-mail. Settings on the DomainKeys Verification Settings page apply to the selected domain.

Important: DomainKeys / DKIM Signature Verification will **not** be processed when an address exists in the **"Relay Mail for Addresses (on page 392)"**.

Default actions are specified for each message. You can, however, change the defaults by clicking the hyperlink under Verification Category. A pop-up appears, with the options to change the **Action To Be Taken**.

Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

Enable DKIM. Select this check box to enable the DKIM Verification Settings for the current host.

Enable DomainKeys. Select this check box to enable DomainKeys Verification for the current host.

Total Number of Signatures to Check Per Message. Default set to 5. This is a maximum number of signatures that will be checked and validated for a message. *Examples* (on page 178).

Verification Settings

- **Verification Category.** This lists all possible verification categories for this domain.
  - *No Signature* (on page 173)
  - *Invalid Signature* (on page 173)
  - *DNS Unreachable* (on page 174)
  - *Invalid DNS Selector* (on page 175)
  - *Verification Failed* (on page 176)
  - *Pass* (on page 177)
- **Action to be taken.** This column lists the action chosen for each corresponding query result.
- **Target.** This column lists the mailbox or e-mail address for a Move to or Forward to action, respectively.
- **Prefix Subject.** (Yes/No) This column lists whether or not the message will have a DomainKeys Result prefix added to the message.
- **With.** This column lists the actual prefix, if chosen, for the corresponding query result.

Save. Click the button to save your changes.

Related Topics

About DomainKeys / DKIM (on page 82)

Domain Selector List (Signatures) (on page 164)

System Signing Options (Selectors) (on page 83)

DomainKey Result - No Signature

The **DomainKeys Verification** Category of **No Signature** page allows you to choose an action when the DomainKeys Verification filter is enabled.

This action activates when the message does not have a signature (Selector).



Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

The action to be taken when the query result is met

- **Action.** Select one of the following actions:
  - **None.** No action is performed**.**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
  - **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was identified with No Signature for DomainKeys.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the DomainKeys options are setup to best suit your filtering requirements.

  - **Reject Connection**. Immediately ends the message connection, and message will not be accepted.
- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as DomainKeys failure, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 178) is entered in the text box to the right and is based on the DomainKeys failure. You can also enter a custom message in this box.

DomainKey Result - Invalid Signature

The **DomainKeys Verification** Category of **Invalid Signature** page allows you to choose an action when the DomainKeys Verification filter is enabled.

This action activates when the message has an invalid signature (Selector).

Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

The action to be taken when the query result is met

- **Action.** Select one of the following actions:
  - **None.** No action is performed**.**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
  - **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was identified with Invalid Signature for DomainKeys.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.

Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the DomainKeys options are setup to best suit your filtering requirements.

  - **Reject Connection**. Immediately ends the message connection, and message will not be accepted.
- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as DomainKeys failure, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 178) is entered in the text box to the right and is based on the DomainKeys failure. You can also enter a custom message in this box.

DomainKeys Result - DNS Unreachable

The **DomainKeys Verification** Category of **DNS Unreachable** page allows you to choose an action when the DomainKeys Verification filter is enabled.

This action activates when the message has an unreachable DNS.

Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

The action to be taken when the query result is met

- **Action.** Select one of the following actions:
  - **None.** No action is performed**.**

- **Delete.** Immediately deletes the message.
- **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
- **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was identified with Invalid Signature for DomainKeys.
- **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the DomainKeys options are setup to best suit your filtering requirements.

- **Reject Connection**. Immediately ends the message connection, and message will not be accepted.

- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as DomainKeys failure, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 178) is entered in the text box to the right and is based on the DomainKeys failure. You can also enter a custom message in this box.

DomainKey Result - Invalid DNS Selector

The **DomainKeys Verification** Category of **Invalid DNS Selector** page allows you to choose an action when the DomainKeys Verification filter is enabled.

This action activates when the message has an invalid DNS selector.



Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

The action to be taken when the query result is met

- **Action.** Select one of the following actions:
  - **None.** No action is performed**.**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
  - **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was identified with Invalid Signature for DomainKeys.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.

Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the DomainKeys options are setup to best suit your filtering requirements.

- **Reject Connection**. Immediately ends the message connection, and message will not be accepted.

- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as DomainKeys failure, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 178) is entered in the text box to the right and is based on the DomainKeys failure. You can also enter a custom message in this box.

DomainKey Result - Verification Failed

The **DomainKeys Verification** Category of **Verification Failed** page allows you to choose an action when the DomainKeys Verification filter is enabled.

This action activates when the message has a failed verification.

Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

The action to be taken when the query result is met

- **Action.** Select one of the following actions:
  - **None.** No action is performed**.**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
  - **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was identified with Invalid Signature for DomainKeys.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.

Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the DomainKeys options are setup to best suit your filtering requirements.

- **Reject Connection**. Immediately ends the message connection, and message will not be accepted.

- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as DomainKeys failure, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 178) is entered in the text box to the right and is based on the DomainKeys failure. You can also enter a custom message in this box.

DomainKey Result - Pass

The **DomainKeys Verification** Category of **Pass** page allows you to choose an action when the DomainKeys Verification filter is enabled.

This action activates when the message is passed.



Important: After updating verification settings be sure to **restart** your **SMTP** and **Queue Manager services**.

The action to be taken when the query result is met

- **Action.** Select one of the following actions:
  - **None.** No action is performed**.**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option.
  - **Insert X- Header (default).** Inserts an X-Header into the message indicating that the message was identified with Invalid Signature for DomainKeys.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the DomainKeys options are setup to best suit your filtering requirements.

  - **Reject Connection**. Immediately ends the message connection, and message will not be accepted.
- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as DomainKeys failure, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 178) is entered in the text box to the right and is based on the DomainKeys failure. You can also enter a custom message in this box.

DomainKeys Default Subject Values

A prefix value, based on the DomainKeys / DKIM return code, is added to the message. The default values are when DomainKeys / DKIM Verification checkbox is enabled:

- **No Signature**. Inserts X-Header with [X-IMail-DomainKeys-Fail] in subject.
- **Invalid Signature**. Inserts X-Header with [X-IMail-DomainKeys-Softfail] in subject.
- **DNS Unreachable**. Inserts X-Header with [X-IMail-DomainKeys-Error] in subject.
- **Invalid DNS Selector**. By default no action taken.
- **Verification Failed**. By default no action taken.
- **None.** By default no action taken.
- **Pass.** By default no action taken.

This subject field is also user configurable for each possible return code.

Example - Total Number Signatures / Message

An incoming message with 5 signatures:

Signature 1: DomainKeys Signature

Signature 2: DKIM Signature

Signature 3: DKIM Signature

Signature 4: DomainKeys Signature

Signature 5: DKIM Signature

Example 1:

- Total Number of Signatures set to "5" and only DKIM enabled.
- Signature 2, 3 & 5 will be checked. Signature 1 & 4 will be ignored.

Example 2:

- Total Number of Signatures set to "2" and only DomainKeys enabled.
- Signature 1 & 4 will be checked. Signature 2, 3 & 5 will be ignored.

Example 3:

- Total Number of Signatures set to "2" and both DomainKeys and DKIM are enabled.
- Signature 1 & 2 will be checked. Signature 3, 4 & 5 will be ignored.

Example 4:

- Total Number of Signatures set to "4" and both DomainKeys and DKIM are enabled.
- Signature 1, 2, 3 & 4 will be checked. Signature 5 will be ignored.

Example 5:

- Total Number of Signatures set to "5" and only DKIM enabled.
- Signature 2, 3 & 5 will be checked. Signature 1 & 4 will be ignored.

DomainKeys / DKIM Wizard

How to get here

The **DomainKeys / DKIM Wizard** was designed to allow and IMail Administrator to quickly setup the necessary items for DomainKeys / DKIM.

Step 1

DomainKeys or DKIM

DomainKeys and DKIM allow messages to be cryptographically signed, which allows receiving servers to verify the source and contents of messages. Both specifications are similar, however, DKIM handles e-mail routing better than DomainKeys and is considered to be the preferred method of signing messages.

- Choose the selector type:
  - **DomainKeys**. Uses Message Algorithm for Preparation Signing.
  - **DKIM**. Uses Header and Body Algorithm for Preparation Signing.
- Requires a selector **Name** to allow identification within the IMail Administration.
- Enter the **DNS Text Record** that will associate the selector in DNS. This text name allows any text string that is a legal DNS domain name.



Example: DNS Text Record set to MyDNSName will be named `"MyDNSName_domainkey.domainname.com"`

- **Description** is optional and is limited to 1024 characters.

Step 2

Choosing your **Algorithm**:

The simple and relaxed header and body algorithms prepare the e-mail before signing occurs. This is known as canonicalization and does not affect the message that is actually sent in any way. These algorithms attempt to handle cases where normal transformations that occur to a message as it is sent will cause a signature to be verified incorrectly. The 'simple' Canonicalization algorithm tolerates almost no modification of the message, while the 'relaxed' canonicalization algorithm allows some typical transformations to occur without breaking the signature (such as modifying whitespace and folding whitespace in the message and its headers). The relaxed canonicalization algorithm is recommended unless it is critical that a message not be modified in any way during transit to a receiving mail server.

- **Header Algorithm (DKIM only)**. DKIM uses both the Header and Body Algorithm as the specified canonicalization method.
  - **Simple**. This algorithm is designed to be the least tolerant. Each header is unfolded per RFC2822 and is converted to lowercase.

  - **Relaxed**. (Set by default) This algorithm tolerates common modifications such as white-space replacement and header line re-wrapping.
- **Body Algorithm (DKIM only)**.
  - **Simple**. This algorithm is designed to be the least tolerant.
  - **Relaxed**. (Set by default) This algorithm tolerates common modifications such as white-space replacement and header line re-wrapping.
- **Message Algorithm (DomainKeys only).** DomainKeys uses the Message Algorithm as the specified canonicalization method.
  - **Simple**. Allows toleration of almost no modification.
  - **No Folding Whitespace (nofws)**. (Set by Default) Allows common modifications such as white-space replacement and header line re-wrapping.

Step 3

Assigning Domains

Please choose which domains are allowed to use this selector for signing. Domains added to the list on the right are able to use this selector for its users.

- By default, when run at the domain level, only the selected domain be selected, otherwise it will be up to the IMail Administrator to select which domains will be assigned.
- This step gives you the capability to also add any existing domains to the selector. Any domains that are in the "Available Domains" box can be assigned the new selector being created.



Note: The selector will not be enabled until the DNS Test is valid. Should the DNS Test fail, all domains set for this selector will be disabled. It will be up to the IMail Administrator to enable the selectors after the DNS has been corrected.

Step 4 (DKIM Selectors Only)

One or Multiple DNS Text Records

This step will only appear when creating a **DKIM selector** and multiple domains have been assigned to the selector. DKIM has the capability to have all domains point to one specified domain for the DNS record. This is the simplest and recommended way of setting up DKIM. If you wish, however, you can choose to enter a DNS record for every domain by selecting the second option in the drop down list.

- By default this feature is selected. Should you want to create a DNS record for each domain, select the second option "All domains use their own DNS records.



Note: DomainKeys is not as flexible as DKIM and requires a DNS text record for each domain, per the RFC.

Step 5

Private Key and DNS Text Record

- This page has generated a private key that must be inserted into the DNS text record that is identified under the text box.



Example: `DnsTextRecord_domainkey.domain.name.com`

- Generate a matching DNS text record for each item listed on the wizard page.

If you do not have access to your DNS records, contact your DNS administrator to add these records. Please note, that it is recommended that you continue to the next screen and save this selector if the process of adding the DNS records will take more than a few minutes.



Tip: Remember to check for the "p=" in front of the key

Step 6

DNS Test and Selector Status

- At this point the DNS text record must exist to be tested for validity. If the DNS record has not yet been created, it is recommended to click **"Done"** to save the selector.



Warning: Click **"Done"** now, as the IMail Server will eventually **time out** and your selector will be lost.

- Also, if the DNS text record has not been created, it is recommended to disable the selector.
- After the DNS text record has been created, it can be tested by editing the selector. The **DNS Test** button is located under the Domains list using the new selector.
- The DNS Test button will display **"successful"** for each domain. A link to assist with DNS problems will display for domains that **"failed".**
- See the following KB for DNS help **-** *http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=72* (http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=727)



Important: After creating a selector be sure to restart your **SMTP and Queue Manager services**.

Related Topics

About DomainKeys / DKIM (on page 82)

Domain Selector List (Signatures) (on page 164)

System Signing Options (Selectors) (on page 83)

Spam Filtering (Domain Level)

How to get here

Use the Domain Level Antispam settings to enable, change, and disable various antispam filters for the selected domain.

- **Premium Filter (on page 280).** (optional only with IMail Premium). Provides fully automated spam protection in addition to the Standard Antispam filter included with all IMail products.
- **Statistical Filter (on page 283).** Examines each word in the body of an e-mail message to determine if the e-mail is spam.
- **Phrase Filter** (on page 288). Searches for spam phrases within the body of e-mail messages and identifies the messages that are spam.
- **HTML Features Filter (on page 291).** Searches HTML features in messages that are subject to spam. Sets how many HTML features must be present in an .htm file in order for a message to be identified as spam and the spam action to take.
- **URL Domain Black List (on page 299).** Searches for domain names that appear as URL links in messages, and lets you set the action to take on such messages.
- **Broken MIME Headers (on page 301).** Uses the Broken MIME Header Filter to identify MIME Header characteristics that result in SPAM e-mail.



Note: Content filtering (on page 303) for authenticated users can be enabled or disabled for all the antispam filters listed above on the domain properties page of an IP'ed domain.

- **SPF[3][4] (Sender Policy Framework).** Enables stronger authentication of e-mail senders using Sender Policy Framework (an extension to the DNS system). Provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.
- **Connection Checks (on page 274).** Verifies that the party connecting to your server is not part of a black list.
- **Logging** (on page 317). Controls where the standard antispam logs are written as well as how much detail is provided in them.

Alias Administration

How to get here

An e-mail alias is an alternative for a user's e-mail address, a group of user's e-mail addresses, or an application that performs additional e-mail functions. An e-mail alias looks like an e-mail address, but it is a name defined within an e-mail domain to represent a logon name. Therefore more than one e-mail alias may refer to a POP3 account. IMail Server supports the following alias types:

- *Standard alias* (on page 186)
- *Group alias* (on page 186)
- *Program alias* (on page 188)
- *Domain alias* (on page 186)

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. IMail Server automatically sets up the postmaster alias to point to the `root` account. You can change the postmaster alias to point to a different mail account.

---

[3] How to get here IMail uses Sender Policy Framework (SPF) to extend the Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) so IMail Server does not accept e-mail unless the sending computer is designated as a legitimate e-mail sender. This feature provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.To accomplish this e-mail security measure, SPF establishes a policy framework and a sender authentication scheme that verifies ...

[4] The Sender Policy Framework (SPF) pageprovides administrators increased capability to stop incoming email from forged (spoofed) email addresses. Use the SPF settings to configure how to process email that is identified as forged email. Settings on the SPF page apply to the selected domain.Enable SPF. Select this checkbox to enable the SPF filter for the current host. Default actions are specified to take for each SPF query result. You can, however, change the defaults by clicking the hyperlink u ...

You can create aliases one at a time in the IMail Administrator or you can add a batch of aliases at one time. For more information about adding aliases with a batch file, see *Adding an Alias (addalias.exe)* (on page 188). If you plan to add a group alias, you can prepare a 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 plan 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.)



Note: 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.

Aliases display as follows:

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Search. Requires entering a minimum of two characters, and the search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered. Search target includes both the "Username" and "Full Name" columns as criteria for search selection.



Caution: Search requires a minimum of two characters for the search process to begin.



Note: Column Titles when clicked will sort the user list for the current session only. Refreshing the page will reset to Username sorting. **Example.** Clicking on the "Disabled" column heading twice will sort all the disabled users to the top of the page.**Search** box. Enter an alias name that you want to search for in the list of available aliases, then click **Search**.

Alias List

- **Name** list. Click an alias name to modify an alias. Click ▲ or ▼ to sort the list.



Note: You cannot change the alias type; for example, you cannot change a Standard alias to a Group alias. If you want to use an existing alias name for another type of alias, delete the existing alias and create a new alias of the desired type. The exception to this rule is that a standard alias will automatically be converted to a Group alias if more than five users are added to it.

- **Type.** This column lists the type of alias: program, group, standard, beeper, or pager.
- **Resolves To.** This column lists the originating program, group, or standard, beeper, or pager for which the alias was created.

Add. Click **Add** to create a new alias name on IMail Server. For more information, see *Adding an Email Alias* (on page 185).

Edit. To edit an aliases, first select, then click Edit.

Delete. Select an alias that you want to delete from the Alias name list, then click **Delete** to delete the alias.

Related Topics

Adding an E-mail Alias (on page 185)

Adding an Alias using Addalias.exe (on page 188)

Add / Edit E-mail Alias

How to get here

Step 1: Enter **Alias Name**, select **Alias Type**, then click **Save.**

Type list:

- *Standard Alias* (on page 186)
  - **Alias Name.** Displays the name of the new alias. Aliases 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 the mail domain .
  - **Type.** Drop down menu displaying the alias type.
  - **Resolves To**. Place one complete mail address per line (no spaces). Enter an e-mail address on each line (for example, userid@domain.com).
  - **Important:** If you enter more than four e-mail addresses, the standard alias is converted to a group alias.
- *Group Alias* (on page 186)
  - **Alias Name.** Displays the name for the new alias. Aliases 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 the mail domain.
  - **Type.** Drop down menu displaying the alias type.
  - **Resolves To.** Enter an e-mail address per line (no spaces). Enter an e-mail address on each line (for example, userid@domain.com).
- *Program Alias* (on page 188)
  - **Alias Name.** Displays the name for the new alias. Aliases 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 the mail domain.
  - **Type.** Drop down menu displaying the alias type.

- **Resolves To**. Enter the program path, filename, and other required command line parameters to be executed when the program alias receives mail. 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 the program to take specified actions on the e-mail.



Tip: Beeper and Pager functionality have been removed from the Web Administration, but can still be accessed using the **Console Administration**.

Related Topics

Learning About Aliases (on page 183)

Creating "nobody" Alias (on page 187)

About Standard Aliases

A standard alias is a name that indicates a single user ID on the same mail server. Mail is sent to:

- Up to four user IDs on the same system.
- Up to four remote mail addresses.
- Another alias.
- Any combination of the above



Important: If you create a standard alias that includes more than four entries, the standard alias is converted to a group alias.

Related Topic

Creating "nobody" Alias (on page 187)

About Domain Aliases

How to get here

A domain alias is another name for a mail host. It can be entered only in the **Domain Aliases** box located on the Domain Properties page.

About Group Aliases

A group alias is a user ID that causes any mail sent to it to go to all the valid mail addresses listed in the group.

If more than four addresses are added to a standard alias, IMail automatically changes the standard alias to a group alias.

Note: We recommend that a group alias be used for less than 50 users. For over 50 users it is recommended that a list be set up instead.

Creating "nobody" Alias

The **"nobody" alias** is a catch-all alias which receives messages from users that do not exist on your host, and forwards the message to the address specified in the "nobody" alias.

Note: "nobody" alias will prevent messages from bouncing back to the sender.

To create a "nobody" alias simply follow instructions for **adding a standard alias** (on page 185), with the standard alias name being **"nobody"**.

Example:

If I have a **standard** "nobody" **alias** pointing to `"unknown@mydomain.com"` and a message with an invalid address to `"gone@mydomain.com"` arrives, the message is forwarded to the `unknown@mydomain.com` mailbox.

This can be useful when a company wants to be sure that all messages are received and answered.

Related Topic

Creating an Email Alias (on page 185)

Allow remote mail to local groups

How to get here

When selected, the SMTP server will accept mail addressed to private group aliases created only with the IMail Client application.

Note: List-server mailing lists are not affected by this setting. Aliases of type Group are affected. You must have "Allow remote mail to local groups" option enabled for a Group alias to work.

Related Topics

SMTP Settings (on page 392)

About Program Alias

A program alias is a user ID that causes any mail sent to it to start a program that can accept the mail message for further processing. The alias consists of a path and executable file name, plus any required command line parameters.

When e-mail is sent to the program alias, the executable program is invoked and the entire content of the e-mail message is passed to the executable program (as a `.tmp` file).

Adding Aliases using "addalias.exe" Utility

Addalias.exe is a utility for adding, modifying, and deleting batches of e-mail aliases stored in a text file. You can also import an existing Windows NT group into IMail and create a group alias. If you invoke Addalias.exe with no command line options (by entering only `addalias` at the MS-DOS prompt), you can manually input command lines, then press **Enter** after each line. Make sure that you press **CTRL-Z** to exit the utility when you are done. *Example* (on page 191)

Basic Command Syntax

```
addalias [-h hostname] [-cX] [-{a|d|m}] alias [=destination]
```

Command	Function
-a aliasname	Adds an alias if the alias does not exist. aliasname is the name of the alias you want to add. Only one alias may be added in a single command line.
-cX	Specifies an alternate delimiting character, which replaces the default delimiter (the equal sign). Spaces are not allowed. (Using -c in a text file affects all lines in the file.)
-d aliasname	Deletes 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	Specifies the virtual domain for the alias. The primary domain is used if no e-mail domain is specified. (Using -h in a text file affects all lines in the file.)
-i groupname	Imports an NT group as a group alias if the alias does not already exist. groupname is the group that you want to import. Only one alias can be added in a single command line.
-l	Lists current aliases. This argument may not be used in a text file.
-m aliasname	Modifies or adds an alias even if the alias exists. aliasname is the alias you want to modify. Only one alias may be modified in

	a single command line.
-?	Displays a summary of argument options.

Important: Windows 2000 and Advanced Server Users. You can import NT groups as an alias only for local and global groups. You cannot import NT groups with Microsoft Active Directory Services (ADS) Universal groups.

Addalias.exe Examples

Adding an Alias to the Default (primary) E-mail Domain (on page 189)

Adding an Alias to a Specific Domain (on page 189)

Deleting an Alias (on page 190)

Importing an NT Group as a Group Alias (on page 420)

Return codes

Addalias.exe 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 IMail Server from another mail system if the other mail server program can create a delimited text file of aliases. *Example* (on page 191)

Adding Alias to a Domain Using "addalias.exe"

Adding an Alias to a Specific Domain Using the addaliase.exe Utility

The following example adds an alias of newalias to the e-mail domain named `secondhost.com` and resolves to e-mail:

```
addalias -h secondhost.com -a newalias e-mail
```

Adding Alias to Primary Domain Using "addalias.exe"

The following examples add an alias of newalias to the default (primary) e-mail domain which resolves to e-mail:

```
addalias -c: -a newalias:email

addalias -a newalias=email

addalias -c: newalias:email

addalias newalias=email
```

```
addalias newalias email
```

Deleting an Alias using "addalias.exe" Utility

The following examples delete an alias:

```
addalias -d oldalias

addalias -h another.net -d alias1
```

Related Topics

Adding an Alias using Addalias.exe (on page 188)

Using a Text File (adduser.exe)

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 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 wks013.augusta.ipswitch.com -f addfour.txt
```

You then get the following messages:

```
current host is wks013.augusta.ipswitch.com

OK: added userid to host wks013.augusta.ipswitch.com

OK: added smith to host wks013.augusta.ipswitch.com
```

```
OK: added test1 to host wks013.augusta.ipswitch.com

OK: added jones to host wks013.augusta.ipswitch.com
```

Note that the user named test1 will have "password" (the default) as his password.

Example File (on page 425)

Addalias Text File Example

Addalias.exe Text File Example

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, enter:

addalias < test.txt

The < symbol tells addalias to use test.txt as output.

You then get the following messages:

```
current host is wks003.augusta.ipswitch.com

added [wks003.augusta.ipswitch.com ] test1 -> me

added [wks003.augusta.ipswitch.com ] test2 -> test1

added [wks003.augusta.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
```

List Administration

How to get here

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

The list server can also *archive messages and send them periodically* (on page 210) as a single message or "digest."

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Search Box. Requires entering a minimum of two characters, and the search will automatically begin narrowing the mailing list names. The search assumes a wildcard automatically after the characters entered.



Caution: Search requires a minimum of two characters for the search to process to begin.

- **List Name.** Click a list name to modify a list. Click ▲ or ▼ to sort the list.
- **List Owner**. Assigned *list owner* (on page 216).
- **List Administrator**. Assigned *List Administrator* (on page 216).

Add. Click **Add** to create a new list on IMail Server. For more information, see *Adding an E-mail List* (on page 196).

Edit. Select and highlight a list, then click **Edit** to update an existing list. See General List Options.

Delete. Select a list that you want to delete from the List list, then click **Delete** to delete the list.

If the List Server has multiple pages, use the page navigation control which appears below the list names.

Default List Settings

- **List Owner's E-mail Address.** Enter the full e-mail address of the list default list owner. This is the mail account that receives all messages (such as Subscribe and Unsubscribe requests) to the list. It is also the account from which help messages are sent and to which error messages are sent.

Note: The List Owner e-mail address does not have access to the List Administration pages unless the e-mail address is same as the local list administrator or has List Administrator permissions for the local domain. See the *User Properties* (on page 126) page.

- **Administrator's Local User ID.** Enter the default list administrator user ID. Enter only a User ID (do not add the full e-mail address) that resides on the local domain for the list administrator. This will allow *local list administration* (on page 216) permissions for only the specified list.

Important: To allow permissions for all lists, the User ID can be given List Administrator rights See the *User Properties* (on page 126) page.

Note: The list administrator and list owner are usually the same person, but a "dummy" user account can be set up to be the list owner in order to hide the identity of the list administrator or to give the impression of more people being involved in the list management.

- **Maximum Message Size (bytes).** Enter the maximum size 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.** Enter the number of recipients each SMTP process will send to. To calculate this number, divide the expected number of subscribers by 25. The result is the number of recipients per message.

Note: We recommend that no more than 25 processes be used by a list.

Example:

You want to send an e-mail to a list of 5,000 subscribers. Divide 5,000 (number of subscribers) by 25 (number of processes) and the result is 200 (recipients per message). So you would have 25 processes that each handle 200 recipients.

If you increase this number, you may need to also increase the number of SMTP processes. For more information about how to change the default number of SMTP processes for IMail Server, see *SMTP Settings Advanced Options* (on page 392).

Related Topics

Creating a List (on page 196)

Adding an Email Alias (on page 185)

Defining a list-server mailing list (on page 196)

Requesting and Subscribing to List Information (on page 214)

Sending mail to a list-server mailing list (on page 214)

Learning About Aliases (on page 183)

Types of List Server Mailing Lists

There are three kinds of basic lists (determined by the setting of **Allow Postings By** on the List Security page):

- *Anyone* (on page 195) (open list). Anyone can post a message to the list; the individual that posts to the list does not have to be a list subscriber.
- *Subscribers* (on page 195). Only a list subscriber can post a message to the list.
- *Moderated* (on page 194). Only a l*ist owner* (on page 216) can post a message to the list. Moderator is used when you want the list owner to review all messages before they are posted to the list.

You can further restrict the message posts with:

A password requirement.

A posters' list.

Those who send mail to a list restricted by a password and/or posters' list will have their mail returned with a "Restricted Post" message.



Note: If there are only a few individuals who the moderator wants to allow to post to the list, the moderator can give those few the appropriate password. However, if there are more than a few individuals who are permitted to post to the list, it may be more efficient to use a posters list.

Related Topics

List Administration (on page 192)

Creating and Managing Lists (on page 196)

Moderated Lists

The characteristics of a moderated list are:

- The moderator can post by addressing mail in the form of listname@domain.com.
- Only the moderator (list owner) can post a message to the list if **Use Password** and **Enable Posters List** are cleared.
- If **Use Password** is selected, the moderator must use a password in order to post to the list. This prevents others from "impersonating" the moderator by using the moderator’s mailing address.
- If **Enable Posters' List** is selected, users in the *posters' list* (on page 213) can post directly to the list and the moderator does not receive their mail. The moderator receives mail only from the addresses that are not in the posters' list.

- If both **Use Password** and **Enable Posters' List** are selected, the moderator receives mail only from those not in the posters' list and the moderator must enter a password in order to post to the list.

Related Topics

List Administration (on page 192)

Creating and Managing Lists (on page 196)

Types of List Server Mailing Lists (on page 194)

Open Lists

The characteristics of an open list are:

- Anyone can post to the list by addressing mail in the form of listname@domain.com .
- If **Use Password** is turned on in the List Security page, all list posters must enter a password to post to the list.
- The **Enable Posters List** option does not affect open lists. If this option is selected, anyone will still be able to post to the list whether they are in the posters list or not.

Related Topics

List Administration (on page 192)

Creating and Managing Lists (on page 196)

Types of List Server Mailing Lists (on page 194)

Subscriber Lists

The characteristics of a subscriber list are:

- 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 domain). In the body of the message, the intended subscriber enters the subscribe command and list name.
- Subscribers post a message by addressing mail in the form of listname@domain.com .
- If **Use Password** is selected in the List Security page, users must enter a password to post a message.
- If **Enable Posters List** is turned on, only subscribers and users in the posters list can post.

For a subscribers only list, users who are in the posters list can post messages to the list without being a subscriber. In this case, the user will not receive any list postings.

- If both **Use Password** and **Enable Posters List** are turned on, a subscriber must enter a password to post. Users in the posters list must enter a password as well.

Related Topics

List Administration (on page 192)

Creating and Managing Lists (on page 196)

Types of List Server Mailing Lists (on page 194)

Creating and Managing Lists

How to get here

Use the Add /Edit List page to create or modify a list. See *Types of List Server Mailing Lists* (on page 194) for information on lists.

Domain Name | List Name. The current domain name used for the list server followed by the List Name.

Directory. Displays top directory path of specified list.

General Options

- **List Name.** Enter a list name with no spaces. **List Name** can not be updated once created.
- **Mail List Name (Title).** Enter a descriptive title to help the list administrator identify the list. The name must be from 3 to 23 characters in length (spaces are OK).
- **List Owner's E-mail Address.** Enter the fully qualified e-mail address of the account *list owner* (on page 216) that the list runs under. This is the mail account that receives all messages (such as Subscribe and Unsubscribe requests) to the list. It is also the account from which help messages are sent and to which error messages are sent. This can be preset when creating new lists using the *Default List Settings* (on page 192).



Note: The List Owner e-mail address will not have access to the List Administration pages unless the e-mail address is same as the local list administrator or has List Administrator permissions for the local domain. See the *User Properties* (on page 126) page.

- **Local List Admin (User ID).** Enter only the User ID (do not add the full e-mail address) that resides on the local domain for the list administrator. This will allow *local list administration* (on page 216) permissions for only the specified list.



Important: To allow permissions for all lists, the User ID can be given List Administrator rights See the *User Properties* (on page 126) page.



Note: The list administrator and list owner are usually the same person, but a "dummy" user account can be set up to be the list owner in order to hide the identity of the list administrator or to give the impression of more people being involved in the list management.

- **Maximum Message Size (bytes).** Enter the maximum size of a message that can be sent to this list. Enter 0 to allow messages to be of unlimited size. This can be preset when creating new lists using the *Default List Settings* (on page 192).
- **Number of Recipients Per Message.** Enter the number of recipients each SMTP process will send to. To calculate this number divide the expected number of subscribers by 25, and enter the result. This can be preset when creating new lists using the *Default List Settings* (on page 192).



Tip: It is recommended that no more than 25 processes be used by any list.

List Subscribers (on page 201). Click this link to search or update users e-mail addresses for a selected list.

Inbound Rules (on page 202). Click this link to view the Inbound delivery rules, which sort incoming mail messages for each list server mailing list.

Help Message (on page 207). Click this link to edit the help text that is sent to anyone who requests help (by sending a list command to imailsrv@domain) or sends an invalid command to this list. This link will become active after the list has been created.

Subscribe Message (on page 207). Click this link will edit the *confirmation text* (on page 207) that will be sent to each person who submits a successful subscribe request to this list. This link will become active after the list has been created.

Security Options

Security Options will determine whether you want a list to be moderated or unmoderated as well as to determine who has access to the list.

- **Allowed Posters.** Drop down list of select users that can post to the list.
  - **Anyone.** Select to let anyone with an e-mail account post mail to a list.
  - **Subscribers.** Select to let only the list subscribers post mail to a list.
  - **Moderators.** Select to let only the list owner post mail. Moderator is used when you want the list owner to review all messages before they are posted to the list.
- **Disallow Subscription (ie: Private List).** Select to reject subscribe requests to a list. List subscribers can only be added one of the following ways:
  - *List administrator* (on page 216) using IMail Administrator to edit the *Users file* (on page 202).
  - List administrator using IMail Web Messaging to change user list permissions.



Note: Unsubscribe requests cannot be disabled.

- **Allow List Unsubscribes Based on Subject Line.** Select this option if you want the list-server mailing list to also accept an Unsubscribe command specified in the message Subject line. When users want to unsubscribe from the list-server mailing list, most list servers expect the Unsubscribe command to be specified in the body of the mail message.

When selected, the list-server mailing list will accept the following commands in the Subject line to unsubscribe to a list:

- unsubscribe
- remove
- signoff



Important: If the list requires a password, passwords are case-sensitive and there must be no leading spaces after the password. See example below.

Example:

The following example assumes there is a list named beer that allows unsubscribes based on the Subject line on an e-mail domain named domain.com.

To unsubscribe from the list:

TO: imailsrv@domain .com

Subject:Unsubscribe beer

- **Disable List Command.** Select if you do not want users to receive a list of the subscribers to your list-server mailing list. If not selected, users can obtain a list of the users subscribed to a list by addressing a message to the list server (for example, `imailsrv@domain.com`) and issuing the *list [listname] command* (on page 214) in the body of the message.



Note: List owners can always receive a list of subscribers regardless of whether the **Disable List Command** option is selected and regardless of the list type.

- **Enable Posters List**. Select to let any user with an e-mail address in the posters' list post to any type of list. If the **Use Password** option is enabled, users in the posters' list must enter a password.

  The posters' list is stored in a file named POSTERS.LST located in IMail Top Directory\Lists\listname.

- **Use Password.** Select to require a person to use a password before posting to the list. The password must be the first entry in the message **Subject** field. The password must be enclosed in brackets and colons. For example, **Subject**:[:password:]Unsubscribe beer

  The **Use Password** setting affects different list types as follows:

  - If Use Password is selected for an *anyone list (open)* (on page 194), all posters are required to enter a password to post to the list.
  - If Use Password is selected for a *subscriber list* (on page 194), the subscribers are required to enter a password to post the list.
  - If Use Password is selected for a *moderated list* (on page 194), the moderator is required to enter a password to post to the list.

Posters File (on page 207). Click this link to view, modify, or enter an e-mail address for users that can post messages to the selected list.

Kill File (on page 208). Click this link to view, modify, or enter an e-mail address for users that are no allowed to post messages to the selected list.

Digest Settings

To set up a *list-server mail digest* (on page 210), first enable digest mode, then set the digest options.

- **Enable Digest Settings.** Select this option to allow users to group the messages sent to this list into a digest.
- **Strip Non-Text Attachments before Posting.** Check box to enable the option to strip non-text attachments, such as graphic files, from messages when the digest posting is sent.
- **Digest Mailbox.** Enter the e-mail address where list postings are stored before the digest mailing is sent out. A copy of all postings will be sent to list_administrator-mailboxname@yourhost.com. This mailbox has the following characteristics:
  - After a posting is sent to the digest list, the Digest Mailbox is emptied and a copy is made in the format: digestmailboxMMDD.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* (on page 216) can view the mailbox from the Web Messaging client and can delete or add messages before the posting is sent. The list administrator can also view posted digests by the MMDD format described in the previous paragraph.
- **Subject Line for Digest Postings.** Enter the text that you want to appear in the digest posting subject line.
- **Include Headers and Trailers When Posting to Digest Mailbox**. Select this option to have the posted digest messages include the header and or trailer messages. We recommend turning off this option because it will make the digest larger and the digest includes its own header and trailer.
- **Enable Digest Header.** Select this option to include a header message at the beginning of the posted digest. For example, you can enter the subscribe/unsubscribe information for the digest and have it appear at the beginning of every message.
  - **Digest Header Message**. Enabled, enter the header message you want to be included at beginning of every message. This information is saved in the `"digest_header.txt"` file.
- **Enable Digest Trailer.** Select this option to include a trailer message at the end of the posted digest. For example, you can enter the subscribe/unsubscribe information for the digest and have it appear at the end of every message. After this option is selected, the message text box is enabled. Enter the trailer message you want to include with the digest messages. This information is saved in the digest_trailer.txt file.

  - **Digest Trailer Message**. Enabled, enter the trailer message you want to be included at the end of every message. This information is saved in the `"digest_trailer.txt"` file.
- **Enable Message Separators.** Select this option to specify lines or characters that will automatically separate messages in the digest posting.
  - **Digest Message Separators.** Enabled, enter the lines or characters that you want to use as a separator between every digest message. This information is saved in the `"digest_separator.txt"` file.

Subscribers. Click this link to search, add and delete digest subscribers. See *Subscribing to a Digest* (on page 209).

Scheduling. Click this link to configure the scheduling of processing messages for Digest subscribers.

Advanced Settings

- **Reply-To list (vs. Sender).** Select this option to have replies from a subscriber go to the list. Clear this option to have replies from a subscriber go to the sender of the original message.
- **Enable Subject Modification.** Select this option and enter text in the text box to prepend a text string to the subject line of every message sent to the list. For example, if you enter [Discussion List] as the prepended text, a message with the subject, "Parrot," will appear on the list server with the subject line: Subject: re:[Discussion List] Parrot. The default text is the name of this list.
- **Enable Header**. Enables the option to display text at the beginning of every message sent to the list.
  - **Header Message.** Enabled, allows a header message to be created that will display at the beginning of the list message. This information is saved in the `"header.txt"` file.
- **Enable Trailer**. Enables the option to display text at the end of every message sent to the list.
  - **Trailer Message.** Enabled, allows a trailer message to be created that will display at the end of the list message. This information is saved in the `"trailer.txt"` file.

Save. Click to save your changes.

Cancel. Click **Cancel** to exit without saving changes.

Related Topics

Testing the List (on page 213)

List Administration (on page 192)

Types of List Server Mailing Lists (on page 194)

Searching Lists for a User (on page 211)

List Subscribers

How to get here

Use the List Subscribers page to add, view, edit and remove users' e-mail address and name for the selected list. You can also search for users associated with the selected list.

Domain Name | List Name. The current domain name used for the list server followed by the List Name.

Search Box. Requires entering at least one character, and the search will automatically begin narrowing the address of names. The search assumes a wildcard automatically after each character are entered.

- **E-mail Address** list. This column displays the list user's e-mail address. Click to modify the e-mail address.
- **Full Name** list. This column displays the user names that are included in the selected list.
- **Add.** Click **Add** to add a new user to the selected list.
- **Remove.** Select an E-mail Address or multiple E-mail Addresses that you want to delete from the list, then click **Remove** to delete the addresses.

Save. Click the save button at the bottom of the screen. A message at the top "Your changes have been saved" will confirm.

Cancel. Click **Cancel** to exit without saving changes.

Related Topic

Adding Users to a List (on page 201)

Adding Users to a List

How to get here

Use the Add List User page to add a new to a selected e-mail list.

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used for the list server.
- **List Name.** The name of the e-mail list.
- **Email Address list.** Enter the new list user's e-mail address.
- **Full name.** Enter the user's First Name and Last Name.

View "Users" File

The purpose of this file, USERS.TXT, is to provide a list of subscribers to anyone who sends a *"list" command* (on page 214) to the list- server mailing list. This file is a list of the user names and e-mail addresses that is updated automatically when someone subscribes or unsubscribes to the list-server mailing list. (You can disable the "list" command on the Security tab.)

Note: This is not the list that is used by the list server to actually send mail to the list.

If you use a text editor to add or delete addresses from the Addresses file, you should also edit this file the same way if you want people who use the *"list" command* (on page 214) to see an updated list of subscribers.

Save. Click to save changes.

Cancel. Click **Cancel** to exit without saving changes.

View "Addresses" File

USERS.LST is the list of e-mail addresses that the list-server mailing list uses to address the mail it sends to this list. This file is updated automatically when someone subscribes or unsubscribes to this list. It is a text file with one address per line ending in a carriage return/line feed.

You can edit this file using a text editor to add or delete addresses that will receive mail from this list. However, you must also edit the *"Users" file (USERS.TXT)* (on page 201) if you want people who use the *"list" command* (on page 214) to see an updated list of subscribers.

Note: This list will ignore any invalid addresses in this file (**for example**, a typing error while editing this file).

Save. Click to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Inbound Delivery Rules for Lists

How to get here

Use Inbound delivery rules to sort incoming mail messages for each list server mailing list.

Use the Inbound Rules page to add new inbound rules, edit and delete inbound rules, move inbound rule evaluation priority up or down, add rules, and set actions to take on a message that matches the rule criteria.

The Inbound Rules list displays information about each of the active inbound rules for the selected mailing list. The inbound delivery rules for lists are stored in the `"rules.ima"` file, located in `...\IMail\ListName` domain top directory for the primary domain, and under `...\IMail\DomainName\ListName` for all non-primary domains.

Note: Rules are processed in the order in which they appear in the Rules list.

Inbound Rules

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Rules List

- **Name** list. Click a rule name to select and update the conditions and settings.
- **Action.** Displays the action to take on a message that matches the rule condition criteria.
- **Conditions**. Displays the conditions selected for each rule.
- **Filename.** Displays the name of the external rule condition file if it is used. See *Storing Search Text in an External Text File* (on page 230).
- **Destination.** Displays the mailbox or e-mail address to forward messages to that match the rule condition criteria. A Destination is only available when **Move to Mailbox** or **Forward** are selected in the *Action Type list* (on page 223).

Add. Click **Add** to create a new mail domain rule. For more information, see *Adding Inbound Delivery Rules for Domains* (on page 223).

Edit. Select a rule and click Edit, or double click a rule, to modify a rule.

Move Up. Select a rule and click **Move Up** to move the rule processing order to a higher priority for e-mail filtering. Rules are processed in the order in which they appear in the Rules list.

Move Down. Select a rule and click **Move Down** to move the rule processing order to a lower priority for e-mail filtering.

Delete. Select a rule that you want to delete from the Inbound Rules list, then click **Delete** to delete the rule.

Related Topics

Overview of Mail Delivery Rules (on page 218)

Rules Dialog (on page 156)

Creating an Outbound Rule for a Host (on page 222)

How Delivery Rules are stored and processed (on page 219)

Rules Syntax (on page 232)

Adding Multiple Conditions to Rules (on page 157)

Adding Rule for Lists

How to get here

Use the Rule Settings page to add new rule conditions, edit rule conditions, delete conditions, move rule condition evaluation priority up or down, add rule conditions, and set actions to take on a message that matches the rule condition criteria.

After you create a rule condition, the new Rule is placed at the bottom of the Rules list. Rules are identified in the list by their sequence in the list, for example (Rule 1, Rule 2; etc.).

Rule Name

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **List Name**. The current list the new rule is being set under.
- **Rule Name.** Enter the name for the rule.

Conditions

Use conditions from an external file. Select to use an external file that includes rule conditions. For more information, see *Storing Search String in an External Text File* (on page 230).

Use conditions from this table. Select to use rule conditions set from the options on the Rule Settings page.

- **Field.** Displays the message field that is filtered: **From Address**, **To**, **Subject**, **Sender**, **Body**, or **Header.**
- **Comparison.** Displays Contains when the delivery rule filter messages contain the search text. Displays **Does Not Contain** when the delivery rule filter message does not contain the search text.
- **Search Text.** Displays the search text that is used in the rule condition.
- **Match Case.** Displays Yes or No to indicate whether the search text must match the text case used in the Search Text condition.
- **Add Condition...** Click **Add** *to create a new rule condition* (on page 156).

  To add more than one condition to a rule, create the first condition, then click:

  - **Add AND/OR...** to create the second condition as you did the first. For more information, see *Adding Multiple Conditions to Rules* (on page 157).



Note: The Add Condition button will only display on a new rule with no conditions, and after an AND/OR has been created.



NOTE: Be aware, that a rule can not be saved when an AND/OR exists without a condition.

- **Edit**. Select a condition and click **Edit** or double click to modify a condition.

- **Delete.** Select a condition that you want to delete from the Conditions list, then click **Delete** to delete the condition.
- **Move Up**. Select a condition and click **Move Up** to move the condition processing order to a higher priority for e-mail filtering. Conditions are processed in the order in which they appear in the Conditions list.
- **Move Down.** Select a condition and click **Move Down** to move the condition processing order to a lower priority for e-mail filtering. Conditions are processed in the order in which they appear in the Conditions list.

Action

- **Action Type.** Select an action to take if a rule traps a message that meets the rule criteria:
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the **Target** box. If the mailbox does not exist, it is created. The default mailbox is "bulk". A POP3 user will see this mailbox only if he logs on to this mailbox using the format `userid-mailbox`. By default, if nothing is entered into the text box, messages meeting the rule criteria will be sent to the user's Main mailbox.
  - **Forward to Address.** Forwards the message to an e-mail address. Enter an e-mail address to forward mail to in the **Target** box. You must enter the full e-mail address, such as Mary@domain1.com .
  - **Delete.** Immediately deletes the message.
  - **Copy.** Delivers the message to its intended recipient as well as copies it to an additional address that you specify in the **Target** box.
  - **Bounce.** Sends the message back to the sender without being processed.
- **Target.** Enter the name of the user's mailbox or e-mail address to forward the message to that matches the rule condition criteria. If you enter a mailbox that does not exist, one is created. A POP3 user will see this mailbox only if he logs on to this mailbox using the format userid-mailbox. By default, if nothing is entered in the text box, messages meeting the rule criteria are sent to the user's Main mailbox.

Save. Click **Add** to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Related Topics

Inbound Rules for Lists (on page 202)

Overview of Mail Delivery Rules (on page 218)

Adding a Rule Condition (on page 156)

Creating an Outbound Rule for a Host (on page 222)

How Delivery Rules are stored and processed (on page 219)

Delivery Rule Syntax (on page 232)

Storing Search String in an External Text File (on page 230)

Adding Multiple Conditions to Rules (on page 157)

Adding a Rule Condition

Use this pop-up dialog to create a rule condition.

Define Condition

- **Where.** Select the message field that you want to filter: **From**, **To**, **Subject**, **Sender**, **Body**, or **Header.**
- **Comparison.**
  - **Contains.** Select to have the delivery rule filter messages that have this search text.
  - **Does Not Contain.** Select to have the delivery rule filter messages that do **not** have the search text.
- **Search Text.** Enter search text that contains the text you want to search. 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", enter: jazz
  - Type search expressions and quantifiers as shown in *text patterns* (on page 235).
  - 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.
- **Match Case.** Select to search for text that matches the case of the search text. To ignore the text case, clear **Match Case.**
- **Save.** Click **Save** to add condition.
- **Cancel.** Click **Cancel** to exit without saving changes.

Related Topics

Inbound Rules for Domains (on page 220)

Overview of Mail Delivery Rules (on page 218)

Delivery Rule Syntax (on page 232)

How Delivery Rules are Stored and Processed (on page 219)

Using Delivery Rules for a List-Server Mailing List

You can use *delivery rules* (on page 218) to reject incoming mail to a list-server mailing list based on the contents of To, From, Sender, Subject, the entire message Header (everything but the body of the message), or the Body of the message. See *Setting Inbound Delivery Rules for IMail Lists* (on page 202).



Note: Delivery rules can also be applied to all *mail for a mail host* (on page 220) or to *mail for individual users* (on page 153).

The "Help" File

How to get here

This file, "`Help.txt`", should contain the command syntax for all valid commands for a list-server mailing list; it should be similar to the Help topic on *List-Server Command Syntax* (on page 214). The contents of this file are e-mailed to anyone who requests help or who sends an invalid command to the list.

Each list has its own `"Help.txt"` file located in top directory `"IMail\domain \lists\listname"` (where listname is the directory name for the particular list) and applies only to the specified list.

Save. Click to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

The "Subscribe" File

How to get here

The contents of this file, `"Subscrib.txt"`, are sent to each person who submits a successful subscribe request to the list-server mailing list.

Each list has its own `"Subscrib.txt"` file located in top directory `"IMail\domain \lists\listname"` (where listname is the directory name for the particular list) and applies only to the specified list.

Save. Click to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

Poster File for a List

How to get here

The List Server uses the `"posters.lst"` file to allow only specified e-mail addresses in the file to be allowed to post to the list.

Each list has its own "`posters.lst`" file located in top directory `"IMail\domain \lists\listname"` (where listname is the directory for the particular list) and applies only to the specified list.

Adding Entries

Enter one entry per line in either of the following formats:

userid@host

fred@widget.com

Save. Click to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Kill File for a List

How to get here

The `"kill.lst"` file is used by the List-Server to deny access to local mailing lists. It lets you to specify mail addresses or mail hosts that you do not want to post to the list.

Each list has its own `"kill.lst"` file located in top directory `"IMail\domain \lists\listname"` (where listname is the directory for the particular list) and applies only to the specified list.

Adding Entries

In the KILL.LST file, enter one entry per line in either of the following formats:

userid@host

For example, to deny access from a user mail account, you would enter: fred@widget.com

@host

For example, to deny access to all users from the mail host widget.com , you would enter: @widget.com

@*partialhost

For example, to deny mail from any mail host ending in widget.com , enter: @*widget.com . This will reject all mail from widget.com, bluewidget.com, nifty.widget.com, etc.



Note: The kill files for lists are different from the *SMTP kill file* (on page 401).

Save. Click to save changes.

Cancel. Click **Cancel** to exit without saving changes.

List Digest Subscribers

How to get here

Use the List Server Mail Digest Subscribers page to search for digest subscribers, add new digest subscribers, and delete existing digest subscribers.

Domain Name (Official Host Name or **OHN)**. The current domain name used to address mail to the mail digest list is displayed.

List Name. The name of the mail digest list.

Search box. Enter an e-mail address or part of an e-mail address that you want to search for in the list of available mail digest list subscribers, then click **Search**.

List Digest Subscribers

- **E-mail Address list.** Displays a list of subscriber's e-mail addresses that are subscribed to the mail digest list.
- **Add.** Click **Add** to add a new subscriber to the mail digest list.
- **Delete.** Select a digest subscriber's e-mail address that you want to delete from the E-mail Address list, then click **Delete** to delete the subscriber.

Save. Click to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Adding to the List Subscriber

To subscribe someone to the List Digest

1. Click **add**
2. Enter their valid **"E-Mail Address"** to subscribe to the mail digest list.
3. Click **OK** to save your changes.

   -or-

   Cancel to exit without saving changes.

Related Topics

Setting Digest Schedule (on page 210)

Subscribing to a Digest

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@your_IMail_server_hostname) and enter the following command in the body of the message:

```
set mode digest listname
```

where listname is the mailing list name. 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 mailing list name.
```

Overview of Mail Digests

How to get here

You can offer subscribers a digest of messages sent to the list-server mailing list. The list server will "archive" messages sent to the list to a digest mailbox. The accumulated messages are then sent periodically to digest subscribers as a single message.

You schedule the digest to be sent on a time-basis (for example daily or weekly) or when the digest reaches a certain size. When subscribers receive a digest, it contains all the messages sent to the list since the last digest was sent.

Digest Scheduling

How to get here

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used for the list server.
- **List Name.** The name of the digest list.
- **Last Processing Date/Time.** Displays the last date and time the list digest was sent.
- **Frequency.** Select how often you want to distribute the list digest.
  - **Daily.** Sends the list digest on a daily basis.
  - **Weekly.** Sends the list digest on a weekly basis.
  - **Bi- Weekly.** Sends the list digest on a bi-weekly basis.
  - **Monthly.** Sends the list digest on a monthly basis.
  - **User- defined.** Sends the list digest on a user-defined basis.
  - **Size- exceeds.** Sends the list digest when the list digest exceeds a specified amount of memory space.
  - **Manual.** Sends the list digest only when the administrator sends it.
- **Next Processing Time.** Select a time (from the hour, minute, and AM/PM list options) to process the list digest.
- **Next Processing Date.** Select a date, on the calendar, to process the list digest. The date populates the text box.
- **Process/Send Now.** Click to send the list digest immediately.

Save. Click to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Example:

If you select **Daily** and set the **Next Processing Date/Time** to 07/18/2008 3:00 AM, then the digest will initially be posted on July 10th 2008, and then every day thereafter at the same time.

Managing Lists

Syntax Message (on page 211)

No List Message (on page 212)

Searching Lists for a User (on page 211)

Syntax Message

How to get here

The syntax message tells subscribers how to send a message that will allow them to subscribe, unsubscribe, review a list of supported lists, receive a list of users, help, request digest mode, or change back to standard mode.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Syntax Message

- **Current Message.** You can use the default message that appears in the text box as your syntax message, or modify it to meet your needs.

Save. Click to save your settings. An "Update Successful" message and the time of the update appear.

Searching Lists for a User

How to get here

You can use the List Search page to search for a list and its members on one or all domains. You can also delete individual or all members from a list.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **All domains.** Select this from the domain drop down to search all available domains.

Search. Enter the name of the list you are searching for in the text box, then click the **Search** button.

- **Email Address.** This column displays the Email Address of the list member.
- **User Name.** This column displays the User Name of the list member.
- **Domain**. This column displays the associated domain name of the listed User Name.
- **List Name.** This column displays the List Name of the list member.
- **List File.** Displays the list member's file name.

Remove. Select a list member, then click **Delete** to remove them from the list.

No List Message

How to get here

The "No List" message is returned when someone tries to perform an action for a list that does not exist.

The contents of this file, NOLIST.TXT, are sent to each person who attempts to subscribe to a non-existent list on this mail host.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

No List Message

- **Current Message.** You can use the default message that appears in the text box as your no list message, or modify it to meet your needs.

Save. Click to save your settings. An "Update Successful" message and the time of the update appear.



You can expand on the standard error message, perhaps giving valid names of list-server mailing lists that exist on this mail host.

Poster's List (Subscribed List)

For a subscribers only list, users who are in the posters list can post messages to the list without being a subscriber. In this case, the user will not receive any list postings.

Posters List (Moderated Lists)

For a moderated list, a user posts messages directly to the list. The messages are not sent to the moderator first.

List Owner Shortcuts for Subscribing and Unsubscribing

The list owner can "subscribe" someone by forwarding a message from that person to the list server.

The list owner can unsubscribe a user by sending a message to the list server with a message in the form: unsubscribe listname user@domain.com.

For example:

```
TO: imailsrv@domain.com

Subject: unsubscribe beer ethel@domain.com
```

Testing a List-Server Mailing List

To test a list-server mailing list:

From a system other than the IMail Server system, send a test mail message to imailsrv@your_IMail_server_hostname. 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 IMail Server system.

See the *List-Server Commands* (on page 214) for a description of the commands accepted by the list server.

Adding a Subscriber by Forwarding

You can add a subscriber by forwarding a message.



Note: You must be able to forward a message unmodified (i.e. with the headers unchanged) in order for this to work; otherwise you will end up adding or removing yourself from the list.

First, you set up a program alias :

1 Expand a mail host folder and select the Aliases folder.

2 Click the Add Alias button.
3 In the "New Alias " dialog box, enter an alias name. (For example, if the list name is Parrots, you might set up an alias named Parrots_add.
4 Select the Program alias type.
5 Click OK.
6 In the Resolves to box, enter the alias properties using the following format:

imailsrv -add domain listname

For example: imailsrv -add exotic.birds.com Parrots

Then, to subscribe a user by forwarding:

Forward a message from the user to the alias (Parrots_add), and the original sender of the message will be subscribed.

Sending Mail to a List

List subscribers can send a message to the list by addressing it to the name of the list-server mailing list. For example, to send a message to the "beer" list on domain.com:

TO: beer@domain.com

Subject: India Pale Ale

... body of message ...

When the list receives a message it is re-sent to all subscribers or it is archived to the digest and resent to the list in the digest.

Related Topics

Requesting and Subscribing to List Information (on page 214)

Requesting and Subscribing to List Information

In order for users to get information about lists on a particular mail host or to subscribe to lists on a particular mail host, users must send a request addressed to imailsrv@domain.com (where domain.com is the name of the mail host) and (when appropriate) include a list name in the body of the message. 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 list-server mailing 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

- Get a digest of messages sent to the list

The following example request commands assume there is a list named "beer" on a mail domain named domain.com.

Requesting List Information

The commands for requesting list information are as follows:

1 `Help.` To get general help from the list server:

```
TO: imailsrv@domain.com
Subject:

help
```

2 `Help [listname. To get help for a specific list:`

```
TO: imailsrv@domain.com
Subject:

help beer
```

3 `List.` To get the names of the list-server mailing lists on the IMail Server:

TO: imailsrv@domain.com
`Subject:`

`list`

4 List [listname]. To get a list of users subscribed to a specific list:

TO: imailsrv@domain.com
`Subject:`

list beer

Subscribing and Unsubscribing to a List or Digest

The commands for subscribing and unsubscribing to lists or list digests are as follows:

1 `Subscribe.` To subscribe to a specific list:

```
TO: imailsrv@domain.com

Subject:

Subscribe beer Fred Farkle
```

2 `Unsubscribe.` To unsubscribe to a specific list:

```
TO: imailsrv@ domain.com

Subject:

Unsubscribe beer Fred Farkle
```

3 `Set mode digest listname.` To receive a digest of messages sent to the list:

```
TO: imailsrv@domain.com
Subject:
set mode digest beer
```

4 `Set mode standard listname.` To cancel digest mode and receive messages as they are sent to the list:

```
TO: imailsrv@domain.com
Subject:
set mode standard beer
```

Local List Administrator

How to get here

The list administrator can modify list properties, add and delete list users, and edit all related files, such as the Syntax Message, No List Message, Help Message, and the Subscribe Message.

On a moderated list, if the list administrator is also the *list owner* (on page 216) (a.k.a. **List Owner's Email Address**), then the list administrator will also be the list moderator.

If a list is moderated, the list owner is known as a "moderator."

The moderator is the only one who can post to a moderated list. (The moderator receives all messages to the list, before they are posted; the moderator can then review the content of the message and then decide to post it or not.)

The list administrator can be a **local list administrator,** which is set in the **Standard List Settings** section of the List Administration page in the **Administrator's Local Username** box. A list administrator can also be a Domain Administrator, who can administer `any` list-server mailing list on the mail domain (see *User Properties* (on page 126) page).

Note: The list administrator and list owner are usually the same person, but a "dummy" user account can be set up to be the list owner in order to hide the identity of the list administrator or to give the impression of more people being involved in the list management.

List Owner

This is the full e-mail address of the mail account that receives all messages (such as Subscribe and Unsubscribe requests) to the list. It is also the account from which help messages are sent and to which error messages are sent.

On a moderated list, the **list owner** is also known as the moderator.

If a list is moderated, the list owner is known as a "moderator."

The moderator is the only one who can post to a moderated list. (The moderator receives all messages to the list, before they are posted; the moderator can then review the content of the message and then decide to post it or not.)

The **list owner** and *list administrator* (on page 192) are usually the same person, but a "dummy" user account can be set up to be the list owner in order to hide the identity of the list administrator. There can be **only one list owner per list**.

List Moderator

If a list is moderated, the list owner is known as a "moderator."

The moderator is the only one who can post to a moderated list. (The moderator receives all messages to the list, before they are posted; the moderator can then review the content of the message and then decide to post it or not.)

LDAP Settings

How to get here

Use the LDAP Settings page to configure host options for OpenLDAP. This information is necessary for an LDAP client to edit the LDAP database. It is not necessary to enter an ID or password if you only want to view the OpenLDAP data.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

LDAP Settings

- **LDAP Admin ID.** Displays the LDAP administrator ID for the e-mail domain. This information is auto-populated. The administrator ID cannot be an IMail user ID.
- **Password.** Enter the LDAP administrator password.
- **Confirm Password.** Enter the password a second time to confirm the original password. The two password entries must match in order for the value to be saved.



Caution: Do not click **Initialize LDAP** unless you want to overwrite the database with the user IDs only that are stored in the Windows registry. First try synchronizing the LDAP database to resolve any problems.



Important: Because the password is randomly generated during installation and importation, we highly recommend that you change it as soon as possible after completing setting up LDAP.



Important: You can also use the *iLDAP.exe utility* (on page 382) to Init or Sync a specified LDAP domain or all the LDAP domains. This utility can be used in the case when the Web Administrator does not properly Init or Sync all the LDAP domains on a server. This issue sometimes occurs on servers running Microsoft Windows 2003 machines with over 30 domains.

LDAP Actions

- **Init LDAP (Initialize the LDAP database).** Click to Initialize the LDAP database created for the current e-mail domain by the *LDAP server* (on page 375).
- **Sync LDAP (Synchronize the LDAP database).** Click to synchronize the LDAP database. Synchronizing removes multiple database entries, deletes old accounts, and adds new accounts.

Save. Click to save settings. An "**Update Successful"** message and the time of the update appear.

Related Topics

About LDAP Server (on page 375)

About LDAP Data (on page 376)

LDAP Service Settings (on page 377)

LDAP User Information (on page 150)

Populating the LDAP Database Using Ldaper.exe (on page 381)

Init & Sync LDAP DB - iLDAP.exe utility (on page 382)

InBound / Outbound Rules

Delivery rules are used to direct mail based on the contents of the **To**, **From**, **Sender**, **Subject**, message **Header**, or the message **Body** fields.

Rules are helpful in filtering out spam and emails that contain certain types of attached files. You can also use rules to direct mail, such as a newsletter, into a specific mailbox.

IMail Administrator supports the following two types of delivery rules:

- **Inbound Delivery Rules** (on page 220). Inbound Delivery Rules apply to incoming mail that is sent by a non-local user. These rules can be created at three levels: e-mail domains, individual users, and list-server mailing lists.
- **Outbound Delivery Rules** (on page 222). Outbound delivery rules filter messages that are sent out by local users through IMail Server and can be created only at the domain level.

Both Inbound and Outbound rules support multiple rule conditions. Delivery rules can also be used in conjunction with forwarding or the Auto Responder to re-route mail from one user to another. For example, a system administrator could route messages containing particular words to a reviewer.

Related Topics

How Delivery Rules are stored and processed (on page 219)

Delivery Rule Syntax (on page 232)

Setting Inbound Delivery Rules for IMail Domains (on page 220)

Setting Outbound Delivery Rules for IMail Domains (on page 222)

Setting Inbound Delivery Rules for IMail Users (on page 153)

Setting Inbound Delivery Rules for IMail Lists (on page 202)

Storing Search String in an External Text File (on page 230)

Examples of Delivery Rules (on page 236)

How Rules are Stored and Processed

All inbound rules are stored in the `rules.ima` file. Since inbound rules can be created for mail domains, users, and mailing lists, there can be multiple `rules.ima` files on your IMail Server. The location of the `rules.ima` file differs depending on whether the rule is for a mail domain, a user, or a list server mailing list.

- For a mail domain, the `rules.ima` file is located in the mail domain's top folder.
- For a user, the `rules.ima` file is located in the user's folder.
- For a list server mailing list, the `rules.ima` file is stored in the list's folder.

Outbound delivery rules are stored in the orules.ima file. Since outbound rules can only be created for mail domains, the `orules.ima` file is located in the mail domain's folder. If you have more than one mail domain on your IMail Server, you may have multiple `orules.ima` files, one file for each host.

IMail Server reads the `rules.ima` and `orules.ima` files during the delivery process. The rule files for the virtual domain are evaluated first, then the rules for users and lists. For more information, see *IMail Processing Order* (on page 27).

Any `rules.ima or orules.ima` file can be copied to other directories. For example, if you create inbound delivery rules for one user, you can copy the `rules.ima` file to the directories of other users to apply the same rules to them.

Related Topics

Overview of Mail Delivery Rules (on page 218)

Storing Search Strings in an External Text File (on page 230)

Using IMail Rules to Filter Spam

Delivery rules are powerful for filtering spam because they offer more options for processing messages than the antispam components. When using the antispam components, if a message is identified as spam, you can delete it, forward it to an e-mail address, or insert an X- Header . When using delivery rules to process a message, you can choose to **Delete**, **Forward**, **Move to Mailbox**, **Copy,** or **Bounce** messages. Delivery rules can be set up at the e-mail domain and user levels.

If a message matches entries in the black lists or fails a verification check, an X-Header is inserted into the message header. Additionally, phrase filtering and statistical filtering can be configured to insert X-Headers. If you want to filter a message with an X-Header, you can set up a rule to search for one of the X-Headers. If a message is trapped by a rule, it is immediately processed according to the action specified in the rule.



Tip: You may want to select the **Insert X- Header** option and set up a mailbox specifically for spam, so that you can evaluate the messages that are trapped to ensure that no legitimate mail gets caught by mistake.

Example 1: *Bouncing spam messages* (on page 55)

Example 2: *Filtering messages listed in a black list for a specific reason* (on page 278)

Example 3: *Sending spam to a specific folder in a user™s account* (on page 239)

Example 4: *Receiving Mailing Lists and Newsletters that are identified as spam* (on page 239)

Related Topics

Delivery Rules Overview (on page 218)

Adding a Rule Condition (on page 156)

Spam X-Header Explanations (on page 330)

Inbound Delivery Rules for Domains

How to get here

Use the Inbound delivery rules page to sort incoming mail messages for the mail domain by adding new inbound rules, editing, deleting, moving inbound rule evaluation priority up or down, and setting actions to take on a message that matches the rule criteria.

The Inbound Rules list displays information about each of the active inbound rules for the selected mail domain. The inbound delivery rules for a mail domain are stored in the `rules.ima file,` located in `...\IMail` domain top directory, for the primary domain, and under `...\IMail\DomainName` for all non-primary domains.

Note: Rules are processed in the order in which they appear in the Rules list.

Inbound Rules

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Rules List

- **Name** list. Click a rule name to select and update the conditions and settings.
- **Action.** Displays the action to take on a message that matches the rule condition criteria.
- **Conditions**. Displays the conditions selected for each rule.
- **Filename.** Displays the name of the external rule condition file if it is used. See *Storing Search Text in an External Text File* (on page 230).
- **Destination.** Displays the mailbox or e-mail address to forward messages to that match the rule condition criteria. A Destination is only available when **Move to Mailbox** or **Forward** are selected in the *Action Type list* (on page 223).

Add. Click **Add** to create a new mail domain rule. For more information, see *Adding Inbound Delivery Rules for Domains* (on page 223).

Edit. Select a rule and click Edit, or double click a rule, to modify a rule.

Move Up. Select a rule and click **Move Up** to move the rule processing order to a higher priority for e-mail filtering. Rules are processed in the order in which they appear in the Rules list.

Move Down. Select a rule and click **Move Down** to move the rule processing order to a lower priority for e-mail filtering.

Delete. Select a rule that you want to delete from the Inbound Rules list, then click **Delete** to delete the rule.

Related Topics

Overview of Mail Delivery Rules (on page 218)

Adding an Inbound Rule Condition (on page 156)

Creating an Outbound Rule for a Domain (on page 222)

How Delivery Rules are stored and processed (on page 219)

Rules Syntax (on page 232)

Storing Search Strings in an External Text File (on page 230)

Adding Multiple Conditions to Rules (on page 157)

Bouncing spam messages (on page 55)

Outbound Delivery Rules for Domains

How to get here

Use Outbound delivery rules to filter messages that are being sent through IMail Server to a non-local address. Outbound delivery rules can only be created for IP domains.



Note: Outbound rules can not be created for virtual domains. Virtual domains will follow the outbound rules of the IP address that it is bound to.

Use the Outbound Rules page to add new outbound rules, edit outbound rules, delete outbound rules, move outbound rule evaluation priority up or down, and add and set actions to take on a message that matches the rule criteria.

The Outbound Rules list displays information about each of the active Outbound rules for the selected mail domain. The outbound delivery rules for a mail domain are stored in the o`rules.ima file,` located in ...\IMail domain top directory, for the primary domain, and under ...\IMail\DomainName for all non-primary domains.



Note: Rules are processed in the order in which they appear in the Rules list.

Outbound Rules

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Rules List

- **Name** list. Click a rule name to select and update the conditions and settings.
- **Action.** Displays the action to take on a message that matches the rule condition criteria.
- **Conditions**. Displays the conditions selected for each rule.
- **Filename.** Displays the name of the external rule condition file if it is used. See *Storing Search Text in an External Text File* (on page 230).
- **Destination.** Displays the mailbox or e-mail address to forward messages to that match the rule condition criteria. A Destination is only available when **Move to Mailbox** or **Forward** are selected in the *Action Type list* (on page 223).

Add. Click **Add** to create a new mail domain rule. For more information, see *Adding Inbound Delivery Rules for Domains* (on page 223).

Edit. Select a rule and click Edit, or double click a rule, to modify a rule.

Move Up. Select a rule and click **Move Up** to move the rule processing order to a higher priority for e-mail filtering. Rules are processed in the order in which they appear in the Rules list.

Move Down. Select a rule and click **Move Down** to move the rule processing order to a lower priority for e-mail filtering.

Delete. Select a rule that you want to delete from the Inbound Rules list, then click **Delete** to delete the rule.

Related Topics

Storing Search Text in an External Text File (on page 230)

Delivery Rule Syntax (on page 232)

Rules Dialog (on page 156)

Adding Multiple Conditions to Rules (on page 157)

Adding Rule for Domains

How to get here

Use the Rule Settings page to add new rule conditions, edit rule conditions, delete conditions, move rule condition evaluation priority up or down, add rule conditions, and set actions to take on a message that matches the rule condition criteria.

After you create a rule condition, the new Rule is placed at the bottom of the Rules list. Rules are identified in the list by their sequence in the list, for example (Rule 1, Rule 2; etc.).

Rule Name

- **Domain Name (Official Host Name** or **OHN)**. The current domain name used to address mail to the users on the mail domain is displayed. For example, company.com is the domain name in the address john.public@company.com.
- **Rule Name**. Enter the name for the rule.

Conditions

Use conditions from an external file. Select to use an external file that includes rule conditions. For more information, see *Storing Search String in an External Text File* (on page 230).

Use conditions from this table. Select to use rule conditions set from the options on the Rule Settings page.

- **Field.** Select the message field to be filtered: **From Address**, **To**, **Subject**, **Sender**, **Body**, or **Header.**
- **Comparison.** Displays **Contains** when the delivery rule filter messages contain the search text. Displays **Does Not Contain** when the delivery rule filter message does not contain the search text.
- **Search Text.** Displays the search criteria that is used in the rule condition.
- **Match Case.** Displays **Yes** or **No** to indicate whether the search text must match the text case used in the Search Text condition.
- **Add Condition...** Click **Add** *to create a new rule condition* (on page 156).

  To add more than one condition to a rule, create the first condition, then click:

  - **Add AND/OR...** to create the second condition as you did the first. For more information, see *Adding Multiple Conditions to Rules* (on page 157).



Note: The Add Condition button will only display on a new rule with no conditions, and after an AND/OR has been created.



NOTE: Be aware, that a rule can not be saved when an AND/OR exists without a condition.

- **Edit**. Select a condition and click **Edit** or double click to modify a condition.
- **Delete.** Select a condition that you want to delete from the Conditions list, then click **Delete** to delete the condition.
- **Move Up**. Select a condition and click **Move Up** to move the condition processing order to a higher priority for e-mail filtering. Conditions are processed in the order in which they appear in the Conditions list.
- **Move Down.** Select a condition and click **Move Down** to move the condition processing order to a lower priority for e-mail filtering. Conditions are processed in the order in which they appear in the Conditions list.

Action

- **Action Type.** Select an action to take if a rule traps a message that meets the rule criteria:
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the **Target** box. If the mailbox does not exist, it is created. The default mailbox is "bulk". A POP3 user will see this mailbox only if he logs on to this mailbox using the format `userid- mailbox`. By default, if nothing is entered into the text box, messages meeting the rule criteria will be sent to the user's Main mailbox.
  - **Forward to Address.** Forwards the message to an e-mail address. Enter an e-mail address to forward mail to in the **Target** box. You must enter the full e-mail address, such as Mary@domain1.com.
  - **Delete.** Immediately deletes the message.

  - **Copy.** Delivers the message to its intended recipient as well as copies it to an additional address that you specify in the **Target** box.
  - **Bounce.** Sends the message back to the sender without being processed.
- **Target. Enter the name of the user's mailbox or e-mail address to** forward the message to which matches the rule condition criteria. If you enter a mailbox that does not exist, one is created. A POP3 user will see this mailbox only if he logs on to this mailbox using the format userid-mailbox. By default, if nothing is entered in the text box, messages meeting the rule criteria are sent to the user's Main mailbox.

Save. Click **Add** to save changes.

Cancel. Click **Cancel** to exit without saving changes.

Related Topics

Overview of Mail Delivery Rules (on page 218)

Adding a Rule Condition (on page 156)

Creating an Outbound Rule for a Host (on page 222)

How Delivery Rules are stored and processed (on page 219)

Delivery Rule Syntax (on page 232)

Storing Search String in an External Text File (on page 230)

Adding Multiple Conditions to Rules (on page 157)

Adding a Rule Condition

Use this pop-up dialog to create a rule condition.

Define Condition

- **Where.** Select the message field that you want to filter: **From**, **To**, **Subject**, **Sender**, **Body**, or **Header.**
- **Comparison.**
  - **Contains.** Select to have the delivery rule filter messages that have this search text.
  - **Does Not Contain.** Select to have the delivery rule filter messages that do **not** have the search text.
- **Search Text.** Enter search text that contains the text you want to search. 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", enter: jazz
  - Type search expressions and quantifiers as shown in *text patterns* (on page 235).

  - 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.
- **Match Case.** Select to search for text that matches the case of the search text. To ignore the text case, clear **Match Case.**
- **Save.** Click **Save** to add condition.
- **Cancel.** Click **Cancel** to exit without saving changes.

Related Topics

Inbound Rules for Domains (on page 220)

Overview of Mail Delivery Rules (on page 218)

Delivery Rule Syntax (on page 232)

How Delivery Rules are Stored and Processed (on page 219)

Adding Multiple Conditions for Domains

You can create multiple conditions for both inbound and outbound rules. By using multiple conditions, you can often combine multiple rules into one, thus, saving time and creating a more compact rules file. Sometimes a rule with only one condition is adequate to fulfill rule filtering requirements. However, when you need to create more complex rules, you may want to use multiple conditions. For example, see *Rule with Multiple Conditions Example* (on page 226).

To add a rule with multiple conditions:

1. Follow the instructions to create a rule as described in *Setting Inbound Rules for Domains* (on page 220) or *Setting Outbound Rules for Domains* (on page 222). After adding the first rule condition, select the new rule condition.
2. Click **Add AND/OR...** This will bring a pop-up window allowing either
   - selection of the **"AND"** button, meaning **"ALL"** the rule conditions must be met for the message to be trapped.
   - or selection of the **"OR"** button, meaning **"ANY"** one of the conditions must be met for the message to be trapped.
3. Create the second condition as you did the first. Continue adding conditions until you are satisfied with the rule.
4. Follow the instructions to set the rule actions as described in the **Actions** section of *Adding Inbound Rules for Domains* (on page 223) or *Adding Outbound Rules for Domains* (on page 223).
5. When you are finished creating the rule, click **Add** to save your changes.

Rule with Multiple Conditions Example

If you want all e-mails from your supervisor containing information 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.

The rules.ima format:

<BOSS>F~supervisor@domain.com!AND!B~project updates:BOSS

Where:

<BOSS>	Rule Name
F~supervisor@domain.com	From Address must contain "supervisor@domain.com"
!AND!	AND means all conditions must be true to be selected
B~project updates	Body of message must contain "project updates"
:BOSS	mailbox name, that message will be forwarded to of user's account.

Attachment Blocking

How to get here

Use the Attachment Blocking page to specify types of attachments to block from incoming and outgoing e-mail messages and actions to take on blocked messages. Attachments are blocked based on message MIME types and filename types. In addition to selecting the types of message attachments to block, you can define actions to take on blocked messages.

An attachment blocking folder exists for each e-mail domain and the attachment blocking options can be based on the current e-mail domain or the primary e-mail domain settings.

Use the Users Attachment Blocking page to search for attachment blocking types in the selected domain, access and edit attachment blocking types, add new attachment blocking types, or delete attachment blocking types.

Important: Remember to restart Queue Manager after making Attachment Blocking or Blocking Message modifications.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account. (Primary and non-primary IP'd domains only)

- **Use.** Drop down menu.
  - **No Filter**. Select this option to disable all Attachment Blocking for this domain.
  - **Current Domain**. Set by Default. Only option when only a primary domain exists. For non-primary domains use this option if you would like the attachment blocking settings to be different than the primary domain.

    - **Primary Domain**. Select this option to allow the current non-primary domain to use the same attachment blocking settings as the primary domain.
- **Content**. Attachment blocking types. See *Adding Attachment Blocking Types* (on page 229), for examples.
- **Type**. Select from File name or MIME type.
- **Action**.Select the action to take on a attachment blocking type match:
    - **Replace Attachment** to replace the attachment with a message that provides information about the blocked attachment.
    - **Strip Attachment** to remove the attachment without a message that provides information about the blocked attachment.
- **Enabled**. Select to enable or disable rules that you have added to the attachment blocking settings, without having to remove the setting.

Add. Select to create a new attachment blocking type. For more information, see *Adding Attachment Blocking Rules* (on page 229).

Edit. Select an attachment blocking type that you want to modify, then click **Edit** to modify an existing attachment type.

Delete. Select an attachment blocking type that you want to delete from the current domain, then click **Delete** to delete the type.

Attachment Blocking Message

The message box includes a default message that provides information about the attachment that has been removed. You can also create a custom message that replaces attachment body content that has been blocked.

When an attachment is blocked and the **Replace Attachment** option is selected in the **Action for match** list (on the *Add Blocker page* (on page 229) accessed by clicking **Add** on the Attachment Blocking page), a custom message is sent in the place of the attachment to the message recipient.

Use:

- **Current Domain.** Select this option to define attachment blocking messages specific to the current e-mail domain.
- **Primary Domain** (default). Select this option to define attachment blocking messages based on the primary e-mail domain's message settings.

This message will replace the body of a blocked e-mail attachment:

Use the default message that is included in the message box or enter a custom message to send e-mail recipients when an attachment is blocked. You can include variables in the custom message:

- **%t** to indicate the message type (MIME or filename)
- **%c** to indicate the filename of the blocked attachment (if applicable)

The contents of the message box are saved in a file named ab-message.txt located in the appropriate e-mail domain's top directory. The message box text should only be edited from the Attachment Blocking **Message** tab and is limited to 924 characters.



Note: If you want to log messages from the attachment blocking feature, make sure that the **Verbose Logging** is selected on the **SMTP Settings** (on page 392) Page.

Related Topics

Adding Attachment Blocking Types (on page 229)

Blocking Message (on page 230)

Adding Attachment Blocking types

Use the Add Blocker page to set options for new attachment blocking types.

- **Type of Blocker** list. Select the type of attachment to block: **Filename** or **MIME** .
- **Content to Search for.** Select from the default file or MIME types or enter a custom file or MIME type that is not included in the list.
  - **Filename.** Default file types are: *.chm, *.cmd, *.com , *.cpl, *.crt, *.csh, *.exe, *.fxp, *.hlp, *.hta, *.inf, *.ins, *.isp, *.js, *.jse, *.ksh, *.lnk, *.mda, *.mdb, *.mde, *.mdt, *.mdw, *.mdz, *.msc, *.msi, *.msp, *.mst, *.ops, *.pcd, *.pif, *.prf, *.prg, *.reg, *.scf, *.scr, *.sct, *.shb, *.shs, *.url , *.vb, *.vbe, *.vbs, *.wsc, *.wsf, and *.wsh.
  - **MIME.** Default MIME types are: **application** and **image/jpeg**.
- **Action for match list.** Select the action to take on a attachment blocking type match:
  - **Replace** to replace the attachment with a message that provides information about the blocked attachment.
  - **Strip** to remove the attachment without a message that provides information about the blocked attachment.
- **Enable Blocker Now** (selected by default). Select to enable or disable rules that you have added to the attachment blocking settings.
- **Add.** Click **Add** to save changes.
- **Cancel.** Click **Cancel** to exit without saving changes.

The attachment blocking rule settings are saved in a file named `"ab.txt"` located in the appropriate e-mail domain 's top directory. In addition to adding attachment blocking rules from the **Attachment Blocking** page, you can edit the settings in the "`ab.txt" file`.

Related Topics

Setting Attachment Blocking Options (on page 227)

Blocking Message

How to get here

The blocking message that a recipient will receive when a message of attachment has been blocked.

Domain: Shows the current selected domain. From this drop down you can switch to any of the domains available to this administrative user account.

- **Use.** Drop down menu.
  - **Current Domain**. Set by Default. Only option when only a primary domain exists. For non-primary domains use this option if you would like the blocking message to be different than the primary domain.
  - **Primary Domain**. Select this option to allow the current non-primary domain to use the same blocking message as the primary domain.
- **Message.** Text that will appear in the body of a blocked attachment.

Save. Click to save your settings.

Storing Search Strings in an External Text (.rul) File

If you need to frequently update and distribute the delivery rules search text, you can use external text files to store the search text. External files were designed to allow frequent updating of rules without creating a new rule.

Important: The following rules are required for external rules:

1. The External Rule file must exist in the same directory as the `"rules.ima"` or `"orules.ima"` file.

2. The External Rule file when referenced in the rule must **not** include the `".rul"` file extension.

3. The External Rule file must have a file extension of `".rul"`

Example:

(mortgage|loans|credit offer), where the pipes mean "or" and separate the conditions. Usage of the "and" condition is not permitted in a `".rul"` file. Also, the `".rul"` file must be located in the same directory as the `"rules.ima"` or `"orules.ima"` file.

To illustrate this, the administrator can use this method to catch mail from known spammers. The administrator might create a text file named "spam1.rul". Each time a new spammer address is discovered, the administrator can add it to the `"spam1.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. For more information, see *External Text File Example* (on page 231) and *Rule Syntax* (on page 232).

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

1 Select a mail domain, or the list that you want to create an external rule for.
2 Click either **Inbound Rules** or **Outbound Rules**, then click **Add** to create a new mail domain rule. The Rule Settings page appears. For more information, see *Adding Inbound Rule Conditions for Domains* (on page 223) or *Adding Outbound Rule Conditions for Domains* (on page 223).

- Click **Use conditions from an external file**, then do one of the following:
  - Enter the name of the file in the second Search text box without the ".rul" extension.



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** because IMail will append it to the filename you enter.

1 Click **Edit** to open and edit the rule file in Windows Notepad (or your default text editor). If the rules file does not exist, one will be automatically created. For information about creating the search text, see *Rule Syntax* (on page 232).
2 Click **Save** to save the rule.

Related Topics

External Text File Example (on page 231)

Overview of Mail Delivery Rules (on page 218)

Delivery Rule Syntax (on page 232)

External Text File Example

To search all new message Headers with conditions from external file "spam.rul" and to send to mailbox "spambox":

```
<Rule 1>H~:spam:spambox
```



Note: The reference to :spam is referring to an external file "spam.rul" that must exist in the same directory as the "rules.ima" file.

The external file "spam.rul" contains the following conditions

```
word1|word2|word3|word4|word5
```

Where word1 or word2 or word3 or word4 or word5 would return a true condition and the message would be moved to the `"spambox"` mailbox.

Important: A colon must precede the `.rul` file name (in this example, spambox). The IMail Server reads the `rules.ima` file and looks for the referenced spam.rul file at the same location as the rules.ima file.

Related Topics

Storing Search Text in an External Text File (on page 230)

Add/Edit Rule Condition (on page 156)

Rules Syntax

Related Topic:

Condition and Quantifier Syntax (on page 234)

Text Patterns (on page 235)

Message Area (on page 236)

When you create a inbound or outbound rules, the rule is entered in the rules.ima (inbound) or orules.ima (outbound) file. Following are examples of the rule syntax for both a single condition and multiple condition rule and explanations of each rule element.

Note: The following characters: **{} () | * + , . : \ []^$** require an **escape "\"** to allow being used in a search string in a rule. If you want to use one of these characters in a search string, precede it with the escape.

Example: To search for a plus sign, enter **\+** in the search string.

Single Condition Rule

Syntax:

message area (on page 236)

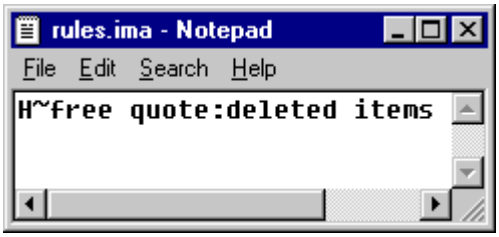
condition (on page 234)

search text (on page 235)

quantifier (on page 234) : mailbox name

Example:

The following represents the syntax for a single condition rule as it appears in the rules.ima file.



Explanation of Rule:	
H	If the Header of the message (From, To, Sender, Subject, Cc)
~	contains
free quote	the words "free quote"
:	send to
deleted items	the mailbox named deleted items

Multiple Condition Rule

Syntax:

message area (on page 236)

condition (on page 234)

search text (on page 235)

quantifier (on page 234)

!AND!/!OR!

message area (on page 236)

condition (on page 234)

search text (on page 235)

quantifier (on page 234) : mailbox name

Example:

The following represents the syntax for a multiple condition rule as it appears in the rules.ima file.



Explanation of Rule:	
S	If the Subject of the message
~	contains
weight loss	the words "weight loss"
!OR!	or
B	the Body of the message
~	contains
weight loss	the words "weight loss"
:	send to
Trash	the mailbox named Trash

Condition and Quantifier Syntax

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

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

Related Topic:

Rule Syntax (on page 232)

Text Patterns (on page 235)

Message Area (on page 236)

Text Patterns

Text Pattern	Expression
Any character	. (period)
Any of the values separated by vertical bars within 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
Any punctuation character	\p
Any non-punctuation character	\P

Note: 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

Related Topic:

Rule Syntax (on page 232)

Condition and Quantifier Syntax (on page 234)

Message Area (on page 236)

Message Area

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

Related Topic:

Rule Syntax (on page 232)

Condition and Quantifier Syntax (on page 234)

Text Patterns (on page 235)

Example for Entering Rules in the Rules.ima File

In This Section

Examples of Delivery Rules (on page 236)

Sending to Specific Folder for User (on page 239)

Receiving Mailing Lists and Newsletters that are Identified as Spam (on page 239)

Determining Which Rule Trapped a Message (on page 240)

Examples of Delivery Rules

Inbound delivery rule for a host. A school administrator can set up an inbound delivery rule that scans for offensive language in mail messages and deliver such

messages to a special user account that can be reviewed by a faculty member. *Example*[5]

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 a local user. *Example* (on page 239)

Inbound delivery rule for a list-server mailing list. A system administrator can set up an inbound delivery rule for a list-server mailing list to scan the body of all messages addressed to the list and scan for language that indicates that the e-mail came from a spammer or bulk mailer. If such messages are found, they can be deleted. For example, the rule can search for one of the following 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

Example (on page 238)

An Inbound delivery rule for an individual user. You could set up an inbound delivery rule for a sporting goods salesman to have all messages with baseball, softball, bat, base, homerun, or cap in the Subject line be automatically placed in his mailbox named Baseball. *Example*[6]

An Inbound delivery rule combined with the Info Manager. You could set up an inbound 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. *Example*[7]

---

[5] Enter the following rule into the e-mail domain 's rules.ima file:
```
H~(word1|word2|word3)!OR!
B~(word1|word2|word3):spamboxH~(word1|word2|word3)!OR!
B~(word1|word2|word3):spamboxNote: Replace word 1, word 2, and word 3 with the offensive words you want to search for. The vertical bar represents "or", therefore, this rule will search for word 1, or word 2, or word 3.If you do not want the user to access spambox because you want to monitor the mail yourself (as the mail administrator), put a forward ...
```

[6] Example for entering rules in the rules.ima fileThe following rule will search the Subject field for baseball or base or bat or cap or homerun or softball and upon a match will send the message to the user's "baseball" mailbox.
```
S!(baseball|base|bat|cap|homerun|softball):baseball
```

[7] Enter the following rule into the e-mail domain 's rules.ima file:
```
H~(word1|word2|word3)!OR!
B~(word1|word2|word3):spamboxH~(word1|word2|word3)!OR!
B~(word1|word2|word3):spamboxNote: Replace word 1, word 2, and word 3 with the offensive words you want to search for. The vertical bar represents "or", therefore, this rule will search for word 1, or word 2, or word 3.If you do not want the user to access spambox because you want to monitor the mail yourself (as the mail administrator), put a forward ...
```

Related Topics

Rule Syntax (on page 232)

Example for Entering Inbound Rules in the Rules.ima file

Enter the following rule into the e-mail domain 's `rules.ima` file:

```
H~(word1|word2|word3)!OR! B~(word1|word2|word3):spambox
```

```
H~(word1|word2|word3)!OR! B~(word1|word2|word3):spambox
```



Note: Replace word 1, word 2, and word 3 with the offensive words you want to search for. The vertical bar represents "or", therefore, this rule will search for word 1, or word 2, or word 3.

If you do not want the user to access spambox because you want to monitor the mail yourself (as the mail administrator), put a forward file in EACH user's folder. This file can be created in Windows Notepad and must match the name of the sub-mailbox you define in your rule. For example, spambox.fwd.

In the spambox.fwd file, only include the e-mail account that you want the filtered message to go to. For example, if you forward the messages to an "abuse" account, your spambox.fwd file will contain the following: `abuse@your-domain.com`.



Important: Notepad adds the .txt suffix to the filename of any newly created file. Make sure you name the text file with the .fwd suffix instead of the .txt suffix.

Example 4 for Entering Inbound Rules in the Rules.ima file

Enter the following rule or rules in the list's `rules.ima` file:

```
B~to be removed from future mailings:NUL
```

```
B~respond with the word "remove" in the subject line:NUL
```

```
B~advertise with bulk email:NUL
```

```
B~bulk friendly:NUL
```

Example for Entering Rules in the Rules.ima File

Example for entering rules in the rules.ima file

The following rule will search the Subject field for baseball or base or bat or cap or homerun or softball and upon a match will send the message to the user's "baseball" mailbox.

S!(baseball|base|bat|cap|homerun|softball):baseball

Example for Entering Outbound Rules in the Orules.ima file

Enter the following rule in the mail domain's `orules.ima` file:

```
H~(word 1|word 2)!OR!B~(word 1|word 2):admin@domain.com
```

Replace word 1 and word 2 with the offensive language you want to search for. This rule sends any outgoing message that contains word 1 or word 2 to an account named `admin@domain .com`.

Sending spam to a specific folder in a user account

You can allow your users to manage their own spam by directing all messages that are identified as spam into a folder for the user account. The user can then delete the ones that are spam, notify you of any false positives, or set up a forward file that will move specific messages into their Inbox.

To create a rule that moves spam into a specific sub mailbox:

1. Make sure that all of the antispam features are setup with the **Insert** X-Header action to be taken when e-mail is determined to be spam. For more information, see *Setting Inbound Delivery Rules for IMail Domains* (on page 202).
2. Click on an e-mail domain's **Inbound Rules** page, then click **Add**. Enter the following rule parameters:

Field: Header

Comparison: Contains

Search Text: X-IMAIL-SPAM

1. Click **Add**. The new rule is added to the list of rules.

Select the rule you just added.

1. On the **Action Type** list, select **Move to Mailbox**.
2. In the **Target** (address) box, enter the mailbox name that you want to send the message to. For example, "Spam".
3. Click **Save**.

Receiving Mailing Lists and Newsletters that are identified as spam

Sometimes, mailing lists and newsletters are identified as spam because they are sent from bulk mailers. If you do not want to place the domain from which a mailing list/newsletter is sent into the trusted addresses list, you can set up a rule to deliver the message anyway. To do this complete the following steps:

If there is already a rule setup to direct spam into a specific user’s mailbox (for example, Spam), you can have the user create a rule as described below:

Look at the header of one of your mailing list/newsletter messages that was identified as spam. Find the X-IMAIL- SPAM line. Copy and paste this entire line into the text area for a rule. For more information, see Setting Inbound Delivery Rules for IMail lists.

Create a Host Rule to Place Spam in a Specific Mailbox for Users

To set up a host rule to place all messages identified as spam in a specific mailbox, *click here* (on page 239).

Creating a User Rule to Place Spam in the Main Mailbox

1. Look at the header of one of your mailing list/newsletter messages that was identified as spam. Find the X-IMAIL- SPAM line. Copy and paste this entire line into the text area for a rule. For example, if a mailing list/newsletter contains the following X-Header : X-IMAIL-SPAM-DNSBL: (fiveten,7799652 ,127.0.0.4), place the entire line into a rule as follows:
2. Make sure that all of the antispam features are setup with the **Insert X- Header** action to be taken when e-mail is determined to be spam. For more information, see Getting to IMail Inbound Rules Options.
3. Click on an e-mail domain's **Inbound Rules** page, then click **Add**. Enter the following rule parameters:

   Field: Header

   Comparison: Contains
4. Search Text: [paste the X-Header from the message]

   Click **Add**. The new rule is added to the list of rules.
5. Select the rule you just added.
6. On the **Action Type** list, select **Move to Mailbox**.
7. In the **Target** (address) box, enter "Inbox". The mailing list/newsletter will be redirected from the "spam" mailbox to the "Inbox" mailbox.



Note: Even though you may set up a rule to deliver a mailing list/newsletter to your Inbox if it matches a black list, this does not mean that the mailing list/newsletter will not be caught by another antispam component. It is possible that occasionally the list will be identified as spam by content filtering because the content is similar to spam. If this happens create another rule with the new X-Header.

8. Click **Save**.

Determining Which Rule Trapped a Message

If a message is trapped by a rule, an X- IMail-Rule line is placed in the message header to allow you to know which rule caught the message. If multiple rules trap a message, only the first 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 not be included in the X-IMail- Rule line when a message is trapped by a negative rule (does not contain or does not equal).

If a domain rule traps the message, the X-IMail-Rule header will be added to all local deliveries. If a message is trapped by a user's rule, the X-IMail-Rule header 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.

Example X-IMail-Rule line:

X-IMail-Rule: S~ Company Newsletter: Newsletter-Monthly Company Newsletter

Rule Section	Explanation
S	If the Subject of the message
~	Contains
Company Newsletter	Rule Text
:	send to
Newsletter	Name of the mailbox to send the message to
- Monthly Company Newsletter	Message text that caused the message to be trapped.

Disabling the X-IMail-Rule Header

If you want to disable the X-IMail-Rule header, so that it does not appear in the message header, you must add an entry to the registry. In the registry, go to HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global and add the entry BlockRuleHdr with a non-zero value. This is a server wide setting and affects all domain and user rules on the server . If BlockRuleHdr is not present or is set to zero, then the X-IMail-Rule header is enabled and will be displayed in the message header.



Notes: The maximum number of characters that will be displayed in the Rule text section of the X-IMail-Rule line is 199.



Tip: The maximum number of characters that will be displayed in the message data section of the X-IMail-Rule line is 30. The Maximum length of any X- IMail-Rule line is 250 characters.

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 same text, then the message will be trapped again.

White List Administration

How to get here

Use **White List Administration** to create a list of IP, domain, and e-mail addresses that can be trusted and upon which no spam tests are performed.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **Apply to Antispam.** Select the check box to compare messages that are identified by content filters to the trusted addresses in the **IP Addresses and/or Address Ranges to Trust** list. Messages received from these trusted addresses will not be processed as spam.
- **Apply Domains/E-mail Addresses to Content Filtering Only.** This option is available only when Apply to Antispam is selected. Select the check box to allow messages from addresses in the **Domains/E-mail Addresses to Trust** list to only bypass content filtering. If this options is cleared, messages from addresses in the Domains/E-mail Addresses list will bypass both content and connection filtering.
- **Apply to Attachment Blocking.** Select the check box to compare messages with attachment blocking settings to the trusted addresses in the **IP Addresses and/or Address Ranges to Trust** list. Messages received from these trusted addresses will not have file attachments blocked.

IP Addresses and/or Address Ranges to Trust

- **IP Addresses.** This column lists the IP Addresses to trust.
- **Net Mask.** This column lists the Address Ranges to trust for the corresponding IP Address /
- **Add.** To add a new IP address to the white list.
- **Edit**. Select address to modify, and click the **Edit** button.
- **Delete.** To delete an existing address from the white list, select the address and click the **Delete** button.

Note: Wild card capability for white list trusted addresses has been added.

Wild Card Examples for Trusted Addresses (on page 243).

Domains and/or E-mail Addresses to Trust

- **Domain or E-mail.** This column lists the Domain or E-mail addresses to trust.
- **Add.** To add a new domain or e-mail address to the white list.
- **Edit**. Select address to modify, and click the **Edit** button.
- **Delete.** To delete an existing domain or e-mail address from the white list, select the the address and click the **Delete** button.

Save. Click to to save your settings. An "Update Successful" message and the time of the update appear.

Related Topics

Expressing an IP Address Range with a Mask (http://technet2.microsoft.com/windowsserver/en/library/ed02cb9b-0637-4b0f-9dc2-8d9571b8960c1033.mspx?mfr=true)

Wild Card Examples for Trusted Addresses (on page 243)

Wild Card Examples for Trusted Addresses

The **Wild Card** capability for trusted domain addresses has been added to minimize multiple domain name that are within the same group. For security purposes this wild card capability requires a minimum of 2 levels to work correctly.

Example 1:

mail1.domain.com mail2.domain.com mail3.domain.com mail4.domain.com	Replace with: ***.domain.com**

Example 2:

work1.mail.domain.com work2.mail.domain.com work3.mail.domain.com	Replace with: ***.mail.domain.com**

Examples that will NOT work:

*.com	Requires a minimum of two levels
*h.domain.com	Not designed with capability to split words

Peer List

How to get here

IMail Server lets you set up "peer" servers to allow users for a specific domain to be spread across multiple physical systems. This can be used when the mail traffic on your IMail Server becomes heavy enough to slow down mail processing. How much traffic your mail server can handle will depend on your system's hardware configuration. See also *How Peering Works* (on page 246).

Peer List displays all IP Addresses of other IMail Servers.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **IP Address**. Displays all IP addresses of other mail servers.

Note: Before you create the peer list, you need to *set up the peer servers* (on page 244). Once set, then see *Creating the Peer List* (on page 244)

Important: The domain alias cannot be a primary domain associated with a particular host. Do not enter IP addresses in the **Domain Aliases** box.

Important: On each of the three computers, make sure that **Default Host** on the **System > System Settings** tab is empty when using peer lists.

Add. Click **Add** to create a new **Peer List (on page 244).**

Edit. To edit a Peer List, first select, then click Edit.

Delete. Select a Peer that you want to delete then click **Delete.**

Related Topics

How Peering Works (on page 246)

Example of Peering (on page 246)

Creating the Peer List (on page 244)

Creating Peer List

How to get here

Before you create the peer list, you need to *set up the peer servers* (on page 244). Once you have done that, you set up the peer list as follows:

1 Enter the IP Address (not a virtual address) of an IMail Server that you want to peer with the current mail server into the text box at the bottom of the Peer List, then click **Add.**
2 Repeat above step until you have added all of the peer servers you want to include.
3 Repeat steps 1, and 2 on each mail domain server that will be used as a peer server.

Important: You do not need to add the local current server's IP address in the peer list. You need to enter only the other peers. *Example* (on page 246).

Note: The server does not have to be restarted after editing the peer list.

4 On each peer mail server, make sure the primary domain (for example, ipswitch.net) is the only entry in the **Domain Aliases** box on the *Domain Properties page* (on page 47). This alias names the primary domain used to send and receive mail.

Important: The domain alias cannot be a primary domain associated with a particular host. Do not enter IP addresses in the **Domain Aliases** box.

Important: On each of the three computers, make sure that **Default Host** on the **System > System Settings** tab is empty when using peer lists.

Related Topics

How Peering Works (on page 246)

Setting Up Peer Servers (on page 244)

Example of Peering (on page 246)

Setting Up Peering

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

1 Install a licensed copy of IMail Server Version 8.1 or later on each computer that will function as a peer mail server.
2 In your Domain Name System (DNS) zone file, add MX records for the peer servers. *Example* (on page 246).
3 In the hosts file on each of the mail servers, make entries for all the other mail servers.
4 On each mail server, use IMail Administrator to *set up the Peer List* (on page 244).

Related Topics

How Peering Works (on page 246)

Creating the Peer List (on page 244)

Example of Peering (on page 246)

How Peering Works

Suppose you have two systems with IMail installed on each system and you set up the two systems as peer servers. Each system has a portion of the user database for a single mail host.

When mail is sent to an e-mail address, the sending server does a DNS lookup to get the mail domain name and address associated with the e-mail address. If the IMail Server that is handling mail for the message is configured for peering, mail comes in for a user on the mail domain and the mail is directed to one of the peer mail 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 mail server. If the user is found in the user database, it forwards the mail. If either peer server is down, the other peer server receives and holds mail until the first server comes back up.



Note: When using peer servers, do not select the **Disable SMTP "VRFY"Command** on the **Services** > **SMTP** tab. Peer servers need to use this command to verify a user that is on the other peer.

Related Topics

Setting Up Peer Servers (on page 244)

Creating the Peer List (on page 244)

Example of Peering (on page 246)

Example of Peering

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 each of the three servers, make the three entries:

- 1.1.1.1 mail1.ipswitch.net
- 2.2.2.2 mail2.ipswitch.net
- 3.3.3.3 mail3.ipswitch.net

On each of the three machines, make sure the domain (for example, ipswitch.net) is the only entry in the **Domain Aliases** box on the *Domain Properties page* (on page 47). This alias names the primary domain used to send and receive mail.

Important: The domain alias cannot be a primary domain associated with a particular host. Do not enter IP addresses in the **Domain Aliases** box.

Important: On each of the three computers, make sure that **Default Host** on the **System > System Settings** tab is empty when using peer lists.

CHAPTER 7

Anti-virus

The IMail Administrator Help covers both versions of the IMail Anti-virus.

Please select the Anti-virus solution that is installed on your system.

In This Chapter

IMail Antivirus powered by BitDefender - Settings 249
IMail Anti-virus powered by Symantec - Settings 252

IMail Antivirus powered by BitDefender - Settings

How to get here

IMail Anti-virus powered by BitDefender®

Important for Upgraders. New automated features for virus definition updates have been added and enabled. Be aware that any manual schedule that has been previously setup will continue run.

Tip: It is up to the IMail Administrator to disable any manual schedules that were previously set.

`"AVUpdate.exe"` is no longer required to update your virus definitions with IMail Server v11.01 or later. Queue Manager has been enhanced to handle all the virus definition updates without requiring a service restart.

BitDefender® Settings

- **Enable Virus Scanning.** Select this option to have the IMail Anti-virus Server scan messages for viruses.

Note: Virus scanning can be enabled/disabled per domain on the *Setting Domain Properties page* (on page 41).

- **Repair Infected Files.** Select this option to attempt to repair a mail message that is infected. The infected portion is removed and a new file is created containing the repaired message. The initial infected file is deleted.
- **Enable Automatic Updates** (On by default). New installs and upgrades this option is enabled. This setting controls the automatic scheduling for downloading virus definition updates.

Important: It is recommended to keep your Automatic Updates enabled to keep your virus definitions up to date.

  - **Run Update Every 4 Hours** (Set to 4 by default). Select how often you would like to check for BitDefender® definition updates.
- **Subscription Days Remaining**. Number of days left before your license expires.
- **Last Updated**. Date/Time of last BitDefender® virus definition update.

Note: This is the date/time of the last virus definition update that was available for download from BitDefender®. See the following registry key to see the last date/time an update was checked: `HKLM\Software\Ipswitch\IMail\Global\BitDefLastCheck`

- **Update Now.** This button will manually check for a virus definition update.
- **Infected File Actions** that occur if IMail Anti-virus Server is unable to repair an infected file. The action also occurs if the **Repair Infected Files** option is cleared.
  - **Delete File.** Does not deliver the message and deletes it from the spool directory.
  - **Bounce Message.** Sends a bounce message back to the sender informing him/her that the message was not delivered.
  - **Redirect Message.** The infected message is redirected to the address entered into the **Redirect Address** box.
- Enable either of the following notifications that will be sent for infected messages:
  - **Alert Administrator.** Select this option to send one e-mail (per infected message) to the e-mail address entered in the **Alert Address** box. The e-mail that is sent to the administrator contains the following information: sender, intended recipient, message ID, subject, virus detected, and the action taken.
  - **Alert Recipients.** Select this option to send an e-mail to the intended recipients informing them that the message was redirected or deleted.

Other Options

- **Definition Path.** Directory name where BitDefender definitions are located. This folder is under the IMail directory by default.

- **Update URL.** The URL for BitDefender updates. AVupdate.exe will run automatically per the set schedule above.
- **Redirect Address.** If you set the **Infected File Action** option to **Redirect Message**, enter the address where you want the infected messages to be sent.



Tip: You may want to set up a mailbox specifically for use with this option

- **Alert Address.** If the **Alert Administrator** option is selected, enter an address in which you want to receive e-mail messages with details about infected files.

Save. Click **Save** to save your settings. An "Update Successful" message and the time of the update appear.

Related Topics

Overview of IMail Anti-virus powered by BitDefender® (on page 251)

Logging for IMail Anti-virus powered by BitDefender® (on page 252)

Overview of IMail Anti-virus powered by Bitdefender®

IMail Anti-virus powered by BitDefender® is equipped with cutting-edge proactive B-HAVE technology that represents the last minute alternative for advanced protection against malware. B-HAVE relies on a dynamic heuristic scanner especially engineered and designed to improve and enhance the current security technology, while also overcoming the architectural limitations inherent in many other dynamic solutions.

B-HAVE creates a virtual, isolated and self-contained computer, mimicking your system configuration. This environment represents the ideal location for applications' and files' threats investigation, because it ensures your computer is exposed to absolutely zero risk.

Bitdefender® is one of the most comprehensive virus scanners available, and with its integration into IMail Server, you can be sure that your mail server will not be compromised. IMail Anti-virus powered by BitDefender® works with IMail Server to find and repair infected messages before they get to your mail customers. IMail Anti-virus powered by BitDefender® searches all incoming and outgoing mail for viruses, worms, trojan horses, and other destructive code. It does this by comparing all mail messages with a list of known virus definitions.

If IMail Anti-virus powered by BitDefender® for IMail Server detects a virus, it can attempt to repair the infected file, delete the message, or bounce the message back to the sender.

Related Topics

IMail Anti-virus powered by BitDefender® - Settings (on page 249)

Logging for IMail Anti-virus powered by BitDefender® (on page 252)

Logging for IMail Anti-virus powered by BitDefender

IMail Anti-virus log for BitDefender® is named `"AVUpdate.log"` located in (default setup):

```
c:\Program Files\Ipswitch\IMail\
```

"AVUpdate.log" sample log:

Logs Date / Time when `"AVUpdate.exe"` is started

Time Stamp - Checking for Updates

Time Stamp - Updates found, stopping Queue Manager and SMTPD32

Time Stamp - Installing updates

Time Stamp - Starting Queue Manager and SMTPD32

Time Stamp - Update complete

Note: `"AVUpdate.log"` is a single file that constantly appends to itself. It is up to the IMail Administrator to move it to a backup folder, and clear the current log.

Related Topics

Overview of IMail Anti-virus powered by BitDefender® (on page 251)

IMail Anti-virus powered by BitDefender® - Settings (on page 249)

IMail Anti-virus powered by Symantec - Settings

How to get here

IMail Anti-virus powered by Symantec™

Select the following options to configure the anti-virus server.

- **Enable Virus Scanning.** Select this option to have your IMail Anti-virus powered by Symantec™ Server scan messages for viruses.

Note: Virus scanning can be enabled/disabled per domain on the *Setting Domain Properties page* (on page 41).

- **Repair Infected Files.** Select this option to attempt to repair a mail message that is infected. The infected portion is removed and a new file is created containing the repaired message. The initial infected file is deleted.
- **Pass File by Name.** If IMail Anti-virus is installed on the same computer as IMail, select this option to increase performance. If IMail Anti-virus is installed on a remote server, do not select this option.
- Select one of the following **Infected File Actions** that occur if your IMail Anti-virus powered by Symantec™ Server is unable to repair an infected file. The action also occurs if the **Repair Infected Files** option is cleared.
  - **Redirect Message.** The infected message is redirected to the address entered into the **Redirect Address** box.
  - **Bounce Message.** Sends a bounce message back to the sender informing him/her that the message was not delivered.
  - **Delete File.** Does not deliver the message and deletes it from the spool directory.
- Enable either of the following notifications that will be sent for infected messages:
  - **Alert Administrator.** (on page 255) Select this option to send one e-mail (per infected message) to the e-mail address entered in the **Alert Address** box.
  - **Alert Recipients.** Select this option to send an e-mail to the intended recipients informing them that the message was redirected or deleted.

Other Options

- **Server IP Address.** Enter the IP address of the computer that IMail Anti-Virus Server is installed on.
- **Server Port .** Enter the port that you want IMail Anti-virus Server to run on. The default port is 7777.



Note: If you change the IP Address or port number after installation, you must change them in the configuration file (`symcscan.cfg`).

- **Redirect Address.** If you set the **Infected File Action** option to **Redirect Message**, enter the address where you want the infected messages to be sent.



Tip: You may want to set up a mailbox specifically for use with this option

- **Alert Address.** If the **Alert Administrator** option is selected, enter an address in which you want to receive e-mail messages with details about infected files.

Save. Click **Save** to save your settings. An "Update Successful" message and the time of the update appear.

Related Topics

Overview of IMail Anti-virus powered by Symantec™ (on page 254)

Overview of IMail Anti-virus powered by Symantec

IMail Server is equipped with state of the art anti-virus technology to provide increased security for your mail system. Symantec's ScanEngine is one of the most comprehensive virus scanners available, and with its integration into IMail Server, you can be sure that your mail server will not be compromised.

IMail Anti-virus powered by Symantec™ searches all incoming and outgoing mail for viruses, worms, trojan horses, and other destructive code. It does this by comparing all mail messages with a list of file extensions and known virus definitions.

It also uses heuristic technology to discover new viruses by searching for general characteristics of existing viruses. If it detects a virus, IMail Anti-virus powered by Symantec™ can attempt to repair the infected file, delete the message, or send a bounce message back to the sender. A log file entry is generated and an e-mail is sent to alert the administrator of the problem. In addition, the System Administrator can set a "Redirect Address" to which infected e-mail messages are sent. Optionally, the administrator can send a message to the intended recipients informing them that the message could not be delivered.

Anti-Virus Administration (Symantec)

You can administer IMail Anti-virus powered by Symantec™ from:

- **IMail Administrator.** Click the IMail Administrator **Anti-Virus** tab. The Anti-Virus Settings page opens. Use this page to enable virus scanning, set actions on infected files, configure the anti-virus server IP address and port (Symantec™ AV only), and redirect infected messages/files and alert e-mail addresses.
- **Symantec™ Anti-Virus Scan Engine Web Administrator.** You can access Symantec's Scan Engine protocols and administration settings through Symantec™ Anti-Virus Scan Engine Web Administrator. You can access the Scan Engine Web Administrator at the address entered in the **Server IP Address** on the *IMail Anti-virus powered by Symantec™ - Settings* (on page 252) followed by :8004 (the default port for the Scan Engine Web Administrator). For example, http://123.100.100.80:8004

  -OR-

  by clicking the **Symantec™** icon on the **Anti-Virus Settings** page. The default password for the Scan Engine Web Administrator is `"admin"`.

You can customize a number of anti-virus settings in the Anti-Virus Scan Engine Web Administrator such as:

- HTTP bind address for the IMail Anti-Virus powered by Symantec™ Server
- HTTP port number that the IMail Anti-Virus powered by Symantec™ Server runs on
- Scan Engine Web Administrator password
- Type of information to log

For more information, click **Help** in the Symantec™ Anti-Virus Scan Engine Web Administrator.

Related Topics

Updating Symantec™ Virus Definitions (on page 255)

Enabling Anti-Virus Logging (on page 255)

Alert Administrator Email

The e-mail that is sent to the administrator contains the following information: sender, intended recipient, message ID, subject, virus detected, and the action taken.

Updating Symantec Virus Definitions

By default, Symantec™ LiveUpdate connects to the Symantec Web site to update the virus definitions every 2 hours. You can also use the *Symantec™ Anti-Virus Scan Engine Web Administrator* **(on page 254)** to manually update virus definition updates or schedule virus definition updates to a specified time interval.

Note: You can view the date of the last virus definition file date on the *Symantec™ Anti-Virus Scan Engine Web Administrator* **(on page 254) on the LiveUpdate page**.

Enabling Symantec Anti-virus Logging

IMail Anti-virus Server logs error messages and files to the Windows Application Event Log. However, logging is not enabled by default. If you want IMail Anti-Virus Server to log error messages, you must enable logging in *Symantec™ Anti-virus Scan Engine Web Administrator* **(on page 254).**

To log events to the Windows Application Event Log:

1. On the Symantec™ Anti-Virus Scan Engine administrative interface, in the left pane, click **Monitors**.
2. On the **Windows Logging** list, select the appropriate logging level. The default logging level for the Windows Application Event Log is **None**.
3. To save your settings click on the save image located at the top left of the page:



4. For your changes to take effect be sure the service is restarted.

Related Topics

Viewing Log Files (on page 256)

Viewing Anti-virus Log Files

IMail Anti-virus Server logs to the Windows Event Viewer.

To view the Windows Log:

1. Open the Event Viewer (located in the Windows Control Panel, under Administrative Tools).
2. Under Log, click **Application**.
3. Click any CarrierScan Server event listed in the Application Log to view that log entry.

Error Codes in the SMTP Log

The table below contains possible error codes that will be used to identify failures in the IMail Anti-virus scanning process. These error codes appear in log lines contained in the IMail SMTP Log.

Error Codes	
1	Failed to connect to IMail Anti-virus server.
2	A problem was encountered reading the file to be scanned.
3	The scan was aborted abnormally.
4	Function was called with an abnormal parameter.
5	Error occurred when attempting to receive repaired file
6	Memory allocation occurred.
7	Server could not access the file to be scanned. **Note**: This error usually occurs for local scans when file permissions are set incorrectly or when the file is not in the path specified in the LocalFileScanDir parameter on the server.
9	The attempted repair failed. The message will be treated as an infected file.
15	You do not have a valid license for IMail Anti-virus. Scanning will abort.

Example Log Lines with Error Codes

08:23 10:39 SMTP-(00000164) Failed to initialize Virus Scanner, code=1

08:23 16:28 SMTP-(0000012E) Error From Virus Scanner, code=1

Understanding Anti-virus Entries in the Mail Queue

An anti-virus entry type has been added to the queue file for SMTP32. This entry line helps to identify the status of the virus scan for a particular message. The line will have

a V in the first column, followed by a 1 or a 0. The following chart displays the possible queue entries regarding the anti-virus.

V1	Message has already been scanned.
V0	Message needs to be scanned.
No entry	Message needs to be scanned.

List Server Interaction

Since IMail Anti-virus scans all incoming and outgoing mail messages, special provisions apply concerning the list server. Normally, IMail Anti-virus would unnecessarily scan a list server message twice, once when the message comes in, and another time when the list server sends the message to the list. This would slow down the processing time.

Therefore, all messages destined for a list are marked as scanned (V1) before they are handed over to the list server. If you look in the queue at a list server message, it will always be labeled V1 (see chart above), no matter what stage the message is in. This tells IMail Server to skip the second scan since the file cannot be infected.

CHAPTER 8

Antispam

In This Chapter

Antispam Overview 259
Server Level Antispam Options (Black Lists) 270
Spam Filtering (Domain Level) 279
Using Antispam Log Entries 317
Antispamseeder Utility 333
Troubleshooting 349

Antispam Overview

IMail standard edition includes standard antispam technology; IMail Premium includes Premium Antispam as well as Standard Antispam technology.

Premium Antispam

Commtouch Advanced Security Daemon (a.k.a. ctasd™) a plug-and-play email-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. The daemon adds a layer of e-mail filtering to your mail delivery system in order to provide real-time classification, already in the first minutes after a new outbreak is launched.

Commtouch's GlobalView™ Mail Reputation Service fights unwanted mail at the perimeter, reducing more than 85% of incoming messages at the entry-point, before these messages enter the network. Additionally, GlobalView can optimize traffic flow so that legitimate sources gain optimal access, while unauthorized sources attempting to abuse the network are blocked.

Standard Antispam

All IMail products include standard antispam features. These features are custom configured by the administrator to identify spam and prevent it from clogging your Inbox. Mail messages are passed through several layers of filters and tests to assure that maximum spam detection is achieved.

What You Can Do with the Antispam Features

- Use the *Premium Antispam filter* (on page 280) (optional only with IMail Premium) to automatically manage spam protection. Premium Antispam filter settings are applied before Standard Antispam filter settings.
- Enable *statistical filtering* (on page 284) (content filtering) to analyze each message and determine if it is spam.
- Use *phrase filtering* (on page 289) (content filtering) to configure a phrase list that searches for specific spam phrases within the subject and body of e-mail messages.
- Enable *HTML feature filtering* (on page 291) to search messages for HTML tags that could be used to disguise spam.
- Create a *URL Domain Black List* (on page 299) that searches for domain names (URLs) contained within HREF and IMG SRC HTML tags and in plain text messages.
- Enable *broken MIME header* (on page 301) filtering to treat e-mails with malformed MIME headers as spam.
- Use the *Sender Policy Framework (SPF)* (on page 303) feature to increase the ability to stop incoming e-mail from forged e-mail addresses (spoofed e-mail).
- Use *connection filtering* (on page 274) to compare e-mail messages against configurable DNS black lists to determine if they are from IP addresses that are known to send spam.
- Create a *white list (trusted addresses)* (on page 242) of e-mail addresses, domains, and subnet masks that bypass content filtering.
- Enable *verification checks* (on page 274) (connection filtering) to verify the "Mail FROM" address, HELO/EHLO domain information, and perform a reverse DNS lookup on incoming e-mail messages.
- Configure *delivery rules* (on page 220) to trap messages based on spam X-Headers that are inserted when a mail message fails a spam test.

Which Antispam Settings are Used to Check a Message?

The antispam filters used to scan a message are determined by the IMail domain settings of the IP address that the message is received on. If the message is received on an IP address that is not configured for IMail, the primary domain's antispam filter settings are used.

Spam Actions

If a message is identified as spam, you can set IMail Server to delete it, send it to an e-mail address, or insert an X-header in the message to identify which spam test it failed. You can also create delivery rules to search for the spam X-Headers and process the message accordingly.

Accessing the Antispam Features

The Antispam options are accessed from two levels: the *server level* (on page 89) and *domain level* (on page 182).

Related Topics

Antispam Configuration Overview (on page 262)

Types of Antispam Filters

Sender Policy Framework (SPF) Filtering

SPF extends the Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) so mail servers do not accept e-mail unless the sending computer is designated as a legitimate e-mail sender. This feature enables administrators increased capability to stop incoming e-mail from forged e-mail addresses.

Premium AntiSpam (on page 280)

The optional Premium Antispam filter provides automated spam protection in addition to the Standard Antispam filter included in IMail. You can select actions to take if a message is determined to be spam.

HTML Filtering (on page 291) (Content Filtering)

HTML filtering examines only the HTML portions of an e-mail message, and is comprised of 3 components: an *HTML parser* (on page 292), *HTML Feature filtering* (on page 291), and a URL Domain Black List. The HTML parser is part of the antispam engine that examines the HTML sections of a message. It extracts the text from HTML tags, and passes the text on to the phrase and statistical filters for examination. The HTML Feature filter allows you to specify which HTML tags you want to consider spam indicators. The URL Domain Black List searches for domain names that occur in the URLs of HTML messages.

Phrase Filtering (on page 288) (Content Filtering)

Phrase filtering searches for common spam phrases within the body and/or subject of an e-mail message and identifies the message as spam. Phrase filtering can be enabled/disabled per domain, and works independently of statistical filtering. For more information see *Phrase Filtering* (on page 288).

Statistical Filtering (on page 283) (Content Filtering)

Statistical filtering examines each word in the body of an e-mail and evaluates whether the word is a statistical indicator of spam. The entire message is then evaluated based on the combined *word counts* (on page 349) to determine whether it is likely to be spam. You can create a host specific exclude list, specify what action to take when a message is identified as spam, and specify whether to use the primary domain's word counts or create new ones. For more information see *Statistical Filtering* (on page 283).

A list of words that are not included to determine whether a message is spam. The words in the exclude list are words that have an equal chance of being non-spam as spam. For example, "Mortgage" is a term frequently used in spam. However, if you work

in the financial industry, this term may appear frequently as non-spam. In such a case, you can enter the word "mortgage" into the exclude list. The exclude list should also include common words like proper names. The exclude list is stored in the `exclude-list.txt` file located in the mail domain 's directory.

Attachment Blocking Filtering (on page 227)

Attachment blocking filtering lets administrators specify types of file attachments to block from e-mail messages and actions to take on blocked messages. Attachments can be blocked based on message MIME types and filename types. In addition to selecting the types of message attachments to block, you can define actions to take on blocked messages.

Broken MIME Header Filtering (on page 301)

The Broken MIME Header filter identifies Broken MIME header characteristics that result in SPAM e-mail. You can also define actions to take when Broken MIME headers are identified as SPAM e-mail.

Delivery Rules (on page 220)

You can use domain and user delivery rules to process messages based on the spam X-Headers which are inserted when a message fails a spam test. For more information see *Using Delivery Rules to Filter Mail* (on page 220).

Antispam Configuration Overview

The following topics explain the basic tasks you must complete to configure the IMail Server antispam features. Completing each of these steps establishes your unique spam signature, which determines how IMail Server handles spam. After these tasks are completed, your server will be protected from spam. Also, after you complete the basic setup tasks, you may want to read the Advanced Statistical Filtering topic to learn about other ways to configure the antispam features.

Basic Setup Tasks

To set up the basic antispam configuration, complete the following steps:

Server Configuration:

Configure DNS Black Lists for the Server (on page 277)

Configure Logging Options (on page 319)

IMail Server Domain Configuration:

Configure Connection Checks (on page 274)

Configure SPF Filtering (on page 303)

Configure Premium Antispam (optional) (on page 280)

Configure Content Filtering (on page 303)

Configure HTML Filtering (on page 291)

Configure Broken MIME Header Filtering (on page 301)

Enter White List (Trusted Addresses) (on page 242)

About Your Spam Signature

All of the antispam features that you have configured for IMail Server are collectively referred to as your spam signature. It consists of your specific configurations for:

- White lists (trusted IP, domain, and e-mail addresses)
- DNS black lists
- Verification checks
- Sender Policy Framework (SPF)
- Premium Antispam
- Phrase filtering
- Statistical filtering
- HTML feature filtering
- URL domain black list filtering
- Broken MIME header configuration

If you have too many false positives or are not catching enough spam, you may need to adjust your spam signature.

IMail Antispam Processing Order

The following steps indicate the order in which each antispam component performs, assuming that all default options and settings are not altered after installation. Several things can change this order, such as enabling/disabling the "Content Filtering for Authenticated Users" and "Apply Domains/EMail Addresses to content filtering only" options, but for the most part messages are processed as follows:

1 **White List (on page 242) (Trusted Addresses)**. IMail checks the **Apply to Antispam** option. If this option is enabled, then the IP address (and address present in the MAIL FROM command) for an incoming message is compared against the white list to see if there is a match. If there is a match, all other antispam checks are skipped. However, if the IP address (or MAIL FROM address) does not match, the message is compared against the **DNS Black Lists** (on page 110).



Note: If the **Apply Domains/EMail Addresses to Content Filtering Only** option is enabled (on the **White List** page), then DNS Black Lists, Verification Tests, and **SPF**[89] checks are performed against the message; even if the address in the MAIL FROM command is present on the **White List** page.

2 **Connection Checks** (on page 274). **IMail Server** initiates connection filtering to compare a message's sender information against configured DNS black lists. If the message matches a black list, it is processed according to whether the black list is a "trusted" or standard black list. If the message does not match a black list, verification checks are performed.

3 **Verification checks** (on page 274). If enabled, verification tests are performed to verify the "Mail FROM" address, the HELO/EHLO domain, and a reverse DNS lookup is performed. If a message passes all the checks, content filtering is performed. If a message does not pass all checks, an X-Header is inserted into the message or the message may be deleted. SPF checks are performed next.

4 **SPF Filtering** (on page 303). The SPF feature provides increased capability to stop incoming e-mail from forged e-mail addresses. Using a sender authentication scheme, a domain owner requires that legitimate messages from a domain must meet certain SPF criteria. Messages that do not meet the criteria are not accepted as a legitimate e-mail messages and are processed according to the SPF options selected on the **SPF** tab.

5 **Trusted Domains/Email Addresses** (on page 242) (on the **White List** page). If the **Apply to Domain/EMail Addresses to Content Filtering Only** option is selected, IMail Server checks whether the connecting SMTP server's Domain/EMail address is listed in the **Domain/EMail Addresses** list. If it is listed, the content is not scanned further with content filtering.

6 **Premium Filter** (on page 280). The Premium Antispam filter (optional in IMail Premium only) provides automated spam protection in addition to the Standard Antispam filter included in IMail. If a message does not pass the Premium Antispam filtering, actions selected are applied before Standard Antispam filter settings.

7 **Broken MIME Header** (on page 301). If enabled, the filter identifies broken MIME header characteristics that may be present in SPAM e-mail. You can define actions to take when broken MIME headers are identified in SPAM e-mail. If it is not filtered as a broken MIME header, the message is passed on to either HTML filtering or phrase filtering, depending on whether it contains HTML code.

---

[8] How to get here IMail uses Sender Policy Framework (SPF) to extend the Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) so IMail Server does not accept e-mail unless the sending computer is designated as a legitimate e-mail sender. This feature provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.To accomplish this e-mail security measure, SPF establishes a policy framework and a sender authentication scheme that verifies ...

[9] The Sender Policy Framework (SPF) pageprovides administrators increased capability to stop incoming email from forged (spoofed) email addresses. Use the SPF settings to configure how to process email that is identified as forged email. Settings on the SPF page apply to the selected domain.Enable SPF. Select this checkbox to enable the SPF filter for the current host. Default actions are specified to take for each SPF query result. You can, however, change the defaults by clicking the hyperlink u ...

8 **HTML Feature Filtering** (on page 291). The HTML content filtering occurs during the Phrase Filtering and Statistical Filtering process. If HTML filtering is enabled, the message is examined to determine if it contains HTML code. If it does, the message undergoes **HTML Content Filtering** (on page 291). If the message does not contain HTML components, Phrase Filtering and Statistical Filtering continue to evaluate the message.

- **Feature Filtering.** When a message with HTML code is evaluated, it is compared against the **Feature Filtering** (on page 291) options to detect certain HTML code components that may be present in the message. If the selected HTML code components are present, selected actions are taken on the message.
- **URL Domain Black List.** When a message with HTML code is evaluated, it is also compared against the **URL Domain Black List** (on page 299) to search for domain names that may be present in the message URL links. If a URL that is identified in a message matches a domain name included in the URL Domain Black List, selected actions are taken on the message.

9 **Phrase Filtering** (on page 289). If phrase filtering is enabled, the message is checked to determine if it contains phrases that are in the **phrase list**. If the message passes, it is processed according to the settings for phrase filtering. If the message does not pass, it is processed by statistical filtering.

10 **Statistical Filtering** (on page 284). If statistical filtering is enabled, the message is compared against the spam and non-spam word counts to determine if it is statistically likely to be spam. If it is identified as spam, it is processed according to the settings for statistical filtering. If the message is not identified as spam, it is delivered.

For information on how these antispam components integrate into IMail Server mail processing, see **IMail Server Processing Order** (on page 27).

Installing Updated Antispam Files

Ipswitch maintains several files that are available for download from our website, including an antispam-table.txt file, phrase-list.txt file, and a spamblkm.txt file. These files provide you with updated spam information and are also useful for reverting back to the default configurations. You can download these files from the following locations:

- *ftp://ftp.ipswitch.com /Ipswitch/Product_support/IMail/antispam.zip* ftp://ftp.ipswitch.com/Ipswitch/Product_support/IMail/antispam.zip
- The IMail Ipswitch Support Center at the following location: *http://www.imailserver.com/Support* (http://www.imailserver.com/Support/).

Explanations of Files

- **Spam and Non-Spam Word List** (**antispam-table.txt**)

  Ipswitch continuously updates the antispam-table.txt file in order to keep up with spammers. As we collect new spam statistics, it is integrated into the existing antispam-table.txt file, and the file is then made available to users.

- **List of Default Black Lists** (**spamblkm.txt**)

This is a list of the default black lists used in IMail Server.

- **Sample Phrase List** (**phrase-list.txt**)

  The sample phrase list is provided to assist you in setting up phrase filtering. You may want to examine this file before enabling it in to assure that all of the phrases are suitable for your needs.

- **Sample URL Domain Black List** (**url-domain- bl.txt**)

  The sample URL Domain Black List is provided to let you enable and run the URL Domain Black List feature with minimal effort. The URLs contained in this list are ones that we have collected from spam e-mail. You may want to examine this file before enabling it, to assure that you agree with the domain names that it contains.

Forwarding Spam to CommTouch

The Premium Spam Filter performance can be improved when users forward spam e-mail to Ipswitch. Ipswitch provides the spam mail to Commtouch Advanced Security Daemon (ctasd™) editors to review the spam submission and add spam signature information to it. Then the signature is published to the global database to help other users eliminate spam. For maximum protection, this global database is updated on your IMail Server every few minutes.

Reporting e-mail that is spam to CommTouch:

1. Obtain the message as it was originally received.
2. Send the message as an attachment to **reportfn@blockspam.biz** (mailto:reportfn@blockspam.biz) with the following subject line:
   `[FN Report][Messaging Architects][Date]`



Note: Only the Date tag should be modified. **Example:** `[FN Report][Ipswitch][mm/dd/yyyy]`

Reporting False Positives (Legitimate mail flagged as spam)

1. Submissions must contain the Commtouch `"RefID"` from the header of the message. You can forward the original message as an attachment (`"RefID"` header line included) or retrieve the `"RefID"` and put it in the body of your submission. It is ok to send more than one `"RefID"` per message.

   Header line example:
   `X-CTCH-RefID: str=0001.0A010208.492285A9.0064,ss=4,pt=62280,fgs=12`

2. Send the message to **reportfp@blockspam.biz** (mailto:reportfp@blockspam.biz) with the following subject line:

   `[FP Report][Ipswitch][Date]`



Note: Only the Date tag should be modified. Ex: [FP Report][Ipswitch][mm/dd/yyyy]

Important: This process is only intended for messages that were improperly flagged by Commtouch Premium Antispam. If the message was flagged by other IMail spam filters you must manually adjust the filter to prevent further false positives.

Forwarding Spam Messages (Example)

To forward spam messages, enter an e-mail address in the form of user@domain.com . If the address is located on the same domain, you can omit the domain and only enter the User ID.

Important: If you have chosen the **Forward To** option, be aware of the **Default Max Mailbox Size** limit set in the *Domain Properties* (on page 41). If you receive a large quantity of spam, this limit could be exceeded for the mailbox that stores spam. Make sure that you delete messages from this mailbox on a regular basis. You may also want to set up a **Full Mailbox Notify Address** for e-mail to be sent to when a mailbox is almost full. For more information, see *Setting Domain Properties* (on page 41).

If you want the spam to be sent to a mailbox, place a hyphen between the user and sub-mailbox name, such as root- spam@domain.com. If the account is located on the same mail domain, you can omit the domain and enter root-spam.

Important: If you enter an address with a sub-mailbox that does not exist, the sub-mailbox is created only if **Create** is selected in the **Sub-Mailbox Creation** options of the Domain Properties. For more information, see *Setting Domain Properties* (on page 41).

Antispam FAQs

Will the antispam features slow down mail processing?

Under normal circumstances, the antispam features will not impact mail delivery. However, the verification options may slow down the server, as they are resource intensive.

How does the antispam engine interact with IMail Anti-Virus?

IMail Anti-Virus complements the antispam features of IMail Server. Connection filtering and verification for antispam are completed first, followed by the Anti-Virus scan. Then, the other antispam processes are initiated, beginning with content filtering. See also *IMail Processing Order* (on page 27).

What can I do if legitimate mail is identified as spam?

You can place the e-mail address or domain name, from which the message was sent, in the *white list (trusted addresses)* (on page 242) to always let messages from the e-mail address or domain name to be delivered.

If a small number of messages are being misidentified, you can use the *antispamseeder.exe* (on page 333) utility to add the messages to the antispam-table.txt file. This will increase the likelihood that similar messages will be correctly identified in the future.

If a large number of legitimate mail is being identified as spam, modify the Advanced Options on the Statistical Filter page. Begin by increasing An e-mail is spam when it's calculated probability exceeds option to 95%. If that has no effect, decrease The Probability a new word is spam option to 10%. See Also Advanced Statistical Filtering.

How do I know if the black lists are accurate?

The black lists used are not maintained by Ipswitch, therefore we cannot verify their accuracy. Some black lists are updated more frequently than others, and contain more accurate information. You should be aware of this especially if you decide to configure your own black lists. For your convenience, IMail Server allows you to identify trusted black lists. These are black lists that you have tried and found to be accurate.

Where does Spam go?

By default, messages that are identified as spam are forwarded to a mailbox called "bulk" within the root account. If you have changed the "Forward To" setting, on any of the antispam filter pages, then spam goes to the address that is entered in this field.

How do I access the Antispam features?

Only system and domain administrators can access the antispam tabs. System administrators have access to the server level DNS black lists and logging tabs. Host administrators have access to the host level DNS black lists, connection filtering, statistical filtering, phrase filtering, and Trusted DNS Black Lists.

The antispam tabs can be accessed from two places: the server level and host level. To access the server DNS Black Lists page, mouse over the **IMail Administrator System** tab, then click **DNS Black Lists**. The DNS Black Lists page opens.

To access domain (host) level settings, click the IMail Administrator **AntiSpam** tab. The AntiSpam Settings page opens. The domain level antispam options are displayed on the **Domain Level Spam Filtering** page.

Will the antispam features affect mailing list subscriptions?

Most mailing list subscriptions will not be identified as spam. However, to ensure that mailing list messages are not identified as spam, place the domain name from which the mailing list is sent in the Trusted Addresses list. For more information, see *Creating Trusted DNS Black Lists* (on page 277).

If you do not trust the domain, you can create a host rule to send the message to a folder for the user (for example, spam), and the user can create a user rule that puts the message in his/her Inbox. For more information, see *Using Delivery Rules to Filter Spam* (on page 220).

Do the antispam features work with Web Messaging?

Yes. IMail Server processes mail from IMail Web Messaging in the same way it processes all other mail.

Do I need to use the Antispamseeder.exe utility to alter my word counts?

The file, that ships with the product, is appropriate for most users. However, you may need to alter this file if we have identified words as spam that you do not consider to be spam, or vice versa. For example, the word "mortgage" is identified as spam because in our tests, it occurred 364 times in non-spam, and 7516 times in spam. However, at financial institutions, the word "mortgage" is a non-spam word that occurs frequently. In this case, you need to alter the antispam-table.txt file so that statistical filtering recognizes the word "mortgage" as non-spam. For more information, see *Customizing a Host's Antispam-table.txt file* (on page 342).

Will the antispam features prevent my users from sending spam?

The antispam engine automatically filters mail from all users who are not authenticated. If you are concerned about your authenticated users sending spam, you can prevent this by selecting the Enable content filtering for authenticated users option located on the *Domain Level Spam Filtering* (on page 182) page. By doing this, outgoing mail from authenticated users is always evaluated to determine whether it is spam.

Authenticated users are users who have SMTP Authentication enabled on their e-mail client or users who send mail from IMail Web Messaging. By default, IMail Server forces users to authenticate, unless you select another option such as **Relay Mail for Anyone** or **Relay Mail for Addresses** in the **Mail Relay Settings** located under **Services** tab > **SMTP**. This means that every time a user connects to the IMail Server, he/she must enter his/her user ID and password.

Should I place a domain name in the phrase list or in the URL Domain Black List?

Each location serves a different purpose. The phrase list filters the domain name as it appears in normal text in the body of an e-mail message. The URL Domain Black List will filter the domain name if it appears as a link in HTML code within a message, specifically within HREF and IMG SRC tags.

Server Level Antispam Options (Black Lists)

You can separate DNS black lists into two categories: standard DNS Black Lists and trusted DNS Black Lists. A trusted DNS black list is one that you know is updated frequently, and is more likely to be accurate. You may also identify a black list as trusted because you find that for your uses it produces the least number of false positives. If a message matches one of these black lists, it is automatically deleted.

A standard DNS black list is a black list of which you are uncertain about its accuracy. If a message matches one of these lists, an X-Header is inserted into the message, indicating which black list it matched.

Related Topics

How Black Lists Work (on page 91)

Understanding DNS Black Lists (on page 90)

Server Level DNS Black Lists (on page 89)

Understanding DNS Black Lists

What is a DNS Black List?

DNS black lists are databases of known spammers. These databases contain IP addresses that are known to send spam. They also contain IP addresses that have open mail relays, because a spammer can easily use these systems to send out spam.

How IMail Server Uses DNS Black Lists

IMail Server uses DNS black lists during connection filtering. In order to fully understand how antispam and connection filtering work, it is necessary to understand DNS black lists. Connection filtering compares each message against the configured DNS black lists to see if the IP address of the connecting server is listed. If the result is positive, the message is either deleted or an X-Header is inserted into the message.

"Standard" and "Trusted" DNS Black Lists

You can separate DNS black lists into two categories: standard DNS Black Lists and trusted DNS Black Lists.

A trusted DNS black list is one that you know is updated frequently, and is more likely to be accurate. You may also identify a black list as trusted because you find that for your uses it produces the least number of false positives.

Warning: If a message makes a match on the **Trusted Black List**, it is automatically **deleted**.

A standard DNS black list is a black list of which you are uncertain about its accuracy. If a message matches one of these lists, an X-Header is inserted into the message, indicating which black list it matched.

Configurable for Each Host

DNS black lists are configurable for the entire server, which enables a system administrator to decide which DNS black lists are available to each domain. Each domain administrator is then responsible for enabling the configured black list for the domain. A domain cannot use a black list that is not configured and enabled for the server.

Related Topics

Server Level Antispam Options (Black Lists) (on page 270)

How Black Lists Work (on page 91)

Server Level DNS Black Lists (on page 89)

Trusted Black Lists (on page 277)

Add/Edit the DNS Black List (on page 92)

How Black Lists Work

DNS black list databases contain a list of IP addresses that are known to send spam. They also contain IP addresses that have open mail relays, because a spammer can easily hijack these systems to send out spam. Each black list has different reasons for why an IP address is blacklisted. Among the more common reasons are: dialups, bulk mailers, spammers and open relays.

Categorizing IP Addresses in Separate Domains

Just as black lists have different criteria for including IP addresses, they also have different ways of categorizing the IP addresses. Some black lists use different domains (called query domains) to separate IP addresses based on the reason they are blacklisted. One domain will contain only IP addresses for dialup accounts, another domain will contain only IP addresses for bulk mailers. This type of categorization allows you to select the reasons for which you do not want to accept black listed mail, and use the domain that contains IP addresses for that reason.

Categorizing IP Addresses by a Reason Code/IP Address

Other black lists return a reason code/IP address (i.e. 127.0.0.3) as to why an IP address is black listed. Although all IP addresses are listed in one domain, each will contain a reason code that explains why it is included. For example, a code of 127.0.0.3 may represent a dial-up account, and a code of 127.0.0.4 might represent a bulk mailer. The Fiveten black list is an example of one of these black lists.

How to Determine Which Method a Black List Uses

Unfortunately, there is no standard across black lists. One black list may use separate query domains, and another may use reason/IP codes. Likewise, there is no standard across the reason/IP codes that are returned. For one black list, 127.0.0.3 may represent dial-ups, and on another black list this code may represent bulk mailers. The best resources for finding out this information are the black lists themselves. By going to their web sites, you can learn how each black list classifies the listed IP addresses.

Related Topics

Server Level Antispam Options (Black Lists) (on page 270)

Understanding DNS Black Lists (on page 90)

Server Level DNS Black Lists (on page 89)

Trusted Black Lists (on page 277)

Add/Edit the DNS Black List (on page 92)

DNS Black Lists (Server Level)

How to get here

Server level DNS black lists are spam databases that store information about IP addresses that are known to send spam. IP addresses that have open mail relays (relays mail for anyone) are also commonly listed in black lists, because those servers have the potential to be easily hijacked by spammers. Each black list compares the IP addresses from which an e-mail is sent against the spam database to look for a match. If a domain's IP address is listed in one of the black lists, mail from that domain should be suspected of being spam.

All black lists must be configured and enabled at the server level before an IMail e-mail domain can use them. This lets a system administrator decide which black lists to allow an e-mail domain to use. Only black lists that are enabled on the DNS Black Lists page are available for use in domain (host) level configurations.

Use DNS Black Lists Options to add, edit and delete server black lists. All black lists that are currently configured for the server are displayed in the DNS black list. The DNS black list information is stored in the `"spamblkm.txt"` file located in the `"...\IMail"` top directory.

Note: DNS black lists must be enabled at the server level before they are made available for use at the email domain level. DNS black lists are then used at the domain level (when bound to an IP address), where administrators can choose which black lists to enable for the host on the *Connection Checks* (on page 274) page.

- **Add.** Click this button to *Add to DNS Black List* (on page 92) page.
- **Edit.** Select the DNS to edit and click this button to *Edit the DNS Black List* (on page 92) to the DNS Black List.
- **Delete.** Select an item on the DNS Black List to delete and click the **Delete** button.

Important: Updates made to the DNS Black List will not successfully update until the "Save" button has been clicked, and the message "Your changes have been saved" is displayed at the top.

Save. Click to save your settings. An "Update Successful" message and the time of the update appear.

Related Topics

Server Level Antispam Options (Black Lists) (on page 270)

Understanding DNS Black Lists (on page 90)

How Black Lists Work (on page 91)

Adding a DNS Black List (on page 92)

Setting Connection Checks Options (on page 274)

Add/Edit DNS Black List

How to get here

This pop-up enables you to either edit an existing DNS black list or configure a new DNS black list.

Important: Fields cannot be left blank or contain spaces.

- **Name.** Enter a name in the text box to identify a new black list. This can be any name that you want, and will be used in log lines to identify the black list entry.
- **Server.** In the text box, enter the domain name or IP address of the DNS server to contact for black list queries. This field contains an asterisk (*) by default, which indicates that the default IMail Server DNS is used for black list queries, where it relays the DNS query to the DNS server for the black list. Using the asterisk eliminates the need to enter the IP address or domain.

- **Query Domain.** In the text box, enter the domain to query in the zone file. This name usually matches the server domain name. However, sometimes a black list will contain multiple zones to query on the same server. When this happens, the server name and the query domain will be different. The only way to know this is to read the documentation for the black list being used.
- **Type.** Select the type of lookup that the black list performs from the list box.
  - **ADDR (ADDRESS).** This type of black list uses a message's "FROM" address to determine whether the message is spam.
  - **DNS.** This type of black list checks the IP address of the connecting SMTP server against spam databases to determine whether the message is spam. If the IP address is listed in one of the black list's databases, the message is identified as spam.
  - **HELO.** This type of black list checks the domain supplied in the HELO or EHLO command to determine whether to accept the message. The domain name that is given in the HELO/EHLO command must match the IP address.
  - **RHS (RIGHT-HAND SIDE).** This type of black list checks the information following the @ symbol supplied in the "MAIL FROM" command to determine whether the message is spam.
- **Enable.** Select the check box to enable the black list.
- **TCP/IP First.** Some black lists, especially ones that supply .txt records, have packets that are too large to transmit via the UDP protocol. These lists disable UDP access and require TCP to query the black list. Select this check box to allow the administrator to flag a list as one of these types.

OK. Click this button to add to DNS black list. The new black list appears on the DNS Black Lists page, but will not be permanent until the **"Save"** button is clicked.

Cancel. Click this button to cancel adding a new black list. No new information should appear on the DNS Black Lists page.

Related Topics

Understanding DNS Black Lists (on page 90)

How Black Lists Work (on page 91)

Setting DNS Black Lists Options (on page 277)

Setting Connection Checks Options (on page 274)

Connection Checks

How to get here

Use the options on this page to enable/disable the *DNS black lists* (on page 89) for the current domain. Black lists are not enabled by default, so each new e-mail domain must enable the black lists.

DNS black lists compare the sender information from incoming messages against spam databases to identify spam. DNS black lists must be enabled at the server level before they are made available for use at the e-mail domain level. DNS black lists are then used at the domain level (when bound to an IP address), where administrators can choose which black lists to enable for the host.

After a black list is added, it displays in the **Black List** list. The black lists that are available to add are dependent upon which black lists are configured for the server.



Important: If a black list is not configured at the server level, it will not be available for selection to this page.

Administrators have the option to specify whether a message is deleted if it matches a specific number of standard DNS black lists plus the number of enabled verification checks.

Administrators can review messages that match the DNS black lists. If an e-mail matches the criteria of the black lists, an X-Header is inserted in the message indicating which black list it matched and why. The e-mail is then passed on to content filtering for further examination. The message is delivered if no other rules processing takes place.

The **Trusted DNS Blacklist**, is been combined with the **Connection Checks List**. It displays whether or not the black list is enabled for the domain, the server where the domain resides, and its query domain. The query domain usually matches the server domain name. However, sometimes a black list will contain multiple zones to query on the same server. When this happens, the server name and the query domain will be different. The only way to know this is to read the documentation for the black list being used.



Note: A match made on the **Standard DNS Blacklist** will follow the verification check selections

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Connection Checks List

- **DNS Black Lists.** This column displays all existing black lists for the current domain. Click a black list to modify the black list options.
- **Type.** This column displays the type of lookup that the black list performs.
- **Server.** This column displays the domain name or IP address of the DNS server to contact for the corresponding black list's queries.
- **Query Domain.** This column displays the domain that is queried for the corresponding black list.

- **Trusted.** This check box is selected to enable it as a Trusted Black List.

> **Note:** A match made to the Trusted DNS Blacklist will automatically be deleted.

- **Add.** Click **Add** to *create a new black list* (on page 277) for the current domain. For more information, see *Adding a DNS Black List* (on page 92).
- **Delete.** To delete a black list, select its corresponding check box, then click the **Delete** button.

Verification Checks:

Select any of the following verification tests to perform on incoming e-mail messages. If a message fails any of the checks, an X-Header is inserted into the message.

> **Note:** These options are resource intensive and may slow down mail processing.

- **Verify MAIL FROM Address.** Select this check box to have the "From" address of the connecting server verified for each message to ensure that the user is a valid user on the mail server. If the user or server does not exist, the message is identified as spam.
- **Perform Reverse DNS Lookup for Connecting Server.** Select this check box to create a test in which the IP address of the connecting server is used to perform a reverse DNS lookup to determine the domain name. If a domain has a valid PTR record, the message is accepted. If a reverse lookup fails, it means there is no reverse record for that IP address and the message is marked as spam. An IP address with no PTR record is usually either from a dial-up connection or spoofed message, both of which are indicators of spam. However, keep in mind that a significant number of legitimate mail servers do not have a reverse DNS entry. This may cause legitimate mail to be marked as spam (*false positive*[10]).
- **Verify HELO / EHLO domain.** Select this check box to create a test in which the domain passed during the HELO/EHLO is used to perform a DNS query to verify that the domain specified has an A record or an MX record. If this test fails, an X-Header is inserted into the message.
- **Delete Message after x Matches.** Select this check box to delete the message immediately if it matches x number of black lists plus verification check options. Enter a value that is not greater than the number of black lists plus the number of verification check options that are configured.
- **Prefix Subject with.** Select this check box to create a test in which, if selected, the subject of a message identified as spam by connection filtering is modified from the default text to begin with the text entered in the text box. This option does not apply if the **Delete Message after x matches** is selected and a message meets the criteria for the number of black list and verification check matches.

[10] Many black lists used for connection filtering return hits for domains such as yahoo.com, hotmail.com, and msn.com, among others. If you use these black lists, non-spam e-mail from these domains may be identified as spam and processed according to the specified spam action.

Important: The SMTPD service does not accept mail from clients that do not begin the SMTP conversation with "HELO" or "EHLO".

Save. Click to save your changes. An "Update Successful" message and the time of the update appear.

Related Topics

Adding to Black List (on page 277)

Server Level Antispam Options (Black Lists) (on page 270)

Understanding DNS Black Lists (on page 90)

How Black Lists Work (on page 91)

Setting DNS Black Lists Options (on page 277)

Setting White List Administration Options (on page 242)

IMail SMTP Settings - Control Access (on page 400)

Adding to Black List

How to get here

Before adding to the **DNS Black List** for a domain, be sure that it has been added to the system level DNS Black List, found at **System** > **DNS Black Lists.**

DNS Black List selection will only display items that are enabled. This option is set in the **System > DNS Black List**. By default all items added to the **System > DNS Black List** are enabled.

Note: Disabling a an item in the **System > DNS Black List** will automatically remove it from the **Connection Checks** or **Trusted DNS Black List**. Should the item be enabled at a later date it will automatically re-enable the list in **Connection Checks** or **Trusted DNS Black List**.

Caution: A match made to the Trusted DNS Blacklist will automatically be deleted

Creating a Trusted DNS Black List

1. Click **"Add"** on the **Connection Checks** page, and a pop-up will display all available domains that can be selected for the Black List.
2. Select a domain and click **"OK"**. The selected domain will appear on the Connection Checks list.
3. The **"Trusted"** check box must be checked.
4. Click "**Save"** to save this domain to the Standard DNS Black List.



Note: To easily see all domains that are in the **Trusted DNS Black List**, sort the "Trusted" column (click the column title).

Creating a Standard DNS Black List

1 Click **"Add"** at the **Connection Check** page, and the following list will display all domains available to be added to the DNS black list.

2 Select a domain and click **"OK"**. The selected domain will appear in the Connection Checks list. The "Trusted" check box by default is unchecked.

3 Click "**Save"** to save this domain to the Standard DNS Black List.

DNS Black List (Pop-up)

- **DNS Black Lists.** Select a DNS Black List you want to add. This list is maintained under *System > DNS Black Lists* (on page 89).
- **Type.** Displays the type of lookup that the black list performs from the list box (ADDR, DNS, HELO, RHS).
- **Server.** This column displays the domain name or IP address of the DNS server to contact for black list queries. This field contains an asterisk (*) by default, which indicates that the default IMail Server DNS is used for black list queries, where it relays the DNS query to the DNS server for the black list. Using the asterisk eliminates the need to enter the IP address or domain.
- **Query Domain.** This column displays the domain to query in the zone file. This name usually matches the server domain name. However, sometimes a black list will contain multiple zones to query on the same server. When this happens, the server name and the query domain will be different. The only way to know this is to read the documentation for the black list being used.
- **TCP/IP First**. This shows if TCP/IP First check box has been enabled. This check box allows the administrator to flag a list as one of these types.
- **OK.** Click this button after you have made your selection.
- **Cancel.** Click this button to cancel adding a trusted DNS Black List.

Creating a rule to filter messages listed in a black list

Suppose you want to accept all messages whose IP addresses are listed in the FIVETEN black list because they are dialup addresses. You can filter the e-mail based on the X-Header that is inserted into the message and the IP/reason code that is returned from the black list. In the following example, 127.0.0.3 is the IP/reason code for dial up connections used by the FIVETEN black list. For more information on IP/reason codes, see *How Black Lists Work* (on page 91).

Example of creating a rule to accept black lists for specific reasons:

1 Make sure that all of the antispam features are setup with the **Insert X- Header** action to be taken when e-mail is determined to be spam.

2 Set up a delivery rule (Inbound Rule) at either the host or user level that will search for all messages that contain the following X-Header:

X-IMAIL-SPAM-DNSBL: (FIVETEN, +\d, 127.0.0.3)

The rule looks as follows in the **Rules** dialog box:

Header Contains X-IMAIL-SPAM-DNSBL:(FIVETEN, +\d,127.0.0.3)

For more information, see *Setting Inbound Rules* (on page 202).

Choose one of the following rule actions: **Forward**, **Move to Mailbo**x, or **Copy**. For example, select **Move to Mailbox** and in the Address text box enter "Spam".

This rule searches for all messages whose IP addresses are in the FIVETEN black list because they are dialups and sends them to a mailbox called "Spam".

The example rule looks as follows in the rules.ima file: `H~ X-IMAIL-SPAM-DNSBL:(FIVETEN):Spam`



Tip: Initially, you may want to set up a mailbox specifically for spam, then you can then evaluate the messages that are trapped to ensure that no legitimate mail gets caught by mistake.

Spam Filtering (Domain Level)

How to get here

Use the Domain Level Antispam settings to enable, change, and disable various antispam filters for the selected domain.

- **Premium Filter (on page 280).** (optional only with IMail Premium). Provides fully automated spam protection in addition to the Standard Antispam filter included with all IMail products.
- **Statistical Filter (on page 283).** Examines each word in the body of an e-mail message to determine if the e-mail is spam.
- **Phrase Filter** (on page 288). Searches for spam phrases within the body of e-mail messages and identifies the messages that are spam.
- **HTML Features Filter (on page 291).** Searches HTML features in messages that are subject to spam. Sets how many HTML features must be present in an .htm file in order for a message to be identified as spam and the spam action to take.
- **URL Domain Black List (on page 299).** Searches for domain names that appear as URL links in messages, and lets you set the action to take on such messages.
- **Broken MIME Headers (on page 301).** Uses the Broken MIME Header Filter to identify MIME Header characteristics that result in SPAM e-mail.

Note: Content filtering (on page 303) for authenticated users can be enabled or disabled for all the antispam filters listed above on the domain properties page of an IP'ed domain.

- **SPF[11][12] (Sender Policy Framework).** Enables stronger authentication of e-mail senders using Sender Policy Framework (an extension to the DNS system). Provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.
- **Connection Checks (on page 274).** Verifies that the party connecting to your server is not part of a black list.
- **Logging** (on page 317). Controls where the standard antispam logs are written as well as how much detail is provided in them.

Commtouch Premium Filter (Only Premium Versions)

How to get here

In addition to the standard antispam filter included with IMail, the optional Premium Filter provides fully automated spam protection. The Premium Filter, provided in partnership with Commtouch Advanced Security Daemon (a.k.a. ctasd™) is a plug-and-play e-mail-borne spam and malware outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. The daemon adds a layer of e-mail filtering to your mail delivery system in order to provide real-time classification, already in the first minutes after a new outbreak is launched.

The Premium Spam Filter performance can be improved when users *forward spam e-mail to Commtouch* (on page 266). Commtouchs' editors review the spam submission and add spam signature information to it; then the signature is published to the global database to help other users eliminate spam.

---

[11] How to get here IMail uses Sender Policy Framework (SPF) to extend the Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) so IMail Server does not accept e-mail unless the sending computer is designated as a legitimate e-mail sender. This feature provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.To accomplish this e-mail security measure, SPF establishes a policy framework and a sender authentication scheme that verifies ...

[12] The Sender Policy Framework (SPF) pageprovides administrators increased capability to stop incoming email from forged (spoofed) email addresses. Use the SPF settings to configure how to process email that is identified as forged email. Settings on the SPF page apply to the selected domain.Enable SPF. Select this checkbox to enable the SPF filter for the current host. Default actions are specified to take for each SPF query result. You can, however, change the defaults by clicking the hyperlink u ...

When an incoming message is filtered the Commtouch Premium Filter settings are applied before Content Filtering antispam settings but after the Connection Checks.

The Commtouch Premium Filter provides the following classifications for administrators to create, remove, and manage spam.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **Enable Premium Filter** (selected by default if available). Select this check box to enable the Premium Antispam filter for the current mail domain. Default actions are specified to take for each classification. You can, however, change the defaults by clicking the hyperlink under the Classification. An **Action to be Taken** page appears, with the options for that action listed in a list box.



Note: Be sure the *Commtouch Antispam Service* (on page 371) is started.

- **Classification**. This column lists all possible classifications with possible results for this domain.
  - **Confirmed**. Spam messages from known spam sources.
  - **Bulk**. Spam messages from sources that are not confirmed spammers.
  - **Suspected**. Legitimate messages that are sent to slightly larger than average distribution or are unidentified spam messages in the first few seconds of a massive spam outbreak.
  - **Unknown**. Messages for which ctasd does not have any incriminating information, and are therefore assumed to represent legitimate correspondence.
- **Action to be taken**. This column lists the action chosen for each corresponding classification type.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to an e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267).
  - **Insert X- Header**. Inserts an X- Header into the message indicating that the message was identified as spam by the premium filter. For more information, see *X-Header Explanations* (on page 330).
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".
  - **None** (default)**.** No action is performed on messages identified as spam.
- **Target**. This column lists the mailbox or e-mail address for a Move to or Forward to action, respectively.
- **Prefix Subject**. (Yes/No) This column lists whether or not the message will have a classification prefix added to the message.

- **With**. This column lists the actual prefix, if chosen, for the corresponding query result.



Tip: We recommend that you select the **Insert X- Header** option instead of **Delete** until you know that the antispam options are setup to best suit your filtering requirements.

The following actions apply to spam filtering of message header content. These options are available on the Premium Filter Settings page. (Click **Services > Antispam**.)

Premium Connection Checks (IP Reputation)

Commtouch's GlobalView™ Mail Reputation services are used primarily to weed out spam messages and email-borne malware at the entry point before these messages enter the customer's messaging network, thereby relieving the need for resource-consuming downstream filtering. This is accomplished by applying the most up-to-date IP reputation data to the sender IP, before the SMTP connection is accepted.

By applying GlobalView Mail Reputation services to the senders' IP addresses before or during the SMTP session and before their messages enter the messaging network, ctIPd delivers cost-effective benefits such as the following:

- Reduce IT resources such as server count, CPU load, storage, etc.
- Eliminating multiple security risks
- Reducing the level of false positives
- Minimizing the cost of downstream filtering
- Lowering the overall bandwidth consumption
- Optimizing IT labor required to manage the overall messaging process

Additionally, Commtouch GlobalView Mail Reputation services are used as part of an overall strategy to optimize network accessibility so that the network's messaging processes are efficient and focused on allowing legitimate sources full and uninterrupted access. At the same time, the Commtouch GlobalView Mail Reputation services also make access for unauthorized sources with bad reputations attempting to abuse the network more difficult to achieve.

The following actions for **Commtouch IP Reputation** are:

- **Log Only** (Set by default). This setting will take no action on any messages, except to log. Connection checks will be made but all messages will be delivered as usual after logging.
- **Disabled**. This will disable logging and all connection checks.
- **Log With Action.** This setting will allow the following connection checks.
  - Throttle connections identified as suspected, yet unconfirmed, spam sources.
  - Reject connections identified as confirmed spam sources.
- **Reject and throttle connections on the MAIL FROM command.** (Set by default) With IP Reputation enabled, messages will be validated for rejection at the MAIL FROM command.

- **Reject and throttle connections on the DATA command.** With IP Reputation enabled, messages will be validated for rejection at the DATA command.



Setting IP Reputation to validate on the DATA command allows malicious IP's to harvest valid e-mail addresses; since the RCPT TO command occurs before the DATA command.

Related Topic

Default X-Header Classifications (on page 283)

Services for Premium Antispam (on page 371)

Default X-Headers for Premium Filter Classifications

The default values for Premium Filter Classifications when the Premium Filter is enabled:

- **Confirmed.** Inserts X-Header [X-IMAIL-SPAM-CONFIRMED] with subject prefixed with [SPAM].
- **Bulk.** Inserts X-Header [X-IMAIL-SPAM-BULK] with subject prefixed with [BULK].
- **Suspected.** By default no action taken.
- **Unknown.** By default no action taken.

False Positive Example

Many black lists used for connection filtering return hits for domains such as yahoo.com, hotmail.com, and msn.com, among others. If you use these black lists, non-spam e-mail from these domains may be identified as spam and processed according to the specified spam action.

Statistical Filtering

Statistical filtering uses the Bayesian spam filtering technique to calculate the probability of a message being spam based by its contents. Unlike simple content-based filters, Bayesian spam filtering learns from spam and from good mail by examining each word in the body of an e-mail message to determine if it is spam. Each word within a message is compared against known spam and non-spam word counts, and assigned a value based on whether the word is likely to be spam. Then, the entire message is assigned a probability based on the assessment of all combined word counts. If a message is identified as spam, you can choose to delete it, forward it to an e-mail address, or insert an X-Header into it. Words that contain non-alphabetic characters, such as numbers, are treated differently from other words. For more information, see *Identifying Wildcards in E-mail* (on page 346).

To increase the chances of legitimate messages not be identified as spam, you can create a host-specific exclude list. The exclude list contains words that you do not want to be included in the statistical analysis, because they are just as likely to appear in non-spam messages as they are in spam messages. The exclude list is stored in the exclude-list.txt file, which is located in the domain's directory.

A list of words that are not included to determine whether a message is spam. The words in the exclude list are words that have an equal chance of being non-spam as spam. For example, "Mortgage" is a term frequently used in spam. However, if you work in the financial industry, this term may appear frequently as non-spam. In such a case, you can enter the word "mortgage" into the exclude list. The exclude list should also include common words like proper names. The exclude list is stored in the `exclude-list.txt` file located in the mail domain 's directory.

Advanced Statistical Filtering

The advanced statistical filtering options control the underlying functionality of the statistical filtering component. These options are useful for experienced administrators who want to further refine the antispam filtering ability.

Related Topics

Antispam Statistical Filter Options (Content Filtering) (on page 284)

Statistical Filter Options (Content Filtering)

How to get here

Use Statistical Filtering to create and maintain the mail domain specific exclude list, specify the action to take when spam is identified, and specify whether to use the primary mail domain's word counts or create new ones.

A list of words that are not included to determine whether a message is spam. The words in the exclude list are words that have an equal chance of being non-spam as spam. For example, "Mortgage" is a term frequently used in spam. However, if you work in the financial industry, this term may appear frequently as non-spam. In such a case, you can enter the word "mortgage" into the exclude list. The exclude list should also include common words like proper names. The exclude list is stored in the `exclude-list.txt` file located in the mail domain 's directory.

Statistical Filtering uses the Bayesian spam filtering technique to calculate the probability of a message being spam based by its contents. Each word in an e-mail message is examined and evaluated depending on how often the word appears in spam and non-spam e-mail. The entire message is then evaluated based on all of the word values to determine whether it is likely to be spam.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Antispam Table To Use: Set the following options to configure statistical filtering.

- **No Filtering.** Disables statistical filtering for the domain.
- **Current Domain** (selected by default). Select this option to define statistical filtering settings specific to the current mail domain.
- **Primary Domain** (default for non-primary domains; not available for primary domains). Select this option to use the primary mail domain's statistical filtering settings instead of creating new settings for the current mail domain.

Note: The exclude table is not included as part of the use drop down.

Exclude the following words from Statistical Analysis:

- **Add.** Click **Add** to create a new word to filter for the current domain.
- **Edit**. Click a word or phrase, then click **Edit** to modify.
- **Delete.** Select a phrase that you want to delete from the domain, then click **Delete** to delete the phrase.
- Click ▲ or▼ to sort the word list.

If the Word list has multiple pages, you can use the page navigation control which appears below the list.

Action taken on e-mail determined to be spam:

- **Action:**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to an e-mail address entered in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "bulk". *Example* (on page 267)
  - **Insert X- Header** (default). Inserts an X- Header into the message indicating that the message was identified as spam by statistical filtering. For more information, see *Spam X-Header Explanations* (on page 330).
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.
  - **None.** No action is performed on messages identified as spam by the statistical filter.

Tip: We recommended that you select the **Insert X- Header** option instead of **Delete** until you know that the antispam options are setup correctly.

Note: For more spam options see *Using Delivery Rules to Filter Spam* (on page 220).

- **Prefix subject with.** If selected, the subject of a message that is identified as spam by the statistical filter will be modified to begin with **X-IMail-Spam- Statistical**.

These options control the underlying functionality of the statistical filtering feature and are dependant upon each other to effectively identify spam. If you have a significant number of legitimate messages that are being identified as spam (false positives) or vice versa, you may need to adjust these options.



Note: The default settings are appropriate for most systems. We strongly advise that ONLY experienced administrators modify these settings. Setting these options too high or too low could hinder IMail Server's ability to identify spam.

Advanced Options

- **The probability a new word is spam** (default value is 40%). The percentage assigned to new words to determine if they are spam. Enter a value between 0 and 100%.

  The higher the value, the more likely a new word will be treated as if it had previously appeared in **spam** e-mail messages. The lower the value, the more likely a new word will be treated as if it had previously appeared in **non- spam** e-mail messages. For example, if you enter 0, every new word will be treated as if it were non-spam. If you enter 100%, every word will be identified as spam.

  We recommend that this value not be set higher than 40%. The idea behind setting this option at 40% or less is to bias the statistical analysis in favor of being legitimate e-mail, thereby reducing the likelihood of a false positive.

  Example: If this option is set to 20%, a new word will be treated as having appeared in spam emails 20% of the time and as having appeared in non-spam emails 80% of the time.

- **An e-mail is spam when its calculated probability exceeds** (default value is 90%). The closer the value is to 100%, the less likely that spam will be caught. The closer the value is to 0, the greater the probability that you will have false positives. Enter a value between 0 and 100%.

  This option sets the minimum probability percentage at which a message will be identified as spam. Messages with probability values below the value entered are identified as non-spam. Messages with probability values above this value are identified as spam.

  Example: Suppose this option is set to 80%. If an e-mail message is processed and the combined probability for all of the word values within it is 60%, then this message is identified as non-spam because it does not meet the probability benchmark of 80%.

  Example: If the word "Stop" appears in an e-mail for the first time, it is considered a new word and assigned a probability of 40% (probability a new word is spam). If you have the "spam calculated probability exceeds" set to 90%, then "stop" is not considered to be spam. In order for "stop" to be considered spam, its probability will have to increase from 40% to 90%.
- **Maximum number of words used when calculating probability** (default value is 15). The number of individual word values, within each e-mail, used to calculate the probability that an e-mail is spam. You can enter any value in this text box; however, entering anything above 25 may have unpredictable results.

  Each word within an e-mail is assigned two word counts: the number of times the word has occurred in spam, and the number of times that a word has occurred in non-spam. From these values, a spam probability is computed for the word. This setting examines the words whose probabilities deviate most from an average word. These words are both spam and non-spam words.

  Example: Suppose this option is set to 15. Since most words have an average spam probability of 50% (50% likely to be spam, 50% likely to be non-spam), then the fifteen words that are farthest away from 50% are used. So if a word has a spam probability of 5% it will most likely be used. Likewise, if a word has a spam probability of 90%, it will most likely be used. A word that has a 45% probability will most likely not be used.



Note: The value for the **Maximum number of words used when calculating probability** can greatly affect the performance of statistical filtering. The greater the value, the more time is spent determining which words to evaluate within a message. Thus, statistical filtering takes longer to calculate the e-mail probability and mail processing takes longer.

Related Topics

About Statistical Filtering (on page 283)

Creating Separate antispam-table.txt Files for Multiple Email Domains (on page 340)

Installing Updated phrase.txt File (on page 265)

Setting Premium Filter Antispam Options (on page 280)

Word Value (definition)

Each word within an e-mail is assigned two word counts:

- the number of times the word has occurred in spam
- the number of times that a word has occurred in non-spam

From these values, a spam probability is computed for the word. This setting examines the words whose probabilities deviate most from an average word. These words are both spam and non-spam words.

Example: Suppose this option is set to 15. Since most words have an average spam probability of 50% (50% likely to be spam, 50% likely to be non-spam), then the fifteen words that are furthest away from 50% are used. So if a word has a spam probability of 5% it will most likely be used. Likewise, if a word has a spam probability of 90%, it will most likely be used. A word that has a 45% probability will most likely not be used.

Exclude List (definition)

A list of words that are not included to determine whether a message is spam. The words in the exclude list are words that have an equal chance of being non-spam as spam. For example, "Mortgage" is a term frequently used in spam. However, if you work in the financial industry, this term may appear frequently as non-spam. In such a case, you can enter the word "mortgage" into the exclude list. The exclude list should also include common words like proper names. The exclude list is stored in the `exclude-list.txt` file located in the mail domain 's directory.

Phrase Filtering

Phrase Filtering searches for common spam phrases within the body of e-mail messages. If a message contains one of the phrases in the phrase list, it is identified as spam and you can configure how to handle it. Phrases are stored in the phrase-list.txt file, which is located in the IMail top directory. You create this list by adding phrases located at **Antispam** > [Select a domain] > **Spam Filtering** > **Phrase Filtering.**

Related Topics

Configuring Content Filtering (on page 303)

Statistical Filtering (on page 283)

Obtaining a phrase.txt File (on page 265)

Phrase Filter Options (Content Filtering)

How to get here

Use Phrase Filtering to enable/disable phrase searches for the current mail domain, create and maintain the phrase list, and specify an action to take when an e-mail contains one of the phrases.

Phrase Filtering searches for common spam phrases within selected areas of e-mail messages. If a message contains one of the phrases in the phrase list, it is identified as spam and you can configure actions to take on the message. Phrases are stored in the `phrase-list.txt` file, which is located in the IMail top directory.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Use: Set the following options to configure phrase filtering.

- **No Filtering.** Disables phrase filtering.
- **Current Domain** (selected by default). Select this option to define phrase filtering settings specific to the current mail domain.
- **Primary Domain** (default for non-primary domains; not available for primary domains). Select this option to use the primary mail domain's phrase filtering settings instead of creating new settings for the current mail domain.

Scan: Select which part of a message phrase filtering will examine for phrase matches.

- **Subject**
- **Body** (default).
- **Subject and Body**

Action taken on e-mail determined to be spam:

- **Action:**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to an e-mail address entered in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "bulk". *Example* (on page 267)
  - **Insert X- Header** (default). Inserts an X- Header into the message indicating that the message contained a phrase that is in the phrase list. For more information, see *Spam X-Header Explanations* (on page 330).
  - **Move to Mailbox**. Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created.
  - **None.** No action is performed on messages identified as spam by the phrase filter.



Tip: We recommend that you select the Insert X-Header option instead of Delete until you know that the antispam options are setup correctly.

Note: For more spam options see *Using Delivery Rules to Filter Spam* (on page 220).

Prefix subject with. If selected, the subject of a message that is identified as spam by the phrase filter will be modified to begin with **X-IMail-Spam-Phrase**.

Normalize Words. If this option is selected, IMail strips out all *non-alphabetic characters* (on page 290) from words before comparing them to the phrase list.

To Edit an Antispam Phrase Filter:

1. From the Phrase Filtering page, click **Edit Phrases**. The Phrase Filter Text Editor page appears. The **File** information displays the file directory where the `phrase-list.txt` file is saved.
2. Enter text phrases that you want the phrase filter to search for within selected parts of e-mail messages. Press **Enter** after each phrase is entered in the text editor.
3. Click **Save.**

Related Topics

What should be in the Phrase List? (on page 290)

Installing Updated phrase.txt File (on page 265)

Creating Separate antispam-table.txt Files for Multiple Email Domains (on page 340)

Setting Premium Filter Antispam Options (on page 280)

What should be in the phrase list?

The phrase list should contain phrases that occur frequently in spam. The best way to obtain this information is to look at your current rules to see which phrases you filter out. You can also download a sample `phrase-list.txt` file from the Ipswitch web site.

A Note about Entering Domain Names

When you enter a domain name into the phrase list, IMail Server will filter the domain name if it appears in the normal text in the body of an e-mail message. It will not filter domain names found in URLs or links. To accomplish this, you must enter the domain name into the URL Domain Black List. The URL Domain Black List filters the domain name if it appears as a link in HTML code within a message, specifically within HREF and IMG SRC tags.

Normalizing Words

When the **Normalize Words** option is selected, all words in a message are normalized before they are added or compared to the phrase list or antispam-table.txt file. Normalizing consists of stripping out all non-alphabetic characters (any character other than A-Z, a-z).

Example:

F1rst becomes frst

s*e*x*y becomes sexy



Note: If a word containing a number or non-alphabetic character is frequently used in your mail messages, such as a company name, we recommended that you do not enable the **Normalize Words** option.

HTML Features Filter

How to get here

Use HTML Features Filter to select which HTML features to search for in messages, how many of the selected features must appear in order for a message to be identified as spam, and what action to take when a message is identified as spam.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Use: Set the following options to configure HTML features filtering.

- **No Filtering.** Disables HTML features filtering for the selected mail domain.
- **Current Domain** (selected by default). Select this option to define HTML features filtering settings specific to the current mail domain.
- **Primary Domain** (default for non-primary domains; not available for primary domains). Select this option to use the primary mail domain's HTML features filtering instead of creating new settings for the current mail domain.

Select the HTML features to detect:

Nested Table (on page 293)	*Invalid Tag* (on page 294)	*Deceptive URL* (on page 295)
Hyperlink (on page 294)	*Script Tag* (on page 295)	*Embedded Comment* (on page 296)
Image Tag (on page 294)	*Mailto: Hyperlink* (on page 295)	*Deceptive Text* (on page 296)

- **Number of options detected for an e-mail to be considered spam**. Enter the number of the above selected types of HTML features that must appear in an e-mail message before it is identified as spam.
- **Action taken on e-mail determined to be spam**. Specify one of the following actions to take on a message that contains selected HTML features:
  - **Action:**
    - **Delete.** Immediately deletes the message.

- **Forward to Address.** Forwards the message to the e-mail address specified in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
- **Insert X- Header** (default). Inserts an X- Header into the message indicating that it was identified as spam and includes the selected HTML features. See also *X-Header Explanations* (on page 330).
- **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".
- **None.** No action is taken on the message.

- **Prefix Subject With**. If selected, the subject of a message that is identified as spam by the HTML filter will be modified to begin with the text entered in the text box.

Save. Click this button to save your settings.

For more information, see *example configuration for HTML feature filtering* (on page 297).

To Edit an Antispam HTML Features Filter:

1 From the Antispam HTML Features Filter list, select an HTML features filter that you want to edit. The HTML Features Filter Settings page appears.
2 Make the desired changes to the options, then click **Save**.

Related Topics

Using Delivery Rules to Filter Spam (on page 220)

Example Configuration for HTML feature filtering (on page 297)

X-Header Example 1 (on page 297)

X-Header Example 2 (on page 298)

HTML Filtering E-mail Scanning Example (on page 298)

Overview of HTML Filtering

For each HTML section of an e-mail, the HTML filter processes the text outside the angle brackets of an HTML tag as before. The HTML filter processes the text within the angle brackets of an HTML tag as follows. The HTML filter first checks to see if the tag is one of the features the filter has been configured to search for. If it is, the HTML Filter counter counts the number of features found. The e-mail is considered spam if the number of HTML features found equals the number configured for the feature's found count.

HTML filtering is part of content filtering, but is used only on HTML portions of a message. The individual components of HTML filtering are discussed below.

Types of **HTML Filtering**:

- **HTML Parser**

The HTML parser is always used on HTML messages. The parser decodes the HTML code and tags until the text appears as it would when the message is opened. The parser then sends the text on to be processed by statistical and phrase filtering to determine if it is spam.

- **HTML Feature Filtering**

HTML feature filtering lets you define certain HTML tags that will be spam indicators. The HTML features include *Nested Table* (on page 293), *Hyperlink* (on page 294), *Script Tag* (on page 295), *Invalid Tag* (on page 294), *Image Tag* (on page 294), *Mailto Hyperlink* (on page 295), *Deceptive URL* (on page 295), *Embedded Comment* (on page 296). If a message contains a configurable number of these HTML features, it is identified as spam.

- **URL Domain Black List**

The URL Domain Black List is a configurable list of domain names that are known to send spam. IMail Server extracts the primary domain from an http link to determine if the domain name is in the URL Domain Black List. It does this by looking for domains that are used in HREF and IMG SRC tags in the HTML code. If the primary domain matches any of the domain names in the URL Domain Black List, the e-mail is considered spam and the appropriate spam action is taken.

Why do I need HTML Filtering? Why doesn't the Phrase and Statistical Filter Work?

Spammers use a variety of techniques to get around antispam programs that filter on words. The primary way they do this is by disguising the message text in HTML e-mail so that is does not look like text. Unfortunately, if a word does not look like a word, the phrase and statistical filter will not be able to determine if it is spam. The HTML filter component solves this problem by decoding the HTML code to reveal the text, which is then passed on to the statistical filter for word analysis.

Related Topics

Example E-mail as it is scanned with and without HTML Filtering (on page 298)

Nested Tables

Nested Table

A nested table is a table within a table in HTML code, it is displayed as a table tag (<TABLE>) within a table tag. The following is an example of the HTML code for a nested table.

<table>
<tr>
<td>
<table>
<tr>

<td>
Get Paid $1000 A Week To Work From Home.
</td>
</tr>
</table>
</td>
<tr>
</table>

Hyperlinks

Spammers often include links in their messages as a way to get you to visit a website. An HTML link in a message looks like the following:

```
<a href="http ://www.ipswitch.com /sla/index"</a>
```

This may or may not be accompanied by a tag calling an image or graphic. You should be careful when selecting this feature to filter on. Many legitimate HTML e-mail messages contain links in them, and as such would be identified as spam.

Image Tags

Spammers often put images into messages to hide the text from the content filter. Images are characterized by the following HTML code: <IMG src=filename>

Since there are no words outside the HTML tag in the above example, you would only see a graphic when you open the message. The statistical filter alone would not decipher this HTML code, because all words are included within the HTML tag. But the HTML parser will decode the HTML to see if it contains any Image tags.

If you want all messages containing IMG SRC tags to be considered spam, select this option under **HTML Feature Filtering**.

If you want the domain name in such a tag to be considered a spam indicator, place the domain name in the URL Domain Black List.

Invalid Tags

Spammers sometimes insert the message text inside invalid HTML tags in an attempt to confuse statistical word filters. This is because the text, in the invalid tag, is treated as non-spam words and they balance out the spam words. Some examples are shown below:

Examples:

- <comment>Get Rich Quick</comment>

IMail Server treats all non-standard comment formats as invalid tags.

- <Get paid to work from home. Respond now for information on this fantastic offer. There are a limited number of available positions, so don’t miss out. Respond Now!>

In the example above, text e-mail clients hide the message because it appears within an invalid HTML tag.

If you select the **Invalid Tag** option in **HTML Feature Filtering**, messages containing this type of spam trick will be identified as spam.



Note: IMail Server considers any tag that is not HTML 4.0 compliant to be an invalid tag.

Script tag

Spammers sometimes create an entire message composed of nothing but script, such as Javascript. Before the message is loaded, there are no words that the statistical filter would be able to identify. When the message is loaded, the text is displayed as normal, instead of the script.

The HTML parser ignores the script tag in messages. Therefore, if you want messages with scripting to be identified as spam, select **Script Tag** under **HTML Feature Filtering**. IMail will identify all messages containing such a tag as spam.

Mailto: Hyperlink

A Mailto hyperlink allows you to send e-mail directly from a web page, or in this case, an e-mail by clicking a link. The link opens up a new message window in your e-mail client with the recipients e-mail address filled in. Spammers use mailto hyperlinks as a way to get feedback from you.

Example:

```
<a href="mailto:User@domain.com">Email Us</a>
```

Deceptive URLs

Spammers sometimes encode URLs to conceal the hostname or IP addresses from a content filter. Select this option to identify messages with deceptive URLs.

When IMail checks for deceptive URLs, the domain component of the URL is decoded first, then it is checked against the URL Domain Black List. If the domain component of the URL is found in the URL Domain Black List, the e-mail is treated as spam. The following are examples of deceptive URLs:

Plain text examples:

```
http ://7763631671/domainname.htm

http://0xCeBF9e37/domainname.htm

http://0316.0277.0236.067/domainname.htm
```

http://3468664375@3468664375/o%62s%63ur%65%2e%68t%6d

Embedded Comment

Sometimes spammers place a comment in the middle of a word, as shown in the example below:

VIA<!--text here-->GRA

This causes a single word, in this case VIAGRA, to be viewed as two words (VIA and GRA) by the e-mail client. Often, the comments themselves contain neutral words that spammers intentionally use to throw off statistical filters. The statistical filter would not catch this, because it cannot distinguish that there are HTML tags in the text. It would look for the words VIA and GRA when comparing the message to the `antispam-table.txt` file. Now, the HTML parser will extract the comments from the text, so that it can be examined by statistical filtering.

However, if you want embedded comments to be considered spam indicators regardless of the text, select this option under **HTML Feature Filtering**.

Deceptive Text

When the text of an html message is encoded. For example, text outside an html tag is considered encoded when it is in the format of &#ddd where ddd is a decimal number in the range: 48-57, 65-90, or 97-122.

Example

In an effort to get around antispam tests, the following encoding:

There is no

consultation

fees and

absolutely no

obligation.

You will

be amazed at

the rates we

can

provide.

Displays the following message:

There is no consultation fees and absolutely no obligation. You will be amazed at the rates we can provide.

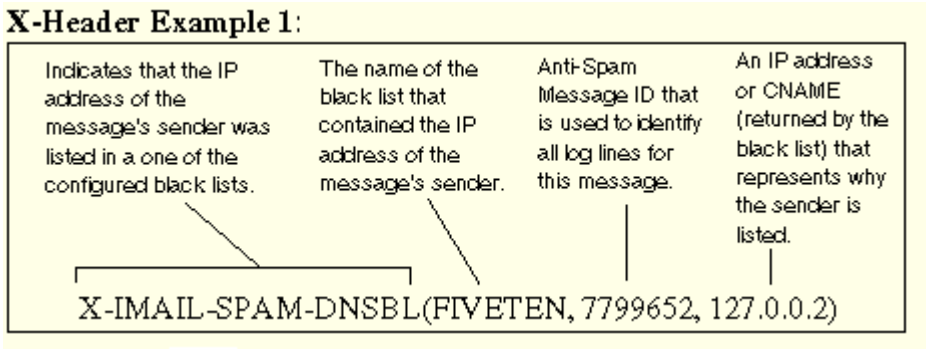
Example HTML Feature Configuration

You should be aware that some of the HTML features available for filter selection are common to all HTML messages, not just spam (i.e. hyperlinks). Selecting one of these features may cause false positives. As you gain experience with the HTML feature filtering options, you will be able to modify the settings based on your preferences. However, below you will find a suggested initial configuration that will enable you to use the HTML feature filter with success.

1. Select **Embedded Comment** and **Deceptive** URL. Both of these elements, especially when they occur together, are strong indicators of spam. Make sure that all other HTML features are cleared.
2. Select **2** from **Number of options detected for an e-mail to be considered spam**. This requires that both an embedded comment and a deceptive URL be present in a message for it to be considered spam.
3. For the option labeled **Action taken on e-mail determined to be spam**, select **Insert X-Header.**

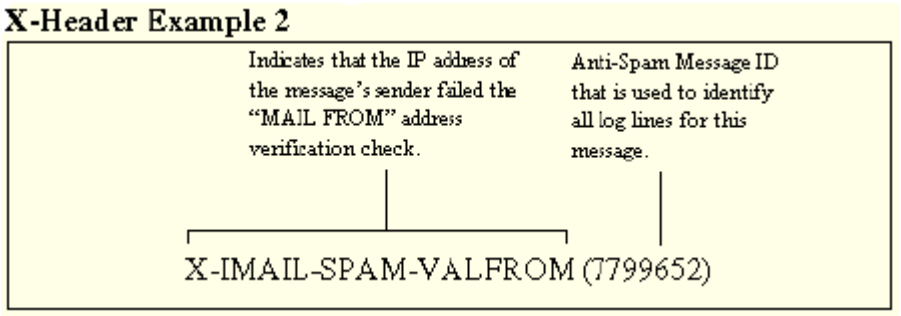
By selecting the Insert X-Header option, your messages are still delivered. You may want to create a delivery rule that moves such messages to a specific mailbox. For more information, see *Using Delivery Rules to Filter Spam* (on page 220).

X-Header Example 1



The above X-Header indicates that the IP address of the message’s sender was found in the FIVETEN black list, which suggests that it is spam.

X-Header Example 2



The above X-Header indicates that the same message also failed the MAIL FROM verification check.

HTML Filtering Example of Scanning E-mail

To better understand how HTML filtering will increase your ability to identify spam, below is an example of an HTML spam message that was filtered first only through statistical and phrase filtering, and then through HTML filtering. In this message the spammer used bogus HTML tags to try to hide the words from spam filters. From the statistical filtering log entries below you can see that IMail Server didn't recognize many words in the e-mail. When this same message was run through HTML filtering, the log entries below show that more words were recognized:

```
Original Message
Date: Tue, 8 Apr 2003 16:04:09 -0400
Message-Id: <TestUser@ipswitch.com>
Mime-Version: 1.0
Content-Type: text/html; charset=us-ascii
From: "Test User" <TestUser@ipswitch.com>
Reply-To: <TestUser@ipswitch.com>
To: TestUser2@ipswitch.com
Subject: hello there
X-Mailer: <IMail v8.00>

<!W>VIA<!Z>GRA<!E> N<!l>o<!k>w<!g>
a<!y>v<!b>a<!Z>I<!Y>l<!X>a<!N>b<!Q>l<!V>e<!H> f<!J>o<!I>r<!D> a<!S>
l<!O>o<!I>w <!A>c<!Z>o<!X>s<!S>t<!J> t<!N>h<!X>e<!U>
e<!L>ff<!V>ec<!W>tiv<!Z>ene<!E>ss<!I>
<!K>o<!G>f<!Y><!F>V<!I>I<!F>AGRA<!C> has<!U> be<!D>en<!L>
p<!Z>r<!B>o<!W>ven<!V>
t<!Z>i<!I>m<!M>e a<!H>nd<!E> tim<!U>e a<!H>g<!G>a<!B>in <!W>in
<!I>cl<!O>i<!D>ni<!O>c<!F>a<!K>l<!I> s<!Y>t<!K>udies <!C>w<!F>i<!F>th
t<!F>h<!M>ous<!K>and<!J>s o<!J>f<!B> p<!H>ati<!J>ent<!N>s<!J>.<!Y><!C>
```

Results When E-Mail is Scanned only with Statistical Filtering
05:23 10:18 SMTP (02940000) word = agra, probability = 0.990000
05:23 10:18 SMTP(02940000) word = udies, probability = 0.400000

Results when E-Mail is scanned through statistical and HTML Filtering
05:23 10:24 SMTP(09380000) word = viagra, probability = 0.911599
05:23 10:24 SMTP(09380000) word = thousands, probability = 0.796194
05:23 10:24 SMTP(09380000) word = proven, probability = 0.748141
05:23 10:24 SMTP(09380000) word = patients, probability = 0.718994
05:23 10:24 SMTP(09380000) word = been, probability = 0.285162
05:23 10:24 SMTP(09380000) word = again, probability = 0.309129

URL Domain Black List

How to get here

Use URL Domain Black List to search for domain names that appear as URL links in messages and set the action to take on such messages. Secondary mail domains can choose to use the primary domain's URL Domain Black List instead of maintaining their own.

The URL domain black lists for the current mail domain is stored in the `url-domain-bl.txt` file, which is located in the IMail top directory.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Use: Set the following options to configure HTML features filtering.

- **No Filtering.** Disables URL domain black list filtering for the selected mail domain.
- **Current Domain** (selected by default). Select this option to define URL domain black list filtering settings specific to the current mail domain. The primary mail domain selects this option to use the primary URL Domain Black List. The secondary mail domains select this option to use the secondary mail domain's URL Domain Black List.
- **Primary Domain** (default for non- primary domains; not available for primary domains). Select this option to use the primary mail domain's URL domain black list filtering instead of creating new settings for the current mail domain.



Note: Because secondary mail domains cannot add or remove words from the primary mail domain's URL domain black list, if you are setting URL domain black lists for a secondary mail domain, the **Add** and **Delete** buttons are disabled for the selected secondary mail domain and the URL domain black list cannot be edited.

Scan. Set the following option to configure the type of text that domain black list filtering scans for hyperlinks (URLs):

- HTML text. Select this option to scan HTML text for hyperlinks embedded in e-mail messages. *Example* (on page 301)
- HTML and Plain Text. Select this option to scan both HTML and plain text for hyperlinks embedded in e-mail messages. *Example* (on page 301)

Action taken on e-mail determined to be spam. Specify one of the following actions to take on a message that matches a URL Domain Black List:

- **Action:**
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to the e-mail address specified in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root- bulk". *Example* (on page 267)
  - **Insert X- Header** (default). Inserts an X- Header into the message indicating that it was identified as spam and includes a matching black list. See also *X-Header Explanations* (on page 330).
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".
  - **None.** No action is taken on the message.
- **Prefix Subject With.** If selected, the subject of a message that is identified as spam by the URL domain black list filter will be modified to begin with the *text* (on page 347) entered in the text box.

To Edit a URL Domain Black List:

1. From the URL Domain Black List page, click **Edit Phrases URL Entries**. The URL Domain Black List Text Editor page appears. The **File** information displays the file directory where the `url-domain- bl.txt` file is saved.
2. Enter the name of the domain or IP address that you want to add to the black list. See below for acceptable entry guidelines. Press **Enter** after each phrase is entered in the text editor.
3. Click **Save**.

Acceptable Entries

If you enter the domain name in the format of www.domain.com , a URL must contain the entire entry (including www.) in order for the message to be identified as spam. Messages with only domain.com in the URL will not be identified as spam. *Example* (on page 300)

If you enter a domain name in the format of domain.com, IMail Server looks for all URLs that contain domain.com, whether or not it is preceded by anything. For example, the URLs www.domain.com and www.mail.domain.com would both be identified as spam, because they both contain the entry domain.com.

Related Topics

HTML or Plain Text Scan Example (on page 301)

HTML Scan Example (on page 301)

URL Domain Black List Entry (Example) (on page 300)

URL Domain Black List Entry (Example)

If you enter www.ipswitch.com into the URL Domain Black List,

the following will be identified as spam:

- Messages containing URLs containing exactly www.ipswitch.com.

The following will not be identified as spam:

- Messages containing URLs containing www.mail.ipswitch.com or other variations.

HTML Scan Example

HTML content is scanned for hypertext links within an e-mail message. If the URL domain exampleblacklist.com is included in the URL Domain Black List and *User friendly Web site* ('javascript:kadovTextPopup(this)') is found in the e-mail scan, then the message is processed as spam.

HTML or Plain Text Scan Example

HTML content and plain text is scanned for hypertext links within an e-mail message.

HTML examples:

- If the URL domain exampleblacklist.com is included in the URL Domain Black List and
  <a href="http ://exampleblacklist.com/example1.htm">User friendly Web site 1 is found in the e-mail scan, then the message is processed as spam.
- If the URL domain exampleblacklist.com is included in the URL Domain Black List and
  User friendly Web site 2 is found in the e-mail scan, then the message is processed as spam.

Plain text examples:

If the URL domain exampleblacklist.com is included in the URL Domain Black List and User friendly Web site 3 is found in the e-mail scan, then the message is processed as spam.

If the URL domain exampleblacklist.com is included in the URL Domain Black List and User friendly Web site 4 is found in the e-mail scan, then the message is processed as SPAM.

Related Topic

HTML feature filtering (on page 291)

Broken MIME Headers

How to get here

The Broken MIME Headers filter identifies Broken MIME header characteristics that result in SPAM e-mail. Broken MIME headers occur when:

- A message opening boundary delimiter is hidden by making it part of the message part header.

- E-mail boundary parameter values exceed 70 characters.
- No e-mail boundary parameters exist.
- MIME type parameters are on a line with no leading white spaces.

Options on this page let you select actions to take when Broken MIME headers are identified as SPAM e-mail.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Set the following options to configure Broken MIME Headers filtering:

- **Enable Broken MIME Headers** (selected by default). Select this check box to enable the Broken MIME Headers filter for the current host.

Action to be taken on e-mail determined to be spam. Specify an action to take if a message is identified as spam:

- **Delete.** Immediately deletes the message.
- **Forward to Address.** Forwards the message to an e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
- **Insert X-Header** (default). Inserts an X-Header into the message indicating that the message was identified as spam by the Broken MIME headers filter. The default value is **Insert X-Header**.
- **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".
- **None.** No action is performed on messages identified as spam.
- **Prefix subject with** (cleared by default). If selected, messages identified as spam are modified to begin the message subject with the *text* (on page 302) entered in the text box to the right of this option.



Tip: We recommended that you select the **Insert X- Header** option instead of **Delete** until you know that the Broken MIME header options are setup to best suit your filtering requirements.

Save. Click this button to save your settings.

Related Topic

Modifying Subject for Broken MIME Headers (on page 302)

Modifying the Subject for Broken MIME Headers

By default, the text that is added to the message subject is:

X-IMail-Broken-MIME-Header

This subject field is also user configurable.

Enable Content Filtering

How to get here

Content filtering for authenticated users can be enabled or disabled on the domain properties page of an IP'ed domain.

Content filtering when enabled will apply the following filtering to authenticated users:

- Premium Filter
- Statistical Filter
- Phrase Filter
- HTML Features Filter
- URL Domain Black List
- Broken MIME Headers

Related Topics

Setting Antispam Phrase Filter Options (on page 289)

Setting Antispam Statistical Filter Options (on page 284)

SPF Filtering

How to get here

IMail uses Sender Policy Framework (SPF) to extend the Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) so IMail Server does not accept e-mail unless the sending computer is designated as a legitimate e-mail sender. This feature provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.

To accomplish this e-mail security measure, SPF establishes a policy framework and a sender authentication scheme that verifies the identity of e-mail servers (domains) for incoming messages. SMTP receivers (such as IMail Server) use this information to evaluate whether the message is from an e-mail server that is authorized to send e-mail from the message sender. Messages that do not meet the SPF criteria are not accepted as a legitimate e-mail message and are processed according to the SPF settings selected on the *SPF page.* (on page 304)

How does SPF work?

SPF policy data is published on a DNS server in a .TXT record. DNS resolvers typically cache SPF data to reduce lookup traffic. Sender domains do not have to run new servers to advertise SPF information; instead, SPF uses the connecting client 's IP address and information from the SMTP envelope to evaluate the SPF policy document published via DNS. After the policy is evaluated, the message is classified and handled

accordingly. For additional information about SPF, go to the *SPF community at http://spf.pobox.com* (http://spf.pobox.com/).

Example:

If a spammer forges mail from the mail server imaspammer.com and uses a different domain in the From address, such as john.doe@notaspammer.com, the receiving e-mail server checks the SPF record for notaspammer.com. If it finds that john.doe@notaspammer.com is not listed as a legitimate e-mail sender on notaspammer.com, the message fails and is processed by the SPF settings on the SPF tab.

Related Topics

Setting Sender Policy Framework (SPF) Options (on page 304)

Setting up an SPF record (on page 305)

Configuring Sender Policy Framework (SPF)

How to get here

The Sender Policy Framework (SPF) page provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses. Use the SPF settings to configure how to process e-mail that is identified as forged e-mail. Settings on the SPF page apply to the selected domain.

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

- **Enable SPF.** Select this checkbox to enable the SPF filter for the current host. Default actions are specified to take for each SPF query result. You can, however, change the defaults by clicking the hyperlink under the SPF result. An Action to be Taken page appears, with the options for that action listed in a list box.
- **SPF Result.** This column lists all possible SPF results possible for this domain.
  - *Fail* (on page 308)
  - *Softfail* (on page 309)
  - *Error* (on page 309)
  - *Temp Error* (on page 310)
  - *Neutral* (on page 311)
  - *None* (on page 311)
  - *Pass* (on page 312)
- **Action to be taken.** This column lists the action chosen for each corresponding query result.
- **Target.** This column lists the mailbox or e-mail address for a Move to or Forward to action, respectively.

- **Prefix Subject.** (Yes/No) This column lists whether or not the message will have an SPF Result prefix added to the message.
- **With.** This column lists the actual prefix, if chosen, for the corresponding query result.

Advanced Options:

- **DNS Timeout** (in seconds). Sets the total amount of time between DNS record checks (lookups).
- **Maximum number of redirects.** Sets the maximum number of redirects allowed when an SPF policy is queried and evaluated.

Save. Click the button to save your changes. An "Update Successful" message and the time of the update appear.

Related Topics

Sender Policy Framework (SPF Filtering) (on page 303)

Setting up an SPF record (on page 305)

SPF community at http://spf.pobox.com (http://spf.pobox.com/)

Setting up an SPF record

Although you do not need an SPF record on your DNS server to evaluate incoming e-mail against SPF policies published on other DNS servers, the best practice is to set up an SPF record on your DNS server. Setting up an SPF record lets other e-mail servers use SPF filtering (if the feature is available on the mail server) to protect against incoming e-mail from forged (spoofed) e-mail addresses that may be associated with your mail server. As SPF records are implemented more widely, SPF filtering will become more effective at identifying spoofed e-mail messages.

About SPF records

SPF records, like MX, A, and PTR records, are included at the DNS domain tree level. These records identify authorized SMTP servers for each domain.

An SPF record consists of the SPF version number followed by strings comprised of mechanisms, prefixes, and modifiers. SPF clients ignore TXT records that do not start with the version string v=spf1.

SPF records are evaluated in a two pass process. First, all mechanisms and prefixes are evaluated, then all modifiers are evaluated. Mechanisms are evaluated from left to right. Modifiers are evaluated on the second pass and can occur anywhere in the record. A generic SPF record takes the format of:

```
version ([prefix] mechanisms) (modifiers)
```

SPF Parameters	Description
v=spf1	SPF version number
all, include, a, mx, ptr, ip4, and exists	Mechanisms. Use one or more in a record string.
"+", "-", "~", and "?"	Prefixes. Precede mechanisms. If a prefix is not included, "+" is implied.
exp	Modifiers. Use 0 - 2 in a record string.

An example SPF record is:

```
v=spf1 +a:mail.domain.com /16 +mx +ptr include:anotherdomain.com
redirect=exampleredirect.com exp=spf-error -all
```

This SPF record includes three directives made up of prefixes and mechanisms:

```
+a:mail.domain.com/16
```

```
+mx
```

```
+ptr
```

```
-all
```

and two modifiers:

```
include:anotherdomain.com
```

```
exp=spf-error
```

Mechanisms identify IP addresses that are authorized to send e-mail from a specified domain. You can use zero or more mechanisms in an SPF record string. Mechanisms usually contain ":" or "/" characters and are case-sensitive. Directives that do not contain "=", ":", or "/" are also mechanisms. Following are mechanism descriptions:

SPF Mechanisms	**Description**
all	Matches all local and remote IPs and goes to the end of the SPF record. Example: v=spf1 +all
include	Specifies other domains that are authorized domains. Example: v=spf1 include:domain.com -all
a	Specifies all IPs in the DNS A record. Example: v=spf1 a:domain.com -all
mx	Specifies all A records for each host's MX

	record. Example: v=spf1 mx mx:domain.com -all
ptr	Specifies all A records for each host's PTR record. Example: v=spf1 ptr:domain.com - all
ip4	Specifies a single IP or an acceptable IP address range. /32 is assumed if no prefix-length is included. Example: v=spf1 ip4:192.168.0.1/16 -all
exists	Specifies one or more domains normally singled out as exceptions to the SPF definitions. An A query is performed on the provided domain, if a result is found a match occurs. Example: v=spf1 exists:domain.com -all

Prefixes designate whether IP addresses pass or fail the SPF lookup test:

SPF Prefixes	Description
+	Pass. The address passed the test. Example: v=spf1 +all
-	Fail. The address failed the test. Example: v=spf1 -all
~	Softfail. The address failed the test, but the result is not definitive. Example: v=spf1 ~all
?	Neutral. The address did not pass or fail the test. Example: v=spf1 ?all

Modifiers provide additional SPF query information and can branch SPF processing. They always contain an "=" character and are case-sensitive. SPF includes two possible modifiers; each can be used once:

SPF Modifiers	Description
redirect	Sends inquiry to another domain. Example: redirect=exampleredirect.com

exp	Sets up an explanation in the SPF record. If an SPF query produces a FAIL result, the explanation is queried and the explanation string provides more information to the nonconforming user. The explanation is typically placed in an SPF log. Example: exp=spf-error

For more information about SPF, go to the *SPF community at http://spf.pobox.com* (http://spf.pobox.com/).

Related Topics

Setting Sender Policy Framework (SPF) Options (on page 304)

Sender Policy Framework (SPF Filtering) (on page 303)

SPF community at http://spf.pobox.com (http://spf.pobox.com/)

SPF Result - Fail

How to get here

The SPF - Fail page allows you to choose an action when the SPF filter is enabled and the result is "Fail." This action activates when the message does not meet the publishing domain's definition of legitimacy.

The action to be taken when the query result is Fail

- **Action.** Select one of the following actions:
- **None.** No action is performed on messages identified as a forged message by the SPF filter.
- **Delete.** Immediately deletes the message.
- **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
- **Insert X- Header (default).** Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
- **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

- **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

SPF Result - Soft Fail

How to get here

The SPF - Soft Fail page allows you to choose an action when the SPF filter is enabled and the result is "Soft Fail." This action activates when the message does not meet a domain 's strict definition of legitimacy, but the domain cannot classify the message as a forgery for certain.

The action to be taken when the query result is Soft Fail

- **Action.** Select one of the following actions:
  - **None.** No action is performed on messages identified as a forged message by the SPF filter.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
  - **Insert X- Header (default).** Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

  - **Prefix subject with.** If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

SPF Result - Error

How to get here

The SPF - Error page allows you to choose an action when the SPF filter is enabled and the result is "Soft Error." This action activates when an error occurred during lookup. The domain 's published records could not be correctly interpreted.

The action to be taken when the query result is Error

- **Action.** Select one of the following action:
  - **None.** No action is performed on messages identified as a forged message by the SPF filter.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
  - **Insert X- Header** (default). Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

  - **Prefix subject with**. If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

SPF Result - Temp Error

How to get here

The SPF - Temp Error page allows you to choose an action when the SPF filter is enabled and the result is "Temp Error." This action activates when a temporary error occurred during lookup. This is a transient error.

The action to be taken when the query result is Temp Error

- **Action.** Select one of the following actions:
  - **None.** No action is performed on messages identified as a forged message by the SPF filter.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
  - **Insert X- Header** (default). Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".

Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

- **Prefix subject with.** If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

SPF Result - Neutral

How to get here

The SPF - Neutral page allows you to choose an action when the SPF filter is enabled and the result is "Neutral." This action activates when a temporary error occurs during lookup. This is a transient error.

The action to be taken when the query result is Neutral

- **Action.** Select one of the following actions:
  - **None.** No action is performed on messages identified as a forged message by the SPF filter.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
  - **Insert X- Header (default).** Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".

Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

- **Prefix subject with.** If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

SPF Result - None

How to get here

The SPF - None page allows you to choose an action when the SPF filter is enabled and the result is "None." This action activates when the queried domain does not publish SPF data.

The action to be taken when the query result is None

- **Action.** Select one of the following actions:
  - **None.** No action is performed on messages identified as a forged message by the SPF filter.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default, messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)
  - **Insert** X- Header (default). Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
  - **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

  - **Prefix subject with.** If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

SPF Result - Pass

How to get here

The SPF - Pass page allows you to choose an action when the SPF filter is enabled and the result is "Pass." This action acitvates when the message meets the publishing domain's definition of legitimacy.

The action to be taken when the query result is Pass

- **Action.** Select one of the following actions :
  - **None.** No action is performed on messages identified as a forged message by the SPF filter.
  - **Delete.** Immediately deletes the message.
  - **Forward to Address.** Forwards the message to a specified e-mail address. Enter an e-mail address in the text box to the right of this option. By default,

messages are sent to the root address and stored in a mailbox called "root-bulk". *Example* (on page 267)

- **Insert X- Header** (default). Inserts an X- Header into the message indicating that the message was identified as a forged message by the SPF filter.
- **Move to Mailbox.** Moves the message to the user's mailbox specified in the text box to the right of this option. If the mailbox does not exist, it is created. The default mailbox is "bulk".



Tip: We recommend that you select the **Insert X-Header** option instead of **Delete** until you know that the SPF options are setup to best suit your filtering requirements.

- **Prefix subject with.** If you want to add a custom prefix subject to messages that are identified as forged, select the **Prefix subject with** check box (cleared by default). The *default subject prefix* (on page 313) is entered in the text box to the right and is based on the SPF query result. You can also enter a custom message in this box.

Default Subject Values for SPF

A prefix value, based on the SPF return code, is added to the message. The default values are if SPF checkbox is enabled:

- **Fail.** Inserts X-Header with [X-IMail-SPAM-SPF-Fail] in subject.
- **Softfail.** Inserts X-Header with [X-IMail-SPAM-SPF- Softfail] in subject.
- **Error.** Inserts X-Header with [X-IMail-SPAM-SPF-Error] in subject.
- **Temp Error.** By default no action taken.
- **Neutral.** By default no action taken.
- **None.** By default no action taken.
- **Pass.** By default no action taken.

This subject field is also user configurable for each possible return code.

Connection Checks

How to get here

Use the options on this page to enable/disable the *DNS black lists* (on page 89) for the current domain. Black lists are not enabled by default, so each new e-mail domain must enable the black lists.

DNS black lists compare the sender information from incoming messages against spam databases to identify spam. DNS black lists must be enabled at the server level before they are made available for use at the e-mail domain level. DNS black lists are then used at the domain level (when bound to an IP address), where administrators can choose which black lists to enable for the host.

After a black list is added, it displays in the **Black List** list. The black lists that are available to add are dependent upon which black lists are configured for the server.

Important: If a black list is not configured at the server level, it will not be available for selection to this page.

Administrators have the option to specify whether a message is deleted if it matches a specific number of standard DNS black lists plus the number of enabled verification checks.

Administrators can review messages that match the DNS black lists. If an e-mail matches the criteria of the black lists, an X-Header is inserted in the message indicating which black list it matched and why. The e-mail is then passed on to content filtering for further examination. The message is delivered if no other rules processing takes place.

The **Trusted DNS Blacklist**, is been combined with the **Connection Checks List**. It displays whether or not the black list is enabled for the domain, the server where the domain resides, and its query domain. The query domain usually matches the server domain name. However, sometimes a black list will contain multiple zones to query on the same server. When this happens, the server name and the query domain will be different. The only way to know this is to read the documentation for the black list being used.

Note: A match made on the **Standard DNS Blacklist** will follow the verification check selections

Domain. Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

Connection Checks List

- **DNS Black Lists.** This column displays all existing black lists for the current domain. Click a black list to modify the black list options.
- **Type.** This column displays the type of lookup that the black list performs.
- **Server.** This column displays the domain name or IP address of the DNS server to contact for the corresponding black list's queries.
- **Query Domain.** This column displays the domain that is queried for the corresponding black list.
- **Trusted.** This check box is selected to enable it as a Trusted Black List.

Note: A match made to the Trusted DNS Blacklist will automatically be deleted.

- **Add.** Click **Add** to *create a new black list* (on page 277) for the current domain. For more information, see *Adding a DNS Black List* (on page 92).
- **Delete.** To delete a black list, select its corresponding check box, then click the **Delete** button.

Verification Checks:

Select any of the following verification tests to perform on incoming e-mail messages. If a message fails any of the checks, an X-Header is inserted into the message.

Note: These options are resource intensive and may slow down mail processing.

- **Verify MAIL FROM Address.** Select this check box to have the "From" address of the connecting server verified for each message to ensure that the user is a valid user on the mail server. If the user or server does not exist, the message is identified as spam.
- **Perform Reverse DNS Lookup for Connecting Server.** Select this check box to create a test in which the IP address of the connecting server is used to perform a reverse DNS lookup to determine the domain name. If a domain has a valid PTR record, the message is accepted. If a reverse lookup fails, it means there is no reverse record for that IP address and the message is marked as spam. An IP address with no PTR record is usually either from a dial-up connection or spoofed message, both of which are indicators of spam. However, keep in mind that a significant number of legitimate mail servers do not have a reverse DNS entry. This may cause legitimate mail to be marked as spam (*false positive*[13]).
- **Verify HELO / EHLO domain.** Select this check box to create a test in which the domain passed during the HELO/EHLO is used to perform a DNS query to verify that the domain specified has an A record or an MX record. If this test fails, an X-Header is inserted into the message.
- **Delete Message after x Matches.** Select this check box to delete the message immediately if it matches x number of black lists plus verification check options. Enter a value that is not greater than the number of black lists plus the number of verification check options that are configured.
- **Prefix Subject with.** Select this check box to create a test in which, if selected, the subject of a message identified as spam by connection filtering is modified from the default text to begin with the text entered in the text box. This option does not apply if the **Delete Message after x matches** is selected and a message meets the criteria for the number of black list and verification check matches.

Important: The SMTPD service does not accept mail from clients that do not begin the SMTP conversation with "HELO" or "EHLO".

Save. Click to save your changes. An "Update Successful" message and the time of the update appear.

Related Topics

Adding to Black List (on page 277)

Server Level Antispam Options (Black Lists) (on page 270)

[13] Many black lists used for connection filtering return hits for domains such as yahoo.com, hotmail.com, and msn.com, among others. If you use these black lists, non-spam e-mail from these domains may be identified as spam and processed according to the specified spam action.

Understanding DNS Black Lists (on page 90)

How Black Lists Work (on page 91)

Setting DNS Black Lists Options (on page 277)

Setting White List Administration Options (on page 242)

IMail SMTP Settings - Control Access (on page 400)

Adding to Black List

How to get here

Before adding to the **DNS Black List** for a domain, be sure that it has been added to the system level DNS Black List, found at **System** > **DNS Black Lists.**

DNS Black List selection will only display items that are enabled. This option is set in the **System > DNS Black List**. By default all items added to the **System > DNS Black List** are enabled.

Note: Disabling a an item in the **System > DNS Black List** will automatically remove it from the **Connection Checks** or **Trusted DNS Black List**. Should the item be enabled at a later date it will automatically re-enable the list in **Connection Checks** or **Trusted DNS Black List**.

Caution: A match made to the Trusted DNS Blacklist will automatically be deleted

Creating a Trusted DNS Black List

1. Click **"Add"** on the **Connection Checks** page, and a pop-up will display all available domains that can be selected for the Black List.
2. Select a domain and click **"OK"**. The selected domain will appear on the Connection Checks list.
3. The **"Trusted"** check box must be checked.
4. Click "**Save"** to save this domain to the Standard DNS Black List.

Note: To easily see all domains that are in the **Trusted DNS Black List**, sort the "Trusted" column (click the column title).

Creating a Standard DNS Black List

1. Click **"Add"** at the **Connection Check** page, and the following list will display all domains available to be added to the DNS black list.
2. Select a domain and click **"OK"**. The selected domain will appear in the Connection Checks list. The "Trusted" check box by default is unchecked.
3. Click "**Save"** to save this domain to the Standard DNS Black List.

DNS Black List (Pop-up)

- **DNS Black Lists.** Select a DNS Black List you want to add. This list is maintained under *System > DNS Black Lists* (on page 89).
- **Type.** Displays the type of lookup that the black list performs from the list box (ADDR, DNS, HELO, RHS).
- **Server.** This column displays the domain name or IP address of the DNS server to contact for black list queries. This field contains an asterisk (*) by default, which indicates that the default IMail Server DNS is used for black list queries, where it relays the DNS query to the DNS server for the black list. Using the asterisk eliminates the need to enter the IP address or domain.
- **Query Domain.** This column displays the domain to query in the zone file. This name usually matches the server domain name. However, sometimes a black list will contain multiple zones to query on the same server. When this happens, the server name and the query domain will be different. The only way to know this is to read the documentation for the black list being used.
- **TCP/IP First**. This shows if TCP/IP First check box has been enabled. This check box allows the administrator to flag a list as one of these types.
- **OK.** Click this button after you have made your selection.
- **Cancel.** Click this button to cancel adding a trusted DNS Black List.

Antispam Logging

How to get here

- **Save Logs To** list. Lets you configure the logging options for the antispam components. Select from four logging options:
  - **No Log**. Select this option to turn off event logging.
  - **spamMMDD.log.** Select to send 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**.**
  - **Log Server.** Select to send event information to the Log file indicated on the Logging tab.
- **Verbose Logging.** Select this option to record more information than standard logging, such as changes to antispam settings and entries in the trusted addresses list or exclude list. This option can create a very large file and may be resource intensive, however, it is especially helpful in troubleshooting issues.

Save. Click this button to save your settings.

Using Antispam Log Entries

IMail Server logs all antispam events, such as error messages, to a separate log file. These events are stored in the log file that is selected in the **Save Logs To** list box in

the *Setting the Antispam Logging Options* (on page 319). The log files also contain text that is returned by a black list if a message's IP address is listed. Other antispam events included in the log file are:

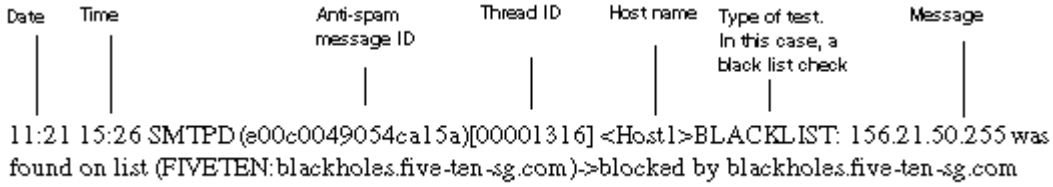
- Enabling/disabling phrase filtering or content filtering
- Initialization of phrase filtering and content filtering for each message
- Verification checks performed on a message and the results
- Connections to DNS black lists and the results of the connection

File Format

The file format for antispam log lines is similar to that of the IMail Server logs, except that antispam log messages also contain an antispam message ID. The generic format of a log file entry is:

```
Date - Time - Anti-Spam Message ID -Thread or Process ID - Host name – Entry Type - Message
```

Example:



File Format for Premium AntiSpam Log Entries

10:17 11:24 SMTP(f593012a00000001) e-mail determined to be spam by Premium filter, Tag = 5AE906968DC04881B0626ADBF612D86F, where Tag is the signature ID of the e-mail that caused the spam.

Thread ID

The thread ID allows you to identify all log entries for specific messages. For example, if you want to identify all log entries for the above example, you would look for every entry that contains the thread ID of (00001316). The thread ID persists across log files so you can find a thread ID in the antispam log and trace the same message in the SMTP log. This is also the same ID that is used to create the Q and D filenames when a message is being processed.

In addition, the thread ID is inserted into the message's X- Header when it is identified as spam .

Setting the Antispam Logging Options (on page 319)

Example Log File (Log_Files_Example.htm)

Antispam Log Messages (on page 319)

Setting the Antispam Logging Options

How to get here

The **Save Logs To** list lets you configure the logging options for the antispam components. Select from four logging options:

- **No Log.** Select this option to turn off the logging of events.
- **spamMMDD.log** (selected by default). Select this option to send 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.
- **Log Server.** Select this option to send event information to the Log Server file indicated on the **Log Files** tab.
- **Verbose Logging.** This option records more information than standard logging, such as changes to antispam settings, and entries in the trusted addresses list or exclude list. This option can create a very large file and may be resource intensive, however, it is especially helpful in troubleshooting issues.
- **Add.** To add a new black list, or edit an existing one, click this button to navigate to the *Add Black List* (on page 92) page.
- **Delete.** To delete an existing black list from the list, select the check box next to the list and click the **Delete** button.
- **Save.** Click to save your settings. An "Update Successful" message and the time of the update appear.

Related Topics

Using Antispam Logs (on page 317)

Antispam X-Header Explanations (on page 330)

Antispam Log Messages

To view a list of all antispam log messages and their explanations, click the following links:

Connection Filtering Log Messages (on page 320)

Content Filtering Log Messages (on page 326)

Log Message Components

Antispam log lines contain all or some of the following components.

- All log messages are preceeded by the following line:

```
month:day hour:minute app_name(connection_ID)
```

- Most log messages also have the following line:

  ```
  [message_id] <domain >
  ```

- Many black list log messages refer to the configured black list as a service and identify the black list by the following line:

  ```
  (name:server :query_domain)
  ```

Connect Filtering Log Messages

BLACKLIST:message_source was found on list (name:server:query_domain)->returned text	The connecting agent sending the message has been found on the specified black list. message_source: This information was sent to the black list server as the source of the message. returned_text: Sometimes the black list server will return text explaining why a message source is black listed.
BLACKLIST:failed to connect to service (name:server:query_domain)	If the black list is configured to use UDP, this means that the initial UDP query sent to the black list server and all retries timed out. If the black list is configured to use TCP, this means that the connection to the server failed.
VALIDATION: (HELO) domain FAILED to receive response from DNS server for HELO domain helo_argument	HELO validation searches for an MX or an A record for the domain passed in the HELO command by the connecting SMTP agent. The queried DNS server failed to respond to the query. helo_argument: The domain passed as the argument to the HELO command by the connecting SMTP agent.

VALIDATION: (HELO) no HELO sent	The connecting SMTP agent failed to send the HELO or EHLO command.
VALIDATION: (HELO) helo_argument domain failed active validation	No MX or A record exists for the domain passed in the HELO or EHLO command. helo_argument: The domain passed in the HELO command by the connecting SMTP agent.
VALIDATION: (MAIL FROM) domain FAILED to resolve MX/A record for mail server mail_from_argument	An MX or an A record could not be found for the sender's mail server. This is a failure since we need the IP address to connect to the mail server and validate the user. mail_from_argument: The e-mail address passed in the MAIL FROM command.
VALIDATION: (MAIL FROM) domain FAILED to connect to remote_mail_server	A connection to the SMTP server for the user passed in the MAIL FROM command was attempted, but failed. The server name was successfully converted to an IP address, but no server exists at the address or it is not running. remote_mail_server: The sender's mail server according to the MAIL FROM command.
VALIDATION: (MAIL FROM) domain FAILED to communicate with server remote_mail server	A connection was made to the remote SMTP server to validate the user, but the connection was terminated or failed. remote_mail_server: The sender's mail server, according to the MAIL FROM command.

VALIDATION (MAIL FROM) no MAIL FROM sent	No MAIL FROM command was sent by the connecting SMTP agent.
VALIDATION:(MAIL FROM) <remote_user> user does not exist on remote system	The user passed in the MAIL FROM command does not exist on the remote server. This is only logged if a successful conversation has taken place and the user is not a valid user on the remote SMTP server. remote_user: The user passed in the MAIL FROM command.
VALIDATION: (MAIL FROM) domain FAILED SMTP server error:mail_server_error	The SMTP server connected to, returned an error prior to validation of the user. The SMTP error is included in the log message. mail_server_error: The SMTP server error returned by the remote SMTP server.
VALIDATION: (REVDNS) connecting_agent address does not have a valid MX or A record, message rejected	The connecting SMTP agent does not have a valid MX or A record. connecting_agent: The IP address of the connecting SMTP agent.
VALIDATION: (REVDNS) domain FAILED to receive reply from DNS server	A query was made to the DNS server for the mail server and no response was retuned. This does not mean that no MX or A record exists for the connecting SMTP agent, just that the DNS server did not respond to queries.

VALIDATION: (REVDNS) domain FAILED reverse DNS validation for address (connecting_agent)	The mail server's DNS server returned a reply to the query for an MX or an A record for the connecting SMTP agent. However, there was no MX or A record. connecting_agent: The IP address of the connecting SMTP agent.
message failed check<check_name> which was marked as trusted, deleting	A trusted black list entry failed its check. The message is immediately deleted. check_name: The display name of the blacklist.
message failed failed_checks of total_checks checks, deleting	Connection filtering is set to delete messages after a specific number of checks have failed (including active validation checks). This number has been reached and the message will be deleted. failed_checks: The number of checks the message failed. total_checks: The total number of checks configured for the host.
Verbose Log Messages	Explanation

BLACKLIST:connecting to service(name:server:query_domain)	This is logged just prior to querying a black list server.
BLACKLIST:retrying service (name:server:query_domain)	This black list uses UDP, so it may not respond in a timely manner. This is logged if a query times out and must be retried.
BLACKLIST:message_source was not found on list (name:server:query_domain)	The connecting agent is not on the specified black list. message_source: This is the information that was sent to the blacklist server as the source of the message.
BLACKLIST:received a reply from service (name:server:query_domain)	The queried black list returned a reply. This does not mean that the message source was blacklisted, just that the query was successful.
VALIDATION: (HELO) domain performing DNS lookup for HELO domain helo_argument	This message is logged prior to performing HELO validation. helo_argument:The domain passed by the connecting SMTP agent.

VALIDATION: (HELO) domain received reply from DNS server for HELO domain helo_argument	HELO validation found an MX or an A record for the domain passed in the HELO command by the connecting SMTP agent. This does not mean that the domain has an MX or an A record, just that the DNS server sent a response to the query. helo_argument: The domain passed in the HELO command by the connecting SMTP agent.
VALIDATION: (MAIL FROM) domain validating MAIL FROM address mail_from_argument	This message is logged prior to performing MAIL FROM validization. mail_from_argument: The e-mail address passed in the MAIL FROM command.
validation: (mail from) domain suceeded for user mail_from_argument.	The user passed in the MAIL FROM command exists on the remote SMTP server. mail_from_argument: The e-mail address passed in the MAIL FROM command.
VALIDATION: (REVDNS) domain performing reverse dns lookup on address connecting_agent	This message is logged prior to performing a reverse DNS validation. connecting_agent: The IP address of the connecting SMTP agent.
VALIDATION: (REVDNS) domain reverse DNS validation SUCEEDED for address (connecting agent)	The DNS server for the mail server returned an MX or A record for the connecting SMTP agent. connecting_agent: The IP address of the connecting SMTP agent.

ADMIN: reloading connection filtering settings for domain:DOMAIN	Connection filtering settings for the specified domain have changed. Only changes in IAdmin or web messaging cause a reload. Hand editing of files is ignored until SMTPD is restarted.
ADMIN: finished reloading connection filtering settings for domain: domain	Connection filtering settings for the specified domain have changed. Only changes in IAdmin or web messaging cause a reload. Hand editing of files is ignored until SMTPD is restarted.

Related Topics

Antispam Log Messages (on page 319)

Antispam Logging (on page 411)

Content Filtering Log Messages

Normal Log Messages	Explanation
No good/spam e-mail in Antispam Table for host<host>. Statistical Filtering Disabled	The host's antispam-table.txt does not contain any words from good or spam e-mail. Statistical filtering is therefore disabled.
No Content Filtering Host Information for the Phrase Filter	There is no content filtering host information for the phrase filter. As a result, no phrase filtering was done.
No Content Filtering Host information for the HTML Filter	There is no host information for the HTML filter. As a result, no HTML filtering was done.
matched phrase[<matched phrase>]	The specified phrase was found in the e-mail.
matched HTML features [<matched features>]	The specified HTML features were found in the e-mail.

matched URL domain[<matched URL domain>]	The specified URL domain was found in the e-mail.
Probability e-mail is spam<e-mail probability>:e-mail is spam	The e-mail has been identified as spam. Also includes its calculated probability.
Probability e-mail is spam<e-mail probability>: e-mail is good	An e-mail has been identified as good. Also includes the calculated probability.
Error:unable to open body file<body file name>	The body file indicated cannot be opened.
Unable to find AntiSpam Host Information for <host>	The specified host's content filtering settings were not found.
[<e-mail address/domain>] in trusted addresses	The sender's address or domain was entered as a trusted address. As a result, no content filtering was done.
Verbose Log Messages	Explanation
Phrase Filtering enabled for<host>	Phrase filtering is enabled for the host.
Phrase Filtering disabled for <host>	Phrase filtering is disabled for the host.
Phrase Filtering initialized for <host>	Phrase filtering was successfully initialized for the host.
Statistical Filtering disabled for <host>	Statistical filtering is disabled for the host.
Statistical Filtering enabled for <host>	Statistical filtering is enabled for the host.
Phrase filtering is disabled or there are no phrases to match	Either phrase filtering is disabled or the phrase list is empty.
HTML filtering is disabled for [<host>]	HTML filtering is disabled for the specified host.
Scanning subject for phrases	Phrase filtering is scanning the subject of a message to check for phrases contained in the phrase list.

Scanning body for phrases	Phrase filtering is scanning the body of a message to check for phrases contained in the phrase list.
statistical filtering disabled	Either statistical filtering is disabled, or there is no content filtering host information.
performing statistical analysis	An e-mail is being statistically analyzed.
The following words were used to compute the probability e-mail is spam	The statistical analysis of an e-mail is done. The most interesting words used (if any) in the analysis follows.
word=<word>, probability=<word hash>	An interesting word and its corresponding probability. It is possible for an e-mail not to have any interesting words. In which case, the calculated probability is 0.5.
[<excluded word>] in exclude list	The specified word was found in the exclude list and will be excluded from statistical analysis.
Added Trusted Address, Content Filtering, and HTML Filtering for <host>	The trusted address, content filtering, and HTML filtering for the host have been added to the anti-spam engine.
Notified <host> about updating the HTML Filter.	The anti-spam engine has been notified about the specified host's HTML Filtering changes.
Notified <host> about updated trusted addresses	The anti-spam engine has been notified about the host's content filtering changes.
Notified <host> about updating the Content Filter.	The anti-spam engine has been notified of the specified host's Content Filtering changes.
Got updated Trusted Addresses, Content Filtering, and HTML Filtering for <host>	The anti-spam engine successfully updated the trusted addresses, content filtering, and HTML filtering for the host.
Got updated Content Filtering for <host>	The anti-spam engine successfully updated the content filtering for the host.
Got Trusted Address, Content Filtering, and HTML Filtering for <host>	The anti-spam engine successfully updated the trusted addresses and content filtering for the host.
Created and Initialized Content Filtering for <host>	The anti-spam engine successfully created and initialized content filtering for the host.

Created and Initialized Trusted Addresses for <host>.	The anti-spam engine successfully created and initialized the trusted addresses for the host.
Added Anti-Spam Host Information for <Hostname>	The anti-spam engine successfully added anti-spam host information for the specified host.
Matched Invalid Tag feature [<invalid tag>]	The e-mail contained the following invalid tag.
Matched Nested Table feature [<table tag>]	The e-mail contained a Nested Table with the specified table tag.
Matched Image Tag feature [<image tag>]	The e-mail contained the following image tag.
Matched Deceptive URL feature [<deceptive URL>]	The e-mail contained the following deceptive URL.
Matched Hyperlink feature [<anchor tag>]	The e-mail contained a Hyperlink with the following anchor tag.
Matched Script Tag feature [<script tag>]	The e-mail contained the following script tag.
Matched Embedded Comment feature [<embedded comment>]	The e-mail contained the following embedded comment. Only 255 characters of the comment are displayed.
Matched Deceptive Text feature [<text>}	The text in the HTML encoded e-mail contained deceptive text.
Updated Phrase List for <domain>	The phrase list for the specified domain has been updated.
Got updated <primary> Phrase list for <domain>	The domain, which is configured to use the primary host's phrase list, has gotten the updated phrase list.
Updated HTML features doe <domain>	The HTML features for the domain have been updated.
Got updated <primary> HTML features for <domain>	The specified domain, which is configured to use the primary's HTML features, has gotten the

	updated HTML feature settings from the primary domain.

Related Topics

Antispam Log Messages (on page 319)

Antispam Logging (on page 411)

Spam X-Header Explanations

When an e-mail message matches a DNS black list, included on the Connection Checks page under the **Antispam** > [select a domain] > **Spam Filtering** > **Connections Checks**, an X-Header line is automatically inserted into the message header to indicate the black list that the message matched.

X-Headers are also inserted when a message fails one of the verification checks set in the **Verification Checks** options on the Connection Checks page.

All other spam features can be configured to insert X- Headers. These X-Headers indicate the spam filter that trapped the message and information about why the message was trapped. Additionally, the message ID is inserted into the message's X-Header when it is identified as spam. See the examples and a table of all antispam X-Headers below.

X-Header Example 1 (on page 297)

X-Header Example 2 (on page 298)

X-Header	Explanation
X-IMAIL-SPAM- ADDRBL:(service >,< message id>,< IP address /reason>)	The message matched an ADDR black list.
X-IMAIL-SPAM- DNSBL:(<name of service>,< message ID>, <IP address/reason>)	The message matched a DNS black list.
X-IMAIL-SPAM- HELOBL:(<name of service>,< message ID>,< IP address/reason>)	The message matched a HELO/EHLO black list.
X-IMAIL-SPAM- HELODOMAIN:(<message ID>,< domain name>)	The message failed the HELO/EHLO domain verification.
X-IMAIL-SPAM- INVALIDFROM: (<message ID>, <from address>)	The message contained an invalid "from" address.
X-IMAIL-SPAM-IP4R: (<message ID>, <name of service>)	The message matched an

	IP4R (PTR) black list.
X-IMAIL-SPAM- STATISTICS:(<message ID>,<spam probability>)	The message has been identified as spam by the statistical filter.
X-IMAIL-SPAM-RHSBL: (<name of service>, <message ID>, <address/reason>)	The message matched an RHS black list.
X-IMAIL-SPAM- PHRASE: (<message ID>, <phrase>)	A phrase in the message matched the phrase list.
X-IMAIL-SPAM- VALFROM:(<message ID>)	The message failed the "MAIL FROM" address verification.
X-IMAIL-SPAM- VALREVDNS:(<message ID>)	The message failed the reverse DNS lookup verification.
X-IMAIL-SPAM- VALHELO	The message failed the HELO/EHLO domain verification.
X-IMAIL-SPAM-HTML- FEATURES:(<message ID>,<found features)	The message contained the specified HTML tags.
X-IMAIL-SPAM-URL- DBL:(<message ID>,<domain>)	The message contained HREF or IMG SRC tags with links to a domain in the URL Domain Black List.
X-IMail-SPAM-Premium	The message contained spam content.
X-IMail-SPAM-SPF- None	The domain did not publish SPF data.
X-IMail-SPAM-SPF- Neutral	The domain published SPF data and returned a "?" value.
X-IMail-SPAM-SPF- Pass	The domain published SPF data and the message met the publishing domain's definition of legitimacy.
X-IMail-SPAM-SPF-Fail	The domain published SPF data and the message did not meet a domain's definition of legitimacy. The message was identified as a forged message by the SPF filter.
X-IMail-SPAM-SPF- Softfail	The domain published SPF data and the message did not meet a domain's strict definition of

	legitimacy, but the domain cannot confidently state the message is forged. The message was identified as a forged message by the SPF filter.
X-IMail-SPAM-SPF- Error	There was an error during the SPF record lookup and could not correctly interpret the error.
X-IMail-SPAM-SPF- TempError	There was an error during SPF record lookup. For example, the server was up, but it gave an error.
X-IMail-Broken-Mime- Header	The message included a broken MIME header.
X-IMAIL-Attachment- Blocked	The message included a file attachment type or MIME type that was selected to be blocked.
X-IMAIL-ThreadID: (<message ID>)	Message written to a mailbox includes a ThreadID to simplify tracing the message path through the logs. The ThreadID corresponds to the ID number placed in the syslogs and the number given to corresponding Q and D files.
X-IMAIL-SPAM-CONFIRMED	Premium Antispam Confirmed X-Header for spam messages from known spam sources.
X-IMAIL-SPAM-BULK	Premium Antispam Bulk X-Header for spam messages from sources that are not confirmed spammers.
X-IMAIL-SPAM-SUSPECTED	Premium Antispam Suspected X-Header for legitimate messages that are sent to slightly larger than average distribution or are unidentified spam messages in the first few seconds of a massive spam outbreak.
X-IMAIL-SPAM-UNKNOWN	Premium Antispam

	Unknown X-Header for messages which Commtouch does not have any incriminating information, and are therefore assumed to represent legitimate correspondence.
X-CTCH-RefID: str=0001.0A01020A.48c14898.006B:SCFSTAT211622a,ss=1,fgs=0	A transaction reference record is added by the IMail Server to the header of every message scanned by Commtouch for technical support purposes.

Related Topics

Using Antispam Logs (on page 317)

Setting Antispam Logging Options (on page 319)

Using IMail Delivery Rules to Filter Spam (on page 220)

Antispam Log Messages (on page 319)

How Black Lists Work (on page 91)

Antispamseeder Utility

Overview (antispamseeder.exe)

The antispamseeder.exe utility, located in the IMail top directory, is used to manage the spam and non-spam word counts contained in the antispam-table.txt file. You can use this utility to modify the antispam-table.txt file in the following ways:

- Re-assign the word counts contained in the `antispam-table.txt` file, when e-mail is incorrectly identified as spam (false positive), or vice versa. This increases the likelihood that such messages will be correctly identified in the future.
- Create a new antispam-table.txt file that applies only to a specific host.
- Add new words to the `antispam-table.txt` file.
- Delete words from the `antispam-table.txt` file that do not occur very often to decrease the size of the file.
- Enter wildcards (i.e. g* *d) into the `antispam-table.txt` file so that statistical filtering will identify such words as spam.

Note: If any of the procedures listed below are performed by a secondary host, that host will either need to copy antispamseeder.exe to the secondary host's directory, or access antispamseeder.exe from the primary IMail domain 's directory.

Procedures:

Resolving incorrectly identified e-mail (on page 339)

Creating a host's antispam-table.txt file (on page 340)

Customizing a host's antispam-table.txt file (on page 342)

Adding new words to the antispam-table.txt file (on page 337)

Modifying the word counts in the antispam-table.txt file (on page 343)

Deleting infrequent words from the antispam-table.txt file (on page 338)

Merging Antispam-table.txt files (on page 336)

Creating URL Domain Black Lists (on page 344)

Simultaneously Merge Domain Links List and Antispam- Table.txt Files (Simultaneously_Merge_Domain_Links_List_and_Antispam_Table_txt_Files.htm)

Identifying wildcards in e-mail (on page 346)

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt file (on page 430)

Preparing Mailboxes for use with antispamseeder.exe

Before a mailbox can be used by antispamseeder to create or alter the `antispam-table.exe` file, several precautions should be taken.

Mailboxes Messages should be Alike

Make sure that each mailbox contains the same type of e-mail messages. For example, one mailbox should contain only spam messages, and another mailbox should contain only non-spam messages.

Mailboxes should be the Same Size

Make sure that all mailboxes contain relatively the same number of e-mail messages. If one mailbox contains substantially more e-mail messages than the other, the word counts will be skewed and content filtering may not function correctly.

Remove Extra Text

You need to clean up all forwarded e-mail messages. Sometimes, a mailbox contains messages that were forwarded by a user (for example, the message was misidentified as spam or should have been identified as spam and the user wants it added to the good word counts). If this is the case, you will need to examine each forwarded e-mail and remove any information that was not included in the original e-mail, before using the mailbox with antispamseeder.exe. Information that needs to be removed is anything that was inserted by the user's e-mail client when the message was forwarded, such as the following:

- Message headers (i.e. To, From, CC , Date, Subject)
- Original message indicators ">"
- Anything that the user inserted into the e-mail including signatures, business cards and comments (for example, "This message was incorrectly identified as spam").

Failure to remove the above items may result in a inaccurate antispam-table.txt file, which will cause statistical filtering to incorrectly identify spam.

Antispamseeder Parameters

The following parameters can be placed in any order within a command.

Command	Function
-c<word count>	Represents the spam count or non-spam count of a word. This can also represent the total number of times the word has occurred in all e-mail messages.
-e<exclude.txt>	Prevents a domain from being added to the URL Domain lack List. Used when you are importing a mailbox into the URL Domain Black List that contains domain names that are not spam.
-good	Identifies the word or mailbox entered as non-spam.
-h<hostname>	Represents the name of the host.
-l	Adds a mailbox or domain to the URL Domain Black List, and updates the antispam-table.txt file. -l can only be used with the spam parameter, not the good.
-lo	Use this parameter to update only the URL Domain Black List.
-m	The mailbox name or path.
-spam	Identifies the word or mailbox entered as spam.
-t<antispam-table.txt>	Identifies the antispam-table.txt file that will be merged with the specified host's antispam-table.txt file. Words that exist in the specified antispam table, but not in the specified host's

	antispam table, are added to the specified host's antispam table.
-w<word>	Represents a word. This is used in conjunction with -c to set the spam or non- spam count of a word within the antispam-table.txt file. It is also used in conjunction with -x to delete a word from the antispam-table.txt file.
-x	Deletes the word specified by the -w parameter from the antispam-table.txt file.

Identifying spam with double byte characters

Some spam contains multi-byte character sets that are not read by IMail. One way to treat all these multi-byte words as spam is to add words of all dashes to the word file. The word file contains words ranging from 4 to 15 characters in length, so you can add a word of each length like this:

```
antispamseeder -spam –w- - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - - -c100 -hdomain.com
```

Merging Antispam-table.txt files

You can use the antispamseeder.exe utility to merge two `antispam-table.txt` files. This is useful when you have modified your `antispam- table.txt` file, but you want to download the latest updated file from the Ipswitch Web site. It is also useful for combining the `antispam-table.txt` files of several domains. Using the procedure below, you can retain your customizations while gaining new statistical information from more recent spam.

To merge two antispam-table.txt files:

1. Identify which antispam-table.txt files you want to merge.
2. Merge the two files by entering the following command in the command prompt substituting the hostname with the name of your mail host, and substituting `antispam-table.txt` with the name of the antispam table that you want to merge with that of the specified host:

antispamseeder.exe –t<antispam-table.txt> - h<hostname>

Example (on page 430)

Note: You can rename the second file, (for example, `antispam-table2.txt`). This is only necessary if you want both files to reside in the same directory. The `antispam-table.txt` files should be placed in the same directory as antispamseeder.exe. If they are in separate directories, you must enter the full path name for the files.
Example:
C:\Program Files\Ipswitch\Collaboration Suite\IMail\Host2\antispam-table.txt.

What happens when you run this command?

First, antispamseeder reads the specified `antispam-table.txt file, and compares it to the antispam-table.txt` file for the specified host. Then, words that are not listed in the host's file are added to it. Since the spam and non-spam word counts for each `antispam-table.txt` file are different, the antispamseeder utility will recalculate the counts for each word that is added to preserve accurate statistics for the word. Therefore, new words are added with the existing word counts, and existing words are **recalculated to** balance the two files word counts.

Related Topics

Antispamseeder Parameters (on page 335)

Installing Updated Antispam Files (on page 265)

Adding a New Word to the antispam-table.txt File

You can use antispamseeder.exe to enter a new word into the `antispam-table.txt` file and to assign a word count to the word.

To enter a new word into the antispam-table.txt file and assign a word count to it:

1 From the command prompt, enter the following command:

```
antispamseeder.exe -w<word (on page 348)> -c<word count (on page 349)>
[-spam|-good] -h<hostname>
```

Note: If neither the `–spam` nor `–good` parameters are entered, antispamseeder.exe will default to
–spam.

Enter a word that does not exist. For the word count, enter a value between 1 and 5.

2 When this is done, the queue manager is notified and the word values contained in the `antispam-table.txt` file are automatically reloaded to include the word that you entered in the above command.

Example (on page 348)

Parameter	Function
-c<word count>	Represents the spam or non-spam count of a word. This can also represent the total number of times the word has occurred

	in all e-mail.
- h<hostname>	Represents the name of the host.
-w<word>	Represents a word/ This is used in conjunction with -c to set the spam or non-spam count of a word within the antispam-table.txt file.
-spam	Identifies the word as spam.
-good	Identifies the word as non-spam.
- m<mailbox>	The name of the mailbox or mailbox path.

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the antispam-table.txt File (on page 430)

Deleting Words from Antispam-table.txt

You can use antispamseeder.exe to delete words, from a host's `antispam-table.txt` file, that occur infrequently. You may want to delete these words to save space and improve content filtering processing efficiency. This command works by eliminating all words that have occurred less than the number of times specified. For more information, see *Understanding the antispam-table.txt File* (on page 430) to determine whether words should be deleted from the Antispam-table.txt file.

To Delete Words from Antispam-table.txt File:

1. Open the antispam-table.txt file, located in the host's directory.
2. From the command prompt, enter the following command:

   antispamseeder.exe -x –c<total word count> - h<hostname>



Note: The number entered for the total word count must be positive.

3. The words that have occurred fewer times than the total word count entered in the command are removed from the antispam-table.txt file.

Example

If you want to remove all words from the antispam-table.txt file that have occurred fewer than five times in all e-mail messages, enter the following command, where "Host1" is the name of the host:

```
antispamseeder.exe –x –c5 -hHost1
```

After running the above command, and reopening the antispam-table.txt file, notice that all words that had previously occurred less than five times are gone.

Parameter	Function
- c<word count>	Represents the spam count or non-spam count of the word. This can also represent the total number of times the word has occurred in all e-mail messages.
- h<hostname>	Represents the name of the host.
-x	Deletes a word from the antispam-table.txt file.

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt File (on page 430)

Resolving Incorrectly Identified E-mail

When IMail Server incorrectly identifies a mail message (false positive), you can use antispamseeder.exe to add statistical information about the e-mail into the antispam-table.txt file to rebalance the spam and non-spam word counts. This will increase the likelihood that similar e-mail messages will be correctly identified in the future.

To change the word tables to recognize messages that are incorrectly identified as spam (or vice versa):

If you have a significant number of messages that are incorrectly identified as spam, you can place the messages in a mailbox and add the entire contents of the mailbox to the antispam-table.txt file at once. The following procedure explains what to do when legitimate messages have been identified as spam:

1. Place all of the incorrectly identified e-mail (non-spam) in a single mailbox. Make sure that this mailbox contains only non-spam.
2. Create the non-spam word counts within the file by entering the following command in the command prompt substituting the hostname and mailbox with your host name and mailbox name that contains the incorrectly identified (non-spam) messages:

```
antispamseeder.exe –good –h<hostname> –m<mailbox (on page 347)>
```

Example (on page 343)

3 The antispam-table.txt in the host's directory is now updated with the new word counts.

Parameter	Function
- h<hostname>	Represents the name of the host.
-spam	Identifies the word as spam.
-good	Identifies the word as non- spam.
- m<mailbox>	The name of the mailbox or mailbox path.

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt File (on page 430)

Modifying the Word Count of Existing Words (on page 343)

Creating Separate antispam-table.txt Files for Multiple E-mail Domains

There may be occasions where a current e-mail domain (IP-ed domain) does not want to use the primary e-mail domain's (IP-ed domain) `antispam- table.txt` file because administrators for each domain do not agree on the words to use for spam. Or perhaps, the administrator for the primary domain is not satisfied with the `antispam-table.txt` file that ships with the product (*Example* (on page 348)). In these cases, the antispam-table.txt file can be altered.

To create spam and non-spam word counts for an e-mail domain:

Use the contents of the `antispam-table-ini.txt` file. This file includes word counts that are created during installation. This file contains the initial word counts; however, it does not contain changes that were made by the primary e-mail domain.

- Use the antispamseeder.exe utility to create new word counts in the antispam-table.txt file for the e-mail domain. This option is used to take the above option a step further to customize the word counts specific to the secondary (current) e-mail domain.

To create a new antispam-table.txt file:

Important: If the current e-mail domain's directory already contains an `antispam-table.txt` file, you must delete it before selecting the **Current Domain** option as shown in the following instructions. If you do not delete it, the antispam-table.txt file will not be copied to the directory and the word counts will not be updated. You can also backup this file to another location in case you decide to revert to it later.

1. Click the **Domain** tab.
2. In the Domains list, select a domain. The Domain Properties appear.
3. In the left navigation bar, click **Spam Filtering**. The Domain Level Antispam settings appear.
4. Click **Statistical Filter**. The Statistical Filter properties appear.
5. In the **Use** list, click **Current Domain**.

Click **Save**.

Note: The contents of the `antispam-table-ini.txt` are placed in the current e-mail domain's directory when the next mail delivery occurs. You can also stop and restart the Queue Manager to speed the creation of this file. The antispam-table-ini.txt is a copy of the primary e-mail domain's `antispam-table.txt file that was created during the installation process.`

Note: `IMail Server reads the antispam-table.txt` file from the current e-mail domain directory each time that content filtering is performed on a message. This file appears in the current e-mail domain's directory.

Tip: To modify the word counts within the `antispam-table.txt` file, use the antispamseeder.exe. For information on how to use this utility see *Customizing an e-mail domain's antispam-table.txt file* (on page 342).

To use the Primary E-mail Domain antispam-table.txt File for a Virtual IP-ed E-mail Domain:

Note: This option is enabled by default upon installation.

1. Click the **Domain** tab.
2. In the Domains list, select a domain. The Domain Properties appear.
3. In the left navigation bar, click **Spam Filtering**. The Domain Level Antispam settings appear.

4 Click **Statistical Filter**. The Statistical Filter properties appear.
5 In the **Use** list, click **Primary Domain**.
6 Click **Save**.

Note: IMail Server reads the `antispam-table.txt` file from the primary e-mail domain directory each time that content filtering is performed on a message. Therefore, this file will not appear in the current e-mail domain's directory.

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt file (on page 430)

Customizing an E-Mail Domain's antispam-table.txt File

To create new word counts specific to the host (e-mail domain), instead of using the `antispam-table.txt` file for the primary host, you must create the `antispam-table.txt` file using known spam and non-spam e-mail.

To create new word counts specific to the host (e-mail domain):

1 Identify the mailboxes you want to use to create the `antispam-table.txt` file. You need at least two mailboxes, one that contains only spam messages and one that contains only non-spam messages. Make sure that each mailbox contains relatively the same number of e-mails.

Note: If one mailbox contains substantially more e-mail messages than the other, the word counts will be skewed and content filtering may not function correctly.

2 Create the spam word counts within the file. Enter the following command in the command prompt substituting the hostname and mailbox with your host name and the name of the mailbox that contains spam messages:

antispamseeder.exe -spam –h<hostname> –m<*mailbox*> (on page 347)

Example (on page 343)

Note: The mailboxes should be placed in the same directory as antispamseeder.exe. If the mailboxes are in a separate directory, you must enter the full mailbox path.

3 Create the non-spam word counts within the file. Do this by entering the following command in the command prompt substituting the `hostname and mailbox` with your host name and the name of the mailbox that contains non- spam messages:

antispamseeder.exe -good –h<hostname> –m<*mailbox*> (on page 347)

Example (on page 343)

4 The antispam-table.txt in the host's directory is now updated with the new word counts.

Parameter	Command
- h<hostname>	Represents the name of the host.
-spam	Identifies the word as spam.
-good	Identifies the word as non-spam.
- m<mailbox>	The name of the mailbox or mailbox path.

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt File (on page 430)

Example - Spam Word Counts

Creating Spam Word Counts using "antispamseeder.exe"

If your host's name is "Host1", and your mailbox name is "spam", you would enter the following command:

- antispamseeder.exe -spam -hHost1 -mC:IMail\Host1\users\root\spam.mbx

Example - Non-Spam Word Counts

Antispamseeder.exe Example (creating the non-spam word counts).

If you have a host named "Host1" and a mailbox named "good", you would enter the following command:

antispamseeder.exe -good –hHost1 -mC:\Program Files\Ipswitch\Collaboration Suite\IMail\Host1\users\root\good.mbx.

Modifying Word Counts of Existing Words

You can use antispamseeder.exe to reassign a word's count in the antispam-table.txt file. You may need to do this if words are being misidentified. This will alter the word counts to increase the likelihood that the word will be identified correctly in the future. For more information, see an *example of why you may need to alter the word count values* (on page 348).

To change the word count of words that are incorrectly identified as spam (or vice versa):

- From the command prompt, enter the following command:

```
antispamseeder.exe –w<word> –c<word count> [- spam|-good] –h<hostname>
```

When this is done, the queue manager is notified and the word values contained in the antispam-table.txt file are automatically reloaded.

Example (on page 348)

Related Topics

Antispamseeder Parameters (on page 335)

Ensuring Mailing List and Newsletter Delivery

To ensure that mailing list messages and newsletters are not identified as spam, place the domain name from which the mailing list/newsletter is sent in *White List (trusted addresses)* (on page 242).

If you do not trust the domain from which the message is sent, you can create a domain rule to *send the message to a folder for the user* (on page 239) (i.e. spam), then the user can create a rule that puts the message in his/her Inbox.

Related Topics

Using Delivery Rules to Filter Spam (on page 220)

Creating URL Domain Black List with antispamseeder.exe

The easiest method to create a URL Domain Black List is to use the antispamseeder.exe utility. Antispamseeder will extract the domain names from the HTML code of collected spam messages. The procedure for doing this is described below.

Creating/Updating the URL Domain Black List Using Antispamseeder

Enter the following command:

Antispamseeder.exe –lo -e<exclude> –h<hostname> - m<*mailbox* (on page 347)>

Where:

- **Exclude** represents the Exclude file.
- **Hostname** is the hostname of the host for which you are updating the antispam-table.txt file and the URL Domain Black List.
- **Mailbox** is the mailbox that contains the spam messages that you want to use to create the URL Domain links list, and the word counts for the antispam- table.txt file. Note that the mailbox must contain only spam messages, because all domain names in the URL Domain Black List are considered spam domains.

Example:

Suppose you have a host named "Host1", and want to update the URL Domain Black List using the messages in a mailbox called "spam". You have also created an exclude file called excludedomains.txt. Enter the following command:

antispamseeder.exe –lo -eexcludedomains.txt –hHost1 –mC:\Program Files\Ipswitch\Collaboration Suite\IMail\Host1\Users\root\spam.mbx

What happens when I run this command?

Antispamseeder examines each message in the "spam" mailbox for HTML code, specifically HREF and IMG SRC tags. When one of these tags is found, the primary domain name is extracted from it and added to the URL Domain Black List. The new URL domain names will appear under the **DNS Black Lists** on the **Antispam** tab > **Connection Checks**.



Notes:
If a domain name is preceded by www, this section is dropped when the domain name is added to the URL Domain Link list by antispamseeder.

We recommend that you add your domain name to the exclude file. Unless you are certain that a domain name does not exist in the mailbox you are using with antispamseeder, you should include the –e<exclude> parameter every time you run a mailbox through antispamseeder with the –l or –lo parameter.

A list of words that are not included to determine whether a message is spam. The words in the exclude list are words that have an equal chance of being non-spam as spam. For example, "Mortgage" is a term frequently used in spam. However, if you work in the financial industry, this term may appear frequently as non-spam. In such a case, you can enter the word "mortgage" into the exclude list. The exclude list should also include common words like proper names. The exclude list is stored in the `exclude-list.txt` file located in the mail domain 's directory.

How do I know which domains to enter?

You should begin collecting spam in a mailbox or use a spam mailbox that you already have. Since most spam contains URL links, you can use these messages to update the URL Domain Black List with antispamseeder.

Related Topics

Simultaneously Merging URL Domain Links and the Antispam-table.txt files (on page 346)

Antispamseeder Parameters (on page 335)

Preparing mailboxes to use with antispamseeder (on page 334)

Creating an Exclude File

Creating URL Domain Black List and Antispam-Table.txt Files

To save time, you can merge a domain's antispam-table.txt file and URL Domain Black List, with those of another domain, at the same time. This is especially convenient if you are using the same mailbox to accomplish both tasks. The procedure is described below.

Enter the following command:

```
antispamseeder.exe –l [e<exclude.txt>] –h<hostname> - m<mailbox (on page 347)>
```

Related Topics

Installing Updated Antispam Files (on page 265)

Antispamseeder Parameters (on page 335)

Using Antispamseeder.exe to identify wildcards

When IMail Server scans an e-mail, it breaks the e-mail down into the individual words. Each character in each word is then checked to make sure it is a valid character. By default, IMail Server does not recognize non-alphabetic characters (except hyphens) or numbers. When comparing words to the antispam-table.txt file, non-alphabetic characters and numbers in a word are treated as the "-" character. So if the word "2Sexy" is found in an e-mail, it is treated as "–sexy" when it is compared to the antispam- table.txt file.

If you want IMail Server to identify such words as spam or non-spam, you must enter them into the antispam-table.txt file using antispamseeder.exe.

To identify words with non-alphabetic characters or numbers as spam or non-spam:

1. From the command prompt, enter the following command:

   antispamseeder.exe –w<*word* (on page 348)> –c<*word count* (on page 349)> [-spam|-good] -h<hostname>
2. The word that you entered in the above command will be identified as either spam or non-spam, depending on which parameter you entered.



Note: The word count must be positive.

Examples:

Example 1 (on page 431)

Example 2 (on page 430)

Parameters

Parameter	Function
-c<word count>	Represents the spam count or non-spam count of a word. This can also represent the total number of times the word has occurred in all e-mail messages.
- h<hostname>	Represents the name of a host.
- w<word>	Represents a word. This is used in conjunction with -c to set the spam or non- spam count of a word within the antispam-table.txt file.
-spam	Identifies the word entered as spam.
-good	Identifies the word entered as non-spam.

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt File (on page 430)

Using the antispam-table.txt File

The `antispam-table.txt` file is the file that contains the spam and non-spam word counts for use with the content filtering feature in IMail Server. When new versions of IMail Server are released, this file is updated to reflect better word statistics.

This installation wizard dialog lets you decide whether to overwrite this file:

- **Merge.** Adds new words to the current `antispam-table.txt` file.
- **Overwrite.** Replaces the current `antispam-table.txt` file with the updated file.
- **Ignore.** Does not install the updated word counts.



Note: You can manually merge the new word counts from the `antispam-table-ini.txt` file into your current `antispam-table.txt file` after installation, using the `antispamseeder.exe` utility. For more information, see the *Antispamseeder.exe Overview* (on page 333).

Modify Subject for URL Domain Black List

By default, the text that is added to the message subject is:

X-IMail-Spam-URL-DBL

Mailbox Path

If the mailbox resides in the same directory as antispamseeder.exe, enter the name of the mailbox (.mbx) that contains the messages that you want to add to the

antispam-table.txt file. If the mailbox does not reside in the same directory as antispamseeder.exe, enter the full path of the mailbox.

Word (defined for the antispam-table.txt file)

Any word you want to add to the antispam-table.txt file must comply with the following rules:

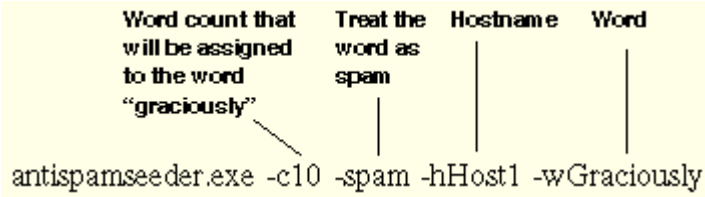
- It must be between 3 and 32 characters.
- It cannot contain any non-alphabetic characters except a hyphen.

Do I need to alter the word tables in the antispam-table.txt file?

The antispam-table.txt file that ships with the product, is appropriate for most users. However, you may need to alter this file if we have identified words as spam that you do not consider to be spam, or vice versa. For example, the word "mortgage" is identified as spam because in our tests, it occurred 370 times in non-spam, and 714 times in spam. However, at financial institutions, the word "mortgage" is a non-spam word that occurs frequently. In this case, you need to alter the antispam-table.txt file so that the antispam engine recognizes the word "mortgage" as non-spam.

Changing the Word Count for a Word (Example)

If you want to alter the entry for the word "graciously" in the antispam-table.txt file so it is treated as spam , enter the following command (where 10 is the word count that you want to assign to the word "graciously", "Host1" is the hostname, and "graciously" is the word).



In essence, you are altering the entry for the word "graciously" in the antispam-table.txt file, therefore increasing the likelihood that this word will be identified as spam in future e-mails.

Before running the above command, the entry for this word looked like this in the antispam-table.txt file:

```
graciously,583326,14,2
```

After running the above command, the entry looks like this in the antispam-table.txt file:

```
graciously,583326,14,10
```

Word count

The word count you want to assign to a word. For example, suppose you enter the following command:

-wstart -c10 -spam -hHost1

The word "start" is now treated as if it has appeared in 10 spam messages.

Troubleshooting

Troubleshooting Antispam

Spam is not being redirected to the mailbox entered in the "Forward To" field

By default, spam is sent to "root-bulk". Root-bulk is a sub-mailbox that did not previously exist on your system. If the host has the **Sub-mailbox Creation** option set to **Bounce** or **Send to Inbox**, then the spam is redirected. See *Setting Domain Properties* (on page 41) for information on how to change the sub-mailbox option.

My Max Mailbox size has been exceeded

If you choose to forward spam messages to a mailbox and receive a large quantity of spam, it is possible that the max mailbox size defined for the mail domain (host) has been exceeded. To remedy this, either delete some of the spam from the mailbox or increase the max mailbox size. To ensure that you are notified of this situation in the future, you may want to set up a Full Mailbox Notify Address, so that you will receive an e-mail when the mailbox is near capacity. For more information, see *Setting Domain Properties* (on page 41).

I am still getting spam

It is not possible for IMail Server to eliminate all spam. It is inevitable that a small percentage will still get through to your mailbox. However, you can adjust the Advanced Statistical filtering options to increase the performance of IMail Server’s antispam component.

There are no black lists available for the host

If there are no black lists displayed on a host’s **Add DNS Black List** list, that means no black lists are enabled at the server level. See *Setting Connection Checks Options (Domain Level Options)* (on page 274) for information on how to enable DNS black lists for the server.

IMail Server is running extremely slow

If you have enabled any of the verification options, this could cause a slowdown. See *Setting Connection Checks Options* (on page 274) for more information on the verification options.

Spam is not being sent to the correct mailbox

Make sure that the mailbox you want spam sent to is entered in the **Forward to Address** field on the *Phrase Filter Options page* (on page 289) and the *Statistical Filter Options page* (on page 284). If the correct mailbox is displayed, check to see if the host has an *inbound delivery rule* (on page 220) that may be trapping the message and sending it to a different mailbox.

Legitimate e-mail is being identified as spam (false positives)

There are several reasons why a legitimate message may be identified as spam. First, make sure that the IP address is not listed in a black list. Do this by examining the message header for the "**X-IMAIL-SPAM:**" line. Second, see if the message failed any verification checks. Sometimes, even legitimate SMTP servers have wrong DNS records. If the message is identified as spam by content filtering, you need to *use the antispamseeder.exe utility to alter the antispam- table.txt file* (on page 333).

Some of my users cannot send outgoing mail

You can do two things to assure that your users' mail is delivered. First, you can enter your mail server's domain name into the trusted addresses list. Second, you can also make sure that the **Enable content filtering for authenticated users** option on the *Setting Domain Level Antispam Options* (on page 182) page is not selected. The second option should only be used if you trust all of your users not to send spam.

I have setup a "Spam" mailbox that all spam messages are sent to, but some of my users cannot see this mailbox. Why?

The "spam" sub-mailbox is not created until the user account receives spam, so it is possible that the account has not received any spam. If the users are POP3 users, they will not see the "spam" mailbox unless they login using the format userid-spam.

Minimizing False Positives

What is a False Positive?

As with any spam product, there is a chance that IMail Server may identify non-spam messages as spam. Such mistakes are called false positives. False positives can occur in both connection and content filtering. *Example* (on page 283)

Why Do False Positives Occur?

False positives resulting from content filtering may include newsletters and other various types of e-mail that people subscribe to. Many of these get caught by the content filters because they may contain ads that look like spam.

How to Prevent False Positives

The following methods are effective in minimizing false positives:

- *White List (trusted addresses)* (on page 242). Add the IP address (or range of addresses), domain names, and e-mail addresses for your network to the trusted address list. Any e-mail received from an IP address in this list will not have connection or content filtering performed on it.
- **Delivery Rules.** Set up *delivery rules* (on page 220) to send spam to a sub-mailbox in each user's directory. To do this, configure *connection filtering* (on page 274) and content filtering *(Phrase Filter* (on page 289) and the *Statistical Filter* (on page 284)) to place X-headers in the message. Then, create a domain rule that searches for a header that contains X- IMAIL-SPAM to place the message in a sub-mailbox (i.e. H~X-IMAIL-SPAM:spam). Users can then make individual rules that move messages back into the main mailbox.
- **Content filtering for authenticated users.** When a client connects to SMTPD32 and authenticates, incoming e-mail is not automatically checked by *connection filtering* (on page 274). If the **Enable content filtering for authenticated users** option on the *Setting Domain Level Antispam Options* (on page 182) page is not selected, mail from authenticated users will not undergo content filtering.

Identifying spam with double byte characters

Some spam contains multi-byte character sets that are not read by IMail. One way to treat all these multi-byte words as spam is to add words of all dashes to the word file. The word file contains words ranging from 4 to 15 characters in length, so you can add a word of each length like this:

```
antispamseeder -spam –w- - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - -c100 -hdomain.com
antispamseeder -spam –w- - - - - - -c100 -hdomain.com
```

Pager Problems

Most problems with pager communications seem to be caused by modem initialization strings. The modem must have the "interface to modem" and "modem to distant end" set to the same baud rate, either 300 or 1200 baud. The modem must have "echo" disabled, "command textual responses" enabled, must return standard Hayes compatible responses, and must accept Hayes compatible commands. The system must be tested at 300 baud.

Once, you've established that the pager works, you can change the baud rate. Modems that return connection information other than "Connect ..." must have the extra connect information turned off. Modems that lock interface speeds must have that option disabled or locked to the desired connect speed (300 baud).

CHAPTER 9

Collaboration

In This Chapter

Collaboration Users 353
Managing Collaboration Groups 356
Public Folders 358
Collaboration Settings 365
Granting Access 366

Collaboration Users

How to get here

You can add, edit, or delete collaboration users, or search for collaboration user account details from the Collaboration Users page.

Search Box. This search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered. Search target includes both the "Name" and "Login Name" columns as criteria for search selection.

Collaboration User List

- **Name**. This column displays the user's account name. This is automatically populated when a new user is added via the *Add IMail User* (on page 143) page. If you click the link under the User's Name, the *Collaboration User Account Details* (on page 354) page appears.
- **Login Name**. This column displays the name the user logs in with. This is automatically populated when a new user is added via the *Add IMail User* (on page 143) page.
- **Email**. Displays the associated e-mail address. This is automatically generated when a new user is added through the *Add IMail User* (on page 143) page.

Add. Click **"Add"** to manually create a new collaboration user.

Delete. Click this button after selecting a user from the list to delete.

Related Topic

Add Collaboration User (on page 354)

Add Collaboration User

How to get here

Clicking the **Add** button on the Collaboration Users page will bring up a pop-up to allow adding a new Collaboration user.

- **Name.** Enter the user's account name in the text box.
- **E-mail.** Enter the user's E-mail address in the text box.
- **Login Name.** Enter the name with which the user logs into the system.
- **Password.** Enter a password for this user into the text box.
- **Confirm Password**. Re-enter password to verify correct spelling.

Save. Click this button to save your changes.

Cancel. Click this button to exit without saving changes.

Collaboration User Account Details

How to get here

Clicking the **Add** button on the Collaboration Users page will bring up a pop-up to allow adding a new Collaboration user.

- **Name.** Enter the user's account name in the text box.
- **E-mail.** Enter the user's E-mail address in the text box.
- **Login Name.** Enter the name with which the user logs into the system.
- **Password.** Enter a password for this user into the text box.
- **Confirm Password**. Re-enter password to verify correct spelling.

Save. Click this button to save your changes.

Cancel. Click this button to exit without saving changes.

Related Topics

Collaboration Users (on page 353)

Collaboration User Folders & Access (on page 354)

Granting Access to a User's Personal Folders (on page 355)

Collaboration User Folders and Access

How to get here

This page displays a specified Collaboration User's personal folders that are available for sharing, as well as other folders that are accessible to this user. The page appears when you click the user name link on the *Collaboration Users* (on page 353) page.

- **Account Name.** This is populated by selecting a specific Name on the Collaboration Users page.
- **Account E-mail.** This is populated by the corresponding user's e-mail address on the Collaboration Users page.
- **This user's personal folders that are available for sharing.** This area displays this user's folders available for sharing. Clicking on a folder will display in box below all Users / Groups with access.
  - **Users or Groups with access to the selected folder**. Selecting a personal folder will display all users with permissions to this folder.
- **Other folders accessible to this user.** This area displays other public folders accessible to this user, and allows you to:
  - **Grant this user rights to a public folder**. Click this link to navigate to Public Folders. You can then select any of the folders in the list and provide access for the specified user.

Granting Access to a User's Personal Folders

You can either grant or change access to a user's personal folders (made available for sharing by the user) via the **Collaboration Users** page.

To grant access to a user's personal folders:

1. From the **Collaboration** tab, select **Manage Collaboration Users**. The **Collaboration Users** page appears.
2. Click the **User Name** to be modified. The **Collaboration User Folders and Access** page appears.
3. There are two views available:
   - This user's personal folders that are available for sharing
   - Other folders accessible to this user
4. Click the personal folder under **This user's personal folders** to view all Users and Groups with access to the selected folder. The Folder Properties page appears.
5. Click **Edit Access Permissions** hyperlink to add or edit access permissions. The Folder Properties page appears displaying all users with access permissions.
6. Click the **Add** button. The **Access Level** page appears with all collaboration users and groups available for access setting.
7. From the **Collaboration Users/Groups** check boxes, you can select all (selects only the current page), or select individual users and groups.
8. From the **Access Level** list box, select one of the following access levels you wish to assign to those users/groups.
   - read
   - read, create
   - read, create, edit
   - read, create, edit, delete
9. Click **Save**. The selected users and groups are displayed on the Folder Properties page.
10. If you are satisfied with the users and groups, click **Save**.

Managing Collaboration Groups

How to get here

Use the **Collaboration Groups** page to create, edit, delete, or search for collaboration groups. Creating Collaboration Groups is a convenient way of organizing certain users with common attributes. For example, you might create a group that contains all the human resources staff. Once you have created a group, you can use it when specifying access (read, create, edit, or delete) to a particular folder or subfolders. For example, you can grant access for a group to a particular folder, or alternatively, you can grant access for a user to a particular group. The latter method will grant the specified user access to every folder belonging to every member of the specified group.

- **Search Box.** This search will automatically begin narrowing the list of users. The search assumes a wildcard automatically after the characters entered. Search target includes both the "Name" and "Login Name" columns as criteria for search selection.
- **Name.** Displays all current collaboration groups.

Add. Click this button to *add a new group* (on page 356).

Delete. Click this button to *delete a group* (on page 357).

Related Topics

Adding a New Collaboration Group (on page 356)

Deleting a New Collaboration Group (on page 357)

Adding a New Collaboration Group

You can only navigate to this page by clicking the Add button on the *Collaboration Groups* (on page 356) page.

To add a new collaboration group:

1. Enter the **Name** for the new group, and click **Save**. This will create the new group and allow new users to be added.
2. Click the **Add** button and the Add Group Members page appears.
3. Choose the members for this new group from the list by selecting the check box to the left of each name. You can either **Select All** by selecting the check box, or you may select one or more individual Collaboration Users from the list.
4. Click **Save** at the bottom of the page. The Group Properties page displays the new users listed.
5. Click **Save** to save your group name change or click **Return To All Groups** to return to the *Collaboration Groups* (on page 356) page displays your new group.



Note: Changing the group name will not apply unless **Save** is clicked. Adding and deleting from a group is saved immediately after adding.

Granting Access to Group

You can either grant or change access to a group or user (made available for sharing by the user) via the **Collaboration Group** page.

To grant access to a group:

1. From the **Collaboration** tab, select **Manage Collaboration Groups**. The **Collaboration Group** page appears.
2. Click the **Group Name** to be modified. The **Group Properties** page appears.
3. There are two views available:
   - **Group Properties** - Members of the group
   - **Access Permissions** - User's with access to group
4. Click **Access Permissions** to display all Users and Groups with access to this item.
5. Click **Add** or click the existing User/Group to Edit. The **Access Level** page appears.
6. From the **Access Level** drop down, select one of the following access levels:
   - Read
   - Read, Create
   - Read, Create, Edit
   - Read, Create, Edit, Delete
7. From the displayed **User/Group** you can select all (selects only the current page), or select individual users and groups check boxes.
8. Click **Save**. The selected users and groups are displayed on the **Access Permissions** page.

Deleting a Collaboration Group

You can only navigate to this page by clicking the **Delete** button on the *Collaboration Groups* (on page 356) page.

To delete a collaboration group:

1. Select a group on the *Collaboration Groups* (on page 356) page. Click the **Delete** button at the bottom of the page.
2. The following message appears: Are you sure you want to permanently **Delete the following Group(s): <name(s) of groups>**.
3. Click **Delete** at the bottom of the page.



Note: If you don't want to continue deleting, click **Cancel** at the bottom of the page.

4. The *Collaboration Groups* (on page 356) page no longer displays the group in the list.

Public Folders

How to get here

The Public Folders page allows you to manage public access and sharing in Calendar, Contacts, Mail, Notes, and Tasks. It allows you to add (create), update, delete, or view public folders. Public folders are folders that are made available to selected users and groups, and are an effective way to collect, organize, and share information with other people. You can use them to store items, such as calendars, contacts, tasks, etc., which are shared by two or more people.



Note: Web client will only display shared contacts and calendars.

A useful example of a public folder is a public contacts folder, where all specified staff will have access to the organization- wide list of contacts. Another example is a public calendar, which lets all staff know when a meeting room is available or in use. When you create a public folder and give, minimally, read access to a user, the folder will appear in the user's calendaring tool the next time they synchronize.

- **Folder Name.** This column displays existing public folders.
- **Type.** This column displays the type of public folder corresponding to the folder name -- either Calendar, Contacts, Mail, Notes, or Tasks.

Add (on page 358). Click this button to create a new public folder. the *Folder Properties* (on page 358) page to add a new folder. After user/group information is entered into the text boxes and saved, the new folder information appears on the Public Folders page.

Delete. Select a check box next to a folder you want to delete, then click this button to delete the folder.

Related Topics

Select Users and Groups Folder Access (on page 359)

Granting Access to Public Folders (on page 364)

Public Folder Properties

How to get here

The Folder Properties Page allows you to add, update, delete, or view the details of public folders for the specified domain.

- **Folder Name.** This column displays existing public folders.
- **Type.** This column displays the type of public folder corresponding to the folder name -- either Calendar, Contacts, Mail, Notes, or Tasks.
  - **[Edit Contacts]** (on page 360). Displays only for public folders set as **Contacts**. Click this link to easily add and remove contacts and groups.

- **Parent.** Selection is not required, and will become a parent folder. Select the Parent folder from the list box. The list box contains a list of all existing Public Folders.
  - **Inherit Access from Parent.** Select this check box if you want this new public folder to allow the newly created folder to inherit the same access rights as the selected parent folder.

Users and Groups Access Rights List

- **User/Group.** This column lists the users and groups that have access rights to the specified folder.
- **Access.** This column lists the level(s) of access the user or group has to the specified folder, i.e. Read, Create, Edit, Delete, or combinations of those levels.
- **Add.** Click **Add** to be taken to *Allow Access to Users and Groups for this item* (on page 359).
- **Delete.** Click Delete after selecting the check box next to the User/Group to remove access from the specified folder.

Save. Click this button to save your settings.

Cancel. Click to cancel changes and return to the Public Folders page.

Related Topics

Public Contacts Folder [Edit Contacts] (on page 360)

Allow Access to Users and Groups

How to get here

- **Item.** Displays the specific folder to which you are giving access.
- **Access Level.** Select the appropriate access level from the list box. The levels are:
  - **Read.** Users/Groups with Read Access can only read shared information.
  - **Read, Create.** Users/Groups with Read, Create access can read and create new information. However, they cannot edit or delete it.
  - **Read, Create, Edit.** Users with this level of access can read, create, and edit information, but cannot delete it.
  - **Read, Create, Edit, Delete.** Users with this level of access can read, create, edit, and delete information.
- **Select All.** Click this check box if you want to select all of the users displayed in the list.
- **User / Group.** Select the check box next to the specific name(s) for whom you want to allow folder access.

Save. Click to save your settings.

Cancel. Click to cancel your settings.

Public Contacts Management

How to get here

The Public Contacts Page allows full administration of the public contacts folder for the selected domain. You can easily add and remove existing IMail Users, Collaboration Groups, and New Contacts.

Public Contacts List

Search Box. Typing will automatically begin narrowing the list. The search assumes a wildcard automatically after the characters entered.

Caution: Search requires a minimum of two characters for the search process to begin.

Note: Column Titles when clicked will sort the list for the current session only. Refreshing the page will reset the original sort.

- **Name.** This column lists the users and groups that have access rights to the specified folder.
- **Address.** This column lists the level(s) of access the user or group has to the specified folder, i.e. Read, Create, Edit, Delete, or combinations of those levels.

IMail User (on page 361). Click to display all available IMail Users for specified domain.

New Contact (on page 361). Click to add a contact that is not a user within the specified domain.

New Group (on page 362). Click to create a Contacts Group, which allows sending a message to a group of addresses.

Note: Public Contacts groups should not be confused with Collaboration groups, which controls permissions access for Collaboration User's contacts and Public Folders.

Delete. Click Delete after selecting the check box next to the User/Group to remove access from the specified folder.

Done. Click this button to return to the Public Folder Properties page.

Related Topics

Public Folder Properties (on page 358)

Public Folder - Access Rights

Adding IMail Users to Public Contact Folder (on page 361)

Creating New Contact for a Public Contact Folder (on page 361)

Creating a New Group within a Public Contact Folder (on page 362)

IMail User Selection

How to get here

The IMail User page will display all IMail Users for the selected domain that are currently not on the public contacts folder being updated.

Clicking column titles will sort ascending/descending. This will allow all System Admins, Domain Admins, List Admins, or Disabled Accounts to sort to the top of the page.

IMail Users List

- **Full Name.** This column lists all available IMail Users for selected domain.
- **Email.** Displays e-mail address of the IMail User.
- **System Admin.** Displays "Yes" or "No" depending on IMail User having System Administrator permissions.
- **Domain Admin.** Displays "Yes" or "No" depending on IMail User having Domain Administrator permissions.
- **List Admin.** Displays "Yes" or "No" depending on IMail User having List Administrator permissions.
- **Enabled.** Displays "Yes" or "No" depending on IMail User's having a disabled account.

Save. Click to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

New Contact for Public Contacts

How to get here

The New Contact page will allow adding a new contact to the Public Folder selected.

Primary Information

- **First Name.** Enter First Name of the New Contact for selected domain.
- **Last Name.** Enter Last Name of the New Contact for selected domain.
- **Email Address.** Enter Email Address of the New Contact for selected domain.

Company Information

- **Company Name.** (Optional) Enter Company Name of the New Contact for selected domain.
- **Job Title.** (Optional) Enter the Job Title of the New Contact for selected domain.

- **Department.** (Optional) Enter the Department of the New Contact for selected domain.

Phone Numbers

- **Home Phone.** (Optional) Enter the Home Phone of the New Contact for the selected domain.
- **Mobile Phone.** (Optional) Enter Mobile Phone of the New Contact for selected domain.
- **Business Phone.** (Optional) Enter Business Phone of the New Contact for selected domain.
- **Business Fax**. (Optional) Enter the Fax number of the New Contact for the selected domain.

Home Address

- **Street.** (Optional) Enter Home Street Address of the New Contact for the selected domain.
- **City.** (Optional) Enter Home City of the New Contact for the selected domain.
- **State.** (Optional) Enter Home State of the New Contact for the selected domain.
- **Zip Code.** (Optional) Enter Home Zip Code of the New Contact for the selected domain.
- **Country.** (Optional) Enter Home Country of the New Contact for the selected domain.

Business Address

- **Street.** (Optional) Enter Business Street Address of the New Contact for the selected domain.
- **City.** (Optional) Enter Business City of the New Contact for the selected domain.
- **State.** (Optional) Enter Business State of the New Contact for the selected domain.
- **Zip Code.** (Optional) Enter Business Zip Code of the New Contact for the selected domain.
- **Country.** (Optional) Enter Business Country of the New Contact for the selected domain.

Save. Click to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

New Groups for Public Contacts

How to get here

The New Groups page allows the IMail Administrator to organization contacts into groups. The New Groups page was designed to manage the creation, maintenance and deletion of all Groups.

The Group Contacts pages has two displayed boxes.

- The left display contains all contacts that currently exist in the Public Contact folder.
- The right display (empty when new) contain all contacts for the Group.

Button Selection

 **(Add to Group)**. Select contact and click to add a member to the group.

 **(Remove from Group)**. Select group member and click to remove a member from the group. If group member was only a recipient (not a contact), then this will permanently remove the recipient from the group after saving.

 **(Add All to Group)**. Click to add all contacts in list to the group.

 **(Remove All From Group)**. Click to remove all group members (from the list on the right) from the group.

 **Note:** Removing a group member (recipient) that does not exist in the contact list, will remove the group member permanently after saving.

Group Options

- **Group Name**. Enter the name for your new group in the text box.
- **Select Public Contact Folder**. From the drop down list box, select any of the other Public Contacts folder you need to for your new Contact Group.

Public Contacts List

- **Name**. This column displays the corresponding names of the selected Public Contact folder that are not currently in the group.
- **Address.** This column displays all e-mail addresses from the selected Public Contact folder that are not currently in the group.

Group Member List

- **Name.** Group member name.
- **Address.** Group member e-mail address.

Create a New Contact.

Add a New Address (on page 364). This will allow adding any e-mail address to a group that does not exist in the selected Public Contact folder. Clicking will pop up a window to add a new contact to the group.

Save. Click to save your settings.

Cancel. Click **Cancel** to exit without saving changes.

Adding a New Contact to a Group

You can add a new contact to a group by clicking the **Add a New Address** link on the Contact Groups page.

- **Name**. Type the name of your new contact in the text box.
- **Email**. Type the e-mail address of your new contact in the text box.l
- **Create a New Contact** (Checked by default).
  - **Create a New Contact (Checked).** Will create a new contact and will also add as recipient to the group.
  - **Create a New Contact (Not Checked).** Will **not** add to the contact list; will only add this address as a recipient to the group.

Save. Click to add the new contact to the Group Members column.

Cancel. Click to cancel your changes.

Granting Access to Public Folders

To grant or change access to a public folder:

1. From the **Collaboration** tab, select **Public Folders**. The **Public Folders** page appears.
2. All shareable **Public Folders** are displayed in the **Folder Name** column. Click the public folder you wish to share. The **Public Folder Properties** page appears, listing existing users and groups that have access to the selected folder.
3. Click the **Add** button at the bottom of the page. The **Access Level** page appears, displaying all users that do not currently have access.
4. From the **Access Level** list box, select one of the following access levels you wish to assign to those users/groups:
   - Read
   - Read, Create
   - Read, Create, Edit
   - Read, Create, Edit, Delete
5. From the **Users/Groups** check boxes, you can select all (selects only the current page), or select individual users and groups.
6. Click **Save**. The selected users and groups are displayed on the **Public Folder Properties** page.

Collaboration Settings

How to get here

Use this page to set and modify the Collaboration settings for the Client and Server , the log settings, the synchronization options for attachments and appointments, and to allow users to self-administer their client folders.

Client Update Settings

Specify the number of minutes between automatic client updates.

- **Update Frequency (minutes).** In the text box, enter the number in minutes of how frequently the client will connect to the Collaboration server in order to synchronize.
- **Clients may set their own synchronization schedule.** Select the check box to allow users to set their own synchronization schedules. Users will be able to set their own schedules for synchronization in their Outlook client.

Server Settings

Specify the interfaces and the port that the Collaboration server will listen on.

- **Interface.** The list box defaults to **All Interfaces,** however, if the server has more than one IP address, you can listen on that specific interface by selecting the appropriate IP address from the list box.



Note: You might typically want to change from All Interfaces to a specific IP address if the server is connected to both the LAN and directly to the Internet on different interfaces, and you only want the server to listen on the local interface.

- **Listen On.** Choose one of three options:
  - **Unsecure port only.** Select this option if you want to listen only on an unsecure port.
  - **Secure port only.** Select this option if you want to listen only on a secure port.
  - **Both secure and unsecure ports.** Select this option if you want to listen on both unsecure and secure ports.
- **Unsecure Port.** In the text box, enter the port number for non-secure communications. The default port number is 8100. You will not be able to enter anything in the text box if you have chosen the **Secure port only** option.
- **Secure Port.** In the text box, enter the port number for secure (SSL) communications. The default port number is 8101.



Note: If you change either the Interface or the Port setting, you must re-run the client setup program on all client computers so they will recognize the new settings.

Log Settings

- **Log Communications.** Select this check box if you want to configure the server to log every transaction with each client to a log file. The file will contain general details of transactions between the server and the clients.
- **Verbose Logging.** Select this check box if you want the log file to contain specific details for each record. You will be unable to select this check box if the **Log Communications** check box is clear.

Attachment Synchronization

- **Synchronize attachments and images on contacts, appointments, and tasks.** Select this option if you want to synchronize attachments and images associated with contacts, appointments, and tasks.
- **Synchronize attachments and images on e-mail.** Select this option if you want to synchronize attachments and images for e-mail.



Note. Be aware that such items may be large and might take considerable bandwidth and storage when synchronizing. You can select neither, one, or both of the options above.

Appointment Synchronization

- **Synchronize all appointments.** Select to allow users to synchronize all their appointments.
- **Synchronize appointments from specified number of weeks in the past.** Select to allow users to synchronize all their appointments from a specified number of weeks in the past. Enter the desired number in the text box.

Client Folder Administration

Select one of the following to allow users to administer access to their folders (via the Outlook client) or not:

- **Users can administer access to their folders by default**
- **Users cannot administer access to their folders by default**

Save. Click to save your settings.

Granting Access

Select the Access Type:

- *Granting Access to a User's Personal Folders* (on page 355)
- *Granting Access to Group* (on page 357)
- *Granting Access to Public Folders* (on page 364)

CHAPTER 10

Services

In This Chapter

Service Administration Overview 367
Premium Antispam (Commtouch) 371
IMAP Settings 373
LDAP 375
POP3 382
Queue Manager 386
SMTP 392
Web Calendaring (Old) 407

Service Administration Overview

How to get here

IMail Service Administration lets you manage a number of system services. The **Service Administration** page lets you get a quick overview of these services and their status.

The list shows which services are installed. Each service, its version number, and its current state (**Stopped** or **Running**) is displayed. You can use the check boxes to the left of the **Name** list to stop and start individual services. By selecting or clearing all check boxes at once, you can also stop or start all services simultaneously. You can also click the link under any service to access its settings page.



Tip: Starting or Stopping multiple services may take a minute.

- **IMail IMAP4 Server Service (on page 373).** Select this check box to let users access remote message stores (on the mail server) as if they were local. Using an IMAP4 mail client, users can read their mail, move or delete mail, create mailboxes - all on the server system.



Note: IMail Web Messaging directly accesses the server to manage mail, and no longer requires IMAP.

- **IMail LDAP Service (on page 375).** Select this check box to publish and provide access to user information on the server, and extend the IMail user database to include standard LDAP attributes such as name, address, organization name, and phone number. LDAP allows each user with an account on the system to add, delete, or modify information in his/her own LDAP entry.
- **IMail POP3 Server Service (on page 382).** Select this check box to let any POP3 mail client communicate with IMail Server.
- **IMail Queue Manager Service (on page 386).** Select this check box to control the flow of messages through the mail queue. The Queue Manager service is a component of the SMTP delivery process.
- **IMail SMTP Service (on page 392).** Select this check box to let the the SMTP server send and receive mail from other Internet hosts using the Simple Mail Transfer Protocol (SMTP) and process all incoming and outgoing mail.
- **Symantec Anti-Virus Scan Engine** (on page 252) (available separately). Select this check box to provide consistently current, premium anti-virus protection.
- **Premium Anti Spam Service** (on page 371) (available only with IMail Premium). Select this check box to provide automatically updated, language-aware premium anti-spam technology.
- **IMail Sys Logger Service (on page 411).** Select this check box to view the log files in the IMail spool directory.
- **IMail WorkgroupShare Service** (on page 353). Select this check box to enable shared Microsoft Outlook calendars and global address books.
- **IMail Commtouch AS Service** (on page 371) (available only with IMail Premium). Select this check box to provide automatically updated, language-aware premium anti-spam technology.
- **IMail Commtouch IP Rep Service** (on page 371) (available only with IMail Premium). Select this check box to provide automatically updated, language-aware premium anti-spam technology.
- **IMail Web Calendar Service (on page 407).** This service is only required for the old Web Calendar from v10 and earlier. Running this service will allow a link to display in the Web Client to give access to the old Web Calendar. Select this check box to let users store schedules, set appointments, and send e-mail date reminder information using a web browser.



Note: Web Calendar no longer requires a service. Running this service will allow a link to display in the Web Client to give access to the old Web Calendar.

- **Ipswitch Instant Messaging Server**. Select this check box to enable secure instant messaging with Smart Tag

Related Topics

Viewing Service Status from a Web Browser

Click the **Services** tab. The Service Administration page appears. Look in the **Current State** column corresponding to the row for the specific service.



Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), and a Start/Stop button appears. This allows you to Start or Stop individual Services from their respective web pages, as well as from the Service Administration page.

Configuring IMail Services (on page 369)

IMail Administrator Services (on page 370)

Configuring IMail Services

To start a service , select the check box to the left of that service and click **Start**. To stop a service, select the check box to the left of that service and click **Stop**.

To verify that you have successfully stopped or started a service, a page with a progress bar appears. The Service Administration page displays the service's new status.

Viewing the Status of IMail Services

Click the **Services** tab. The Service Administration page appears. Look in the **Current State** column corresponding to the row for the specific service.



Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), and a Start/Stop button appears. This allows you to Start or Stop individual Services from their respective web pages, as well as from the Service Administration page.

Logging into IMail Services

Before you can access the Service Administration page, a separate dialog may appear during each browser session prompting you for a Windows User name and Password. This depends on your platform and security settings.

- If the dialog box does not appear, the Services Administration page opens.

- If the dialog box does appear, enter the administrator user name (administrator for the computer) and password. The Services Administration page opens.



Setting Service Administration Options

How to get here

IMail Service Administration lets you manage a number of system services. The **Service Administration** page lets you get a quick overview of these services and their status.

The list shows which services are installed. Each service, its version number, and its current state (**Stopped** or **Running**) is displayed. You can use the check boxes to the left of the **Name** list to stop and start individual services. By selecting or clearing all check boxes at once, you can also stop or start all services simultaneously. You can also click the link under any service to access its settings page.

Tip: Starting or Stopping multiple services may take a minute.

- **IMail IMAP4 Server.** Select this check box to start this service, which lets users access remote message stores (on the mail server) as if they were local. Using an IMAP4 mail client, users can read, move, delete mail, and create mailboxes all on the server system.

Note: IMail Web Messaging directly accesses the server to manage mail, and no longer requires IMAP.

- **Ipswitch Instant Messaging Server.** Select this check box to stop or start IIM . If you click the link, the IIM Home page appears.

- **IMail Web Calendar Service** (Applies only to the old Web Calendar). Select this check box to let users access Web Calendar, which allows them to store schedules, set appointments, and send e-mail date reminder information using a web browser.



Note: Web Calendar no longer requires a service. Running this service will allow a link to display in the Web Client to give access to the old Web Calendar.

- **IMail LDAP Service.** Select this check box to publish and provide access to user information on the server, and extend the IMail user database to include standard LDAP attributes such as name, address, organization name, and phone number. LDAP allows each user with an account on the system to add, delete, or modify information in his/her own LDAP entry.
- **IMail POP3 Server.** Select this check box to let any POP3 mail client communicate with IMail Server.
- **IMail Queue Manager Service.** Select this check box to control the flow of messages through the mail queue. The Queue Manager service is a component of the SMTP delivery process.
- **Premium AntiSpam Service.** Select this check box to enable Commtouchs Advanced Security Daemon (a.k.a. ctasd™). (Available only with IMail Premium)
- **IMail SMTP Server.** Select this check box to allow users to let the SMTP server send and receive mail from other Internet hosts using the Simple Mail Transfer Protocol (SMTP) and process all incoming and outgoing mail.
- **IMail Sys Logger Service.** Select this check box to allow users to view the log files in the IMail spool directory.
- **Ipswitch WorkgroupShare Service.** Select this check box to enable Collaboration.

Premium Antispam (Commtouch)

How to get here



Note: This Service page includes services for both the **Premium Antispam "IMailCommtouchAS"** and **Commtouch IP Reputation "IMailCommtouchIPRep"**.

Use the Commtouch Antispam Settings page to stop and start the **IMailCommtouchAS** and/or the **IMailCommtouchIPRep** service.

This page displays Commtouch license information, configuration settings for Commtouch Advanced Security Daemon (ctasd™), and port settings for both Commtouch's IP Reputation port and Premium Antispam.



Note: Go to **Antispam > Premium Filter** to enable and set *Commtouch Classification* (on page 280) filters.

License Information

- **License Type**. Displays either as a paid subscription or trial evaluation.
- **Days Left**. Number of days left before license expires.

Server Settings

- **Port**. Premium Antispam listening port number. (Default port is 8088)
- **IP Reputation Port**. The HTTP listening server port number. (Default port is 8181)

Proxy Server Settings

- **Enable.** Check box to enable proxy server settings. (Default not enabled)
  - **Port**. Port number used for connectivity with the proxy server.
  - **Server Address**. Specifies the host name or IP address of the proxy server.
  - **Auth**. Specifies the authentication mode for connectivity with the proxy server. Options are Basic or NoAuth.
  - **Username**. The name of an authorized user.
  - **Password**. The password of the authorized user.

Save. Click the save button at the bottom of the screen. A message at the top "Your changes have been saved" will confirm.

Related Topics

IP Ignore List (on page 372)

Commtouch Premium Antispam Filter (on page 280)

IP Ignore List

How to get here

The IP ignore list contains a list of IP addresses of all local mail servers that should automatically be considered non-spammers and should not be validated for spam. When checking the servers from which the suspected message originated, ctasd™ ignores all references to local or remote mail servers predefined in the IP ignore list.



Note: Updating this list requires restarting the **IMailCommtouchAS** service.

- **IP Address.** This column lists all the local mail servers currently set to be considered non-spammers.
- **Subnet Mask.** This column lists the Subnet Masks related to the IP Addresses**.**

Add. Click this button to access the Add **IP Ignore List** page.

Delete. Click this button to remove an existing entry**.**

Important: To edit an existing IP address or subnet mask, click the link under the IP address. The **Add IP Ignore List** page appears with the existing information. Edit the information and click **Save**. Click **Cancel** if you no longer want to edit the IP address.

IMAP Settings

How to get here

Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), and a **Start/Stop** button appears. This allows you to Start or Stop individual Services from their respective web pages, as well as from the **Service Administration** page.

You can use the IMAP Settings page to configure the IMAP Server. IMAP 4 lets users access remote messages stored on the mail server as if they were local. Users can read, move, delete mail, create mailboxes on the server system. Since messages reside on the server, users can access their mailboxes from multiple machines.

Important: After making changes, click **Save**. Stop the service, wait 5-10 seconds and restart the service.

- **Save Logs To.** Choose one of the following from the list box.
  - **No Log.** Select this option to turn off event logging.
  - **SYSMMDD.TXT.** Select to send 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**.**
  - **Log Server.** Select to send event information to the Log file indicated on the Logging tab.
  - **Debug Messages.** Select the check box to write debug messages to the log file for debugging IMAP4 problems. This option is resource intensive.
- **Force Subscribe to Private Mailboxes.** Select the check box to require the IMAP4 client to subscribe to use a private mailbox. A user who is not a subscriber is refused access. Do not enable this option if you wish to use web messaging. Choose this option if users are using Outlook or another client.
- **Force Subscribe to** *Public Mailboxes* (on page 374). Select the check box to require the IMAP4 client to subscribe to use a public mailbox. A user who is not a subscriber is refused access.
- **Allow Unsecured Access.** Select the check box to allow users to login to the system without authenticating via secure mode (such as SSL).

SSL Settings

Note: IMail Server uses OpenSSL Command Line Tool (v0.9.8e) which supports up to 4096-bit RSA and 2048-bit DSA. OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.

- **Enable SSL.** Select the check box to enable a dedicated port that accepts only SSL- encrypted connections from the IMAP4 service. You can change the default port used by the SSL Listener in the SSL port box.
- **SSL Port.** Enter the port used by the dedicated SSL Listener to accept connections. The default IMAP4 SSL port is 993; the valid range is from 1 - 32,000.
- **Enable TLS.** Select the check box to enable the IMAP4 service to accept SSL/TLS connections over the IMAP4 port through use of the STARTTLS command.

Advanced Options

When logging on to IMAP4 , the service returns a welcome message that identifies the mail server version and vendor. You can use the IMAP Advanced options to change the service's welcome message, for example, if you want to hide the mail server version and vendor information.

- **Hello Message.** Enter the text you want display in the IMAP service welcome message. The text is limited to 400 characters or less. If you enter over 400 characters, the system uses the default message. To intentionally revert back to the default message, clear this field.

Save. Click to save your settings. An "Update Successful" message and the time of the update appears.

Related Topic

Managing Mailboxes (on page 375)

Creating Public Mailboxes

The IMAP4 server options provide 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* (on page 143) ID named "public". Any mailboxes in this user's 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.

Note: 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.

Managing Mailboxes

When a user creates a mailbox, the mailbox is created on the IMail Server system. Because the IMail Server will be the permanent storage location for IMAP4 users' mail, you need to configure the server with appropriate disk space and manage the disk space by monitoring mailbox disk usage.

You can set maximum mailbox size and maximum number of messages for each user or you can set the maximum mailbox size and maximum number of messages globally for all users on a selected e-mail domain :

- For more information about global settings for a selected e-mail domain, see *Changing IMail Standard User Settings* (on page 98).
- For more information about individual user settings for a selected e-mail domain, see Changing IMail User File Directory Settings.

Administrators can set an option (on the IMAP4 tab) that determines whether users must subscribe to a private mailbox before they can read it.

LDAP

Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

About LDAP Server

Lightweight Directory Access Protocol (LDAP) provides a standard way for applications to request and manage directory information. LDAP has become another popular feature for standards-based mail servers. A simplified subset of the much more elaborate X.500 Directory Access Protocol, LDAP is more appropriate for many of today's applications, on both the client and server sides, because it makes fewer demands on system resources.

LDAP implementations use a client/server architecture to publish user information (such as address books) on the server and provide access to that directory information from LDAP-enabled clients.

IMail Server supports OpenLDAP to provide the following capabilities to users with LDAP-enabled clients:

- Locate LDAP directory information that may include name, phone number, e-mail address, organization, department, and address.
- List all users at a site.
- Browse for users who meet certain criteria.
- Modify user information in the LDAP directory.
- LDAP Administrators can use an LDAP enabled client to add, delete, and modify user accounts, including any LDAP directory information.

The IMail LDAP server uses OpenLDAP protocol. 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. Also, more information is available at *www.openldap.org* (http://www.openldap.org).

Related Topics

LDAP Data (on page 376)

Setting Up E-mail Domain LDAP Options (on page 54)

Setting IMail LDAP Options (on page 377)

About LDAP Data

IMail Server provides an LDAP database by extending the IMail user database to include standard LDAP attributes (such as name, address, organization name, and phone number) and any other attributes that a site defines.

Each user with an account on the IMail Server has an LDAP entry. When a user is added to the IMail user database an LDAP entry is defined with the following attributes:

Basic User Attributes	
ObjectClass	The type of entry. The value would be "inetOrgPerson".
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.
Surname	The surname or last name of the user.

When a user receives mail on the IMail Server system, his/her LDAP entry is activated.

Using an LDAP enabled client , the user can add, delete, and modify information in his or 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):

Optional User Attributes	
Organization	The user's company.
OU	The department within the company or organizational unit.
Street	The user's street address.
L	The user's city or locality.
ST	The user's state or province.
C	The user's country.
telephoneNumber	The user's telephone number.

These are the most common attributes used in the LDAP entry. The system administrator or the user can define other attributes.

Caution: The **Init LDAP** button initializes the LDAP database created for all e-mail domains by the LDAP server. Do not click **Initialize LDAP** unless you want to overwrite the database with the user IDs only that are stored in the Windows registry. First try synchronizing the LDAP database to resolve any problems.

If the Open LDAP server is not running, you are asked whether you want to start it. Initializing LDAP deletes all user changes to the attribute values and adds all users back to the LDAP server in the default state.

LDAP Service Settings

How to get here

Important: After making changes, click **Save**. Stop the service , wait 5-10 seconds and restart the service.

Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), a Start/Stop button appears and a Restart button appears. This allows you to Start, Stop, or Restart individual Services from their respective web pages, as well as from the Service Administration page.

- **Install Location.** Enter (or **Browse** to) the location of the directory where the OpenLDAP files are located. By default, the installation path for IMail is `"C:\Program Files\Ipswitch\Messaging\IMail\OpenLDAP"`. The following folders are located under the `"..\OpenLDAP"` folder:
  - **bin.** Folder where all OpenLDAP binaries are stored. These are:
    - **Openldap-data.** Folder where all folders with domain specific databases are stored, containing a folder named after each existing domain.

- **schema.** Folder where all OpenLDAP schema files are stored. Schema files are text files that determine the properties of each object.

- **Share\ucdata.** Contains supporting data files for the LDAP server. These files should not be modified.



Important: You can change the OpenLDAP file location, but you must move the OpenLDAP files manually to the location that you specify in this field. The `slapd.exe` file must also be unregistered and re-registered in the new location. You can also browse to the installation location by clicking the **Browse** button.

- **Create New Folder**
  - **New Folder Name.** Enter the name for the folder in which you wish to manually move the OpenLDAP files, as described in the preceding **Important** section. Click **Create**. Click **OK**.

- **Port.** Enter the Port that the LDAP server runs on. This can be changed to allow OpenLDAP to run on the same server as another LDAP server.

LDAP Actions



Note: After clicking Sync LDAP, you need to stop and restart the LDAP server.

- **Sync LDAP.** Click this button to synchronize the LDAP database in order to clean up orphaned accounts or add accounts that do not yet exist.



Caution: The Init LDAP button initializes the LDAP database created for all e-mail domains by the LDAP server. Do not click **Initialize LDAP** unless you want to overwrite the database with the user IDs only that are stored in the Windows registry. First try synchronizing the LDAP database to resolve any problems.

If the Open LDAP server is not running, you are asked whether you want to start it. Initializing LDAP deletes all user changes to the attribute values and add all users back to the LDAP server in the default state.



Important: You can also use the *iLDAP.exe utility* (on page 382) to Init or Sync a specified LDAP domain or all the LDAP domains. This utility can be used in the case when the Web Administrator does not properly Init or Sync all the LDAP domains on a server. This issue sometimes occurs on servers running Microsoft Windows 2003 machines with over 30 domains.

- **Init LDAP.** Click this button to initialize the LDAP database for the server.
- **Save.** Click to save your settings. An **Update Successful** message and the time of the update appears.

Related Topics

About LDAP Server (on page 375)

About LDAP Data (on page 376)

LDAP Settings (on page 54)

LDAP User Information (on page 150)

Populating the LDAP Database Using Ldaper.exe (on page 381)

Init & Sync LDAP DB - iLDAP.exe utility (on page 382)

LDAP Settings

How to get here

Use the LDAP Settings page to configure host options for OpenLDAP. This information is necessary for an LDAP client to edit the LDAP database. It is not necessary to enter an ID or password if you only want to view the OpenLDAP data.

Domain: Shows the current selected domain. From the drop down you can pick any of the domains available to this administrative user account.

LDAP Settings

- **LDAP Admin ID.** Displays the LDAP administrator ID for the e-mail domain. This information is auto-populated. The administrator ID cannot be an IMail user ID.
- **Password.** Enter the LDAP administrator password.
- **Confirm Password.** Enter the password a second time to confirm the original password. The two password entries must match in order for the value to be saved.

Caution: Do not click **Initialize LDAP** unless you want to overwrite the database with the user IDs only that are stored in the Windows registry. First try synchronizing the LDAP database to resolve any problems.

Important: Because the password is randomly generated during installation and importation, we highly recommend that you change it as soon as possible after completing setting up LDAP.

Important: You can also use the *iLDAP.exe utility* (on page 382) to Init or Sync a specified LDAP domain or all the LDAP domains. This utility can be used in the case when the Web Administrator does not properly Init or Sync all the LDAP domains on a server. This issue sometimes occurs on servers running Microsoft Windows 2003 machines with over 30 domains.

LDAP Actions

- **Init LDAP (Initialize the LDAP database).** Click to Initialize the LDAP database created for the current e-mail domain by the *LDAP server* (on page 375).
- **Sync LDAP (Synchronize the LDAP database).** Click to synchronize the LDAP database. Synchronizing removes multiple database entries, deletes old accounts, and adds new accounts.

Save. Click to save settings. An "**Update Successful"** message and the time of the update appear.

Related Topics

About LDAP Server (on page 375)

About LDAP Data (on page 376)

LDAP Service Settings (on page 377)

LDAP User Information (on page 150)

Populating the LDAP Database Using Ldaper.exe (on page 381)

Init & Sync LDAP DB - iLDAP.exe utility (on page 382)

LDAP Information

How to get here

- Enter user information on the LDAP Information page. LDAP user information is published on the server and the information is made available to LDAP-enabled clients.
- **Domain Name (OHN)**. Displays the name of the specified user's domain.
- **Userid.** Displays the ID of the specified user.

The following information can be updated to the LDAP database for the specified user:

- **Full name**
- **Organization**
- **Department**
- **Address**
- **City**
- **State**
- **Postal Code**
- **Country**
- **Telephone**

Related Topics

LDAP Settings (on page 54)

About LDAP Server (on page 375)

About LDAP Data (on page 376)

Setting IMail LDAP Options (on page 377)

Populating the LDAP Database Using Ldaper.exe (on page 381)

Populating the LDAP Database (ldaper.exe)

`Ldaper.exe` populates the LDAP database with user properties for all users on a selected e-mail domain. This may be particularly helpful after you have added a large number of users at once using the *Adduser.exe utility* (on page 422).

Important: If you are upgrading from IMail Server prior to version 8.1, an LDAP database conversion occurs during installation. The conversion can take a lengthy amount of time depending on the number of domains to convert. If the LDAP data is not available after the upgrade, run the LDAP Convert utility to correct the issue. In the command line utility, type: ldaper /CONVERT /Y

Basic Command Syntax

ldaper [options]:

`Ldaper.exe` supports the following command line options. Options can be prefixed with a hyphen or a forward slash.

Option	Explanation
-H	Host name
-U	User ID
-P	Password
-GN	First name
-HN	Last Name (Sur Name)
-S	Street Address
-C	City
-ST	State
-CO	Country
-Z	Postal Code
-T	Telephone
-O	Organization
-OU	Organizational Unit (Department)
- CONVERT	Converts LDAP dbases prior to version 8.1 to the new OpenLDAP dbase schema
-Y	Required option with the CONVERT option
-LSTART	Keeps the LDAP service running

Related Topics

Init & Sync LDAP DB - iLDAP.exe utility (on page 382)

Adding Users Using Adduser.exe (on page 422)

Initializing and Synchronizing LDAP Databases (iLDAP.exe)

iLDAP.exe is a utility to Init or Sync a specified LDAP domain or all the LDAP domains. This utility can be used in the case when the Web Administrator does not properly Init or Sync all the LDAP domains on a server. This issue sometimes occurs on servers running Microsoft Windows 2003 machines with over 30 domains.

Basic Command Syntax

```
iLdap -i|s[<domain>]
```

where domain is the domain you want to Init or Sync. All the domains are initialized or synchronized if no domain is specified.

Command	Function
-i	Initializes the specified LDAP database.
-s	Syncrhonizes the specified LDAP database.

Related Topics

Populating the LDAP Database Using Ldaper.exe (on page 381)

POP3

How to get here



Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), and a **Start/Stop** button appears. This allows you to Start or Stop individual Services from your respective web pages, as well as from the **Service Administration** page.

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 use the "offline" method of accessing the mail server . Mail messages are delivered to the IMail Server system and the mail client periodically connects to the server and downloads the user's mail to the client system. Mail messages are automatically deleted from the server system. Therefore, mail messages are stored only

temporarily on the mail server . This method of access is best suited to users who always read their mail from the same client system.

See Request for Comments (RFC) 1725 for a description of the POP3 protocol.

Related Topics

POP3 Settings (on page 383)

POP3 - Control Access (on page 385)

POP3 Settings

How to get here



Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), Start/Stop and Restart button appears. This allows you to Start, Stop, or Restart individual Services from your respective web pages, as well as from the **Service Administration** page.

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 use the "offline" method of accessing the mail server . Mail messages are delivered to the IMail Server system and the mail client periodically connects to the server and downloads the user's mail to the client system. Mail messages are automatically deleted from the server system. Therefore, mail messages are stored only temporarily on the mail server . This method of access is best suited to users who always read their mail from the same client system.

See Request for Comments (RFC) 1725 for a description of the POP3 protocol.



Important: After making changes, click **Save**. Stop the service, wait 5-10 seconds and restart the service.

- **Save Logs To.** Choose one of the following from the list box.
  - **No Log.** Select this option to turn off event logging.
  - **SYSMMDD.TXT.** Select to send 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**.**
  - **Log Server.** Select to send event information to the Log file indicated on the Logging tab.

- **Enable Debug Messages.** Select the check box to write debug messages to the log file.

- **Use APOP.** Select the check box to secure user authorization (password encryption). For more information, see RFC 1939.



Note: APOP works with the IMail user database only.

- **Enable XTND XMIT Command.** Select the check box to enable the IMail Server to accept outbound mail sent via XTND XMIT. Clients such as WinQVT/Net require this functionality.
- **Allow Remote Password Change.** Select the check box to enable internal commands that allow remote password changes with older mail clients (such as an older version of Eudora).
- **Auto Deny Possible Hack Attempts.** Select the check box to enable a remote IP address to be temporarily denied access (Control Access file).



Note: If more than 512 characters are sent in a POP3 command (other than the POP3 DATA command) the remote IP address is temporarily put in the Control Access file until you stop and restart the IMail service. This data appears to the IMail Server as an attempt to hack into the server. The IP address is not displayed in the *Control Access* (on page 400) list, but it is reported in the log file.

SSL Settings



Note: IMail Server uses OpenSSL Command Line Tool (v0.9.8e) which supports up to 4096-bit RSA and 2048-bit DSA. OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.

- **Enable SSL.** Select the check box to enable a dedicated port that accepts only SSL- encrypted connections from the POP3 service. You can change the default port used by the SSL Listener in the SSL port box.
- **SSL Port.** Enter the port used by the dedicated SSL Listener to accept connections.
- **Enable TLS.** Select the check box to enable the POP3 service to accept SSL/TLS connections over the POP3 port through use of the STARTTLS command.

Advanced Options

When logging on to POP3 , the service returns a welcome message that identifies the mail server version and vendor. You can use the POP3 Advanced options to change the service's welcome message, if for example, you wanted to hide the mail server version and vendor information.

- **Hello Message.** 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. To revert back to the default message, clear this field.

Warning: The default advanced settings should be appropriate for most installations. If you need to change these settings, be aware that they can change the operation of the server.

Save. Click to save your settings. An **"Update Successful"** message and the time of the update appear.

POP3 - Control Access

How to get here

Important: After making changes, click **Save**. Navigate to the POP3 Settings page, stop the service , wait 5-10 seconds and restart the service.

There are two ways to control who connects to this service. You can either grant access to everyone, except specific computers or subnets that you specify, or you can deny access to everyone, except specific computers or subnets that you specify.

- **ALLOW all computers to communicate with this server except.** Select this option from the list box to grant access to specific computers or subnets. Click **Add**. A field with a cleared check box and an empty text box appears. Select the check box if you want to grant access to a single computer and enter its IP Address . If you want to grant access to a group of computers, select the check box and enter the IP address and Subnet Mask in the corresponding text boxes
- **DENY all computers from communicating with this server except.** Select this option from the list box to deny access to specific computers or subnets. Click Add. A field with a cleared check box and an empty text box appears. Select the check box if you want to deny access to a single computer and enter its IP Address in the corresponding text box. If you want to deny access to a group of computers, select the check box and enter the IP address and Subnet Mask in the corresponding text boxes.
- **IP Addresses.** This column lists the IP Address(es) of all computers either allowed or denied POP3 access.
- **Subnet Mask.** This column lists the Subnet Mask(s) of all computer groups either allowed or denied POP3 access.
- *Add* (on page 413). Click this button to add computers or computer groups you want to be granted or denied access to the POP3 service.
- **Delete.** Click this button to delete selected computers or computer groups from the Control Access list.

Add/Edit POP3 Control Access

How to get here

Use the Access Control Add page to add a single computer or group of computers to the POP3 Access Control List.

- **Add a Single Computer.** Select this option if you want to allow or deny access to a single computer. If you select this option, you may enter text into the IP address text box.
- **Add a Group of Computers.** Select this option if you want to allow or deny access to a group of computers. If you select this option, you may enter text into the Subnet Mask text box.
- **IP Address.** Enter the IP address of a single computer that you want to allow or deny POP3 access.
- **Subnet Mask.** Enter the subnet mask of the computer group that you want to allow or deny POP3 access.



Important: You must restart the POP3 service for the changes to take effect.

Related Topics

POP3 - Control Access (on page 385)

Queue Manager

The Queue Manager service allows you to control the flow of messages through the mail queue. This service takes the place of SMTP32exe. by delivering messages to both local and remote destinations. Although the SMTP32.exe program still exists, it simply informs the Queue Manager when a message requires delivery.



Note: When sending mail, if a valid 1xx or 2xx response is not received when connecting, the **Queue Manager** will roll to the next MX record.

The mail queue is also known as the spool is a directory that stores mail messages that are waiting for delivery. Files in the queue include incoming messages, outgoing messages, attachments, and error messages.

The queue manager releases messages one at a time in the order that they were received.

Related Topics

Troubleshooting the Spool Directory (on page 391)

Queue Manager Options

How to get here



Important: After making changes, click **Save**. and restart the service.



Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), and a Start/Stop button appears. This allows you to Start or Stop individual Services from your respective web pages, as well as from the Service Administration page.

The Queue Manager regulates the SMTP32 processes (or threads) so that the maximum number is not exceeded. This ensures that an attempt is made to deliver all messages and that delivery not be delayed by being bumped to a queue run delivery on heavily loaded systems. Files are processed according to priority, with files that have had no delivery attempt being first. Files that need to be retried are then processed based on the time that they were placed in the spool .



Warning: The Queue Manager service is a component of the SMTP delivery process. Disabling the Queue Manager may stop or delay mail delivery.

- **Delivery Threads.** Enter the total number of delivery threads that can be used to deliver messages. Each thread processes one message at a time. This option is set to 30 by default; its minimum value is 5. Since each Queue Manager thread can deliver one message, if the option is set to 30, the Queue Manager can deliver 30 messages at a time.



Caution: You may need to increase the number of SMTP processes if you have a large number of users who subscribe to list server mailing lists. If you do need to increase this value, you should do so in small increments, for, as you increase the number of SMTP processes, you increase the processing load on your mail server.

- **Max Retry Threads.** Enter the maximum number of delivery threads that can be used simultaneously when the system retries to deliver messages in the queue. By default, this option is set to 15. The value for this option cannot be greater than the number of delivery threads and cannot be less than 2.

- **Listen Pipes.** Enter the number of pipes that the queue manager opens in order to listen for files being dropped in the queue by other processes. This option is set to 4 by default. The minimum value for this option is 2 and the maximum is 20. The default value should be sufficient for most servers, but can be increased for better performance on busy servers. You must examine the log files to determine if you need to increase this number. If, prior to a queue run, you find log lines that say "Adding Queue file XXX," this means that the Queue Manager has found files it was not notified of before. In this case, you should increase the number of listen pipes.
- **Retry Timer.** Enter how often, in minutes, the Queue Manager will attempt to re-deliver messages that failed to be delivered on previous queue runs. This option works in conjunction with the **Tries Before Return to Sender** below. This option is set to 30 minutes by default. The minimum value for this option is 10; the maximum is 120.
- **Daily Report Address.** Enter the e-mail address to which a *daily count report* (on page 390) will be sent. If no address is entered, no report will be sent. Through the queue manager, IMail Server compiles and sends a daily report with detail server activity. These reports are sent once a day, 30 seconds after the date changes, to the e-mail address specified in the Daily Report Address text box located on the Queue Manager tab.
- **Outgoing Helo/Ehlo Host Name.** Enter the name you wish to use for outgoing communications with the recipient.
- **Tries Before Return to Sender.** Enter the amount of times that delivery is attempted before returning the mail to the sender. Each time the Retry Timer reaches 0, a deliver attempt is made. We recommend leaving this at the default value of 20.

  Example: If the **Retry Timer** is set to 30 (minutes) and the "**Number of Tries**" is set to 20 (default), then the message will be returned in about 10 hours. We recommend a value of 20.

  Example: If the **Retry Timer** is set to 30 (minutes), and you want to attempt delivery for up to 3 days, then the "**Number of Tries**" box should contain 144.
- **Max Tries for NULL Senders.** Enter the maximum number of times that IMail attempts to deliver a message that has no sender (including postmaster messages). This value must be less than the value entered for **Tries Before Return to Sender** above. If the **Tries Before Return to Sender** value is less than the value entered here, the **Max Tries for NULL Senders** option is not enforced.
  - **Delete After Max Tries.** This will delete after **Max Tries for NULL Senders** criteria has been met.
- **Domain Name Server.** Enter the IP address of the system that provides domain name service for your network. You can enter multiple names here, separated by a space. This options is required in order to send mail externally.
- **Auto Restart on Failure** (recommended). Click this check box to enable SMTPD32 to check the status of the Queue Manager. If it is not running, STMPD32 attempts to restart it. The event is then written to the log file. The Queue Manager status is checked every 2 minutes. If, after two checks, the Queue Manager is not running, IMail Server attempts to restart it. We recommend that you enable this option.

SMTP/Queue Manager Log Settings

- **Save Logs To**. Select the file type from the drop down list, that you want to use for logging SMTP events:
  - **No Log.** Selecting this option disables logging.
  - **SYSMMDD.txt.** Selecting this option causes all inbound and outbound mail to be logged in the file where MM is the month and DD is the day the log was written.
  - **Log Server.** Selecting this option causes messages to be sent to the log file specified on the Log Manager tab.
- **Debug Messages.** Select the check box to write debug messages to the log file.
- **Verbose Logging.** Select the check box to record more information than in standard logging. This can create very large log files; however, this can be helpful in troubleshooting problems.

DNS Caching

The DNS cache is an internal cache of positive DNS queries. The cached DNS response remains active for the length of time specified in the Time to Live (TTL) for the DNS record.



Tip: We recommend enabling this option, since it improves delivery performance by cacheing and reusing positive queries.

- **Max DNS Entries.** Enter the total number of entries allowed in the DNS cache. The DNS cache is a first in, first out list, so the list is updated as new DNS queries are performed. We recommend that you enter a value of 200. However, you can enter any value between 5 and 5000.
- **Clear Cache.** Click this button to clear the DNS cache in the Queue Manager. This is usually not required. When_to_Use.htm
- **Enable DNS Cache.** Select this check box to enable the DNS cache.

Failed Domain Skipping Header

Failed Domain Skipping occurs when IMail Server tries to deliver a message but cannot connect to the domain. The domain is added to a list of failed domains (known as the Skip List), and all recipients for that domain will be skipped for the amount of time entered as the Skip Time.



Tip: We recommend enabling this option, since it increases performance when many messages are destined for unreachable hosts.

- **Max Skip Tries.** Enter the total number of entries allowed in the Skip List. This is a first in, first out list that is updated as new domains are added. We recommend entering a value of 500. However, you can enter any value between 5 and 5000.
- **Clear Skip List.** Click this button to clear the current Skip List from memory.
- **Skip Time** (minutes). Enter the amount of time, in minutes, that failed domains will remain in the Skip List before they are removed. Although we recommend 30, you can enter any value between 2 and 240 minutes.

- **Enable Domain Skipping.** Select this check box to enable Failed Domain Skipping.

Gateway Options

- **Remote Gateway Hostname.** Enter the name of another domain 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 blank.
- **Tries Before Send to Gateway.** Enter 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.
- **Send All Remote Mail Through Gateway.** Selecting this check box causes IMail Server to send all mail to the Remote Mail Gateway Host above, which forwards 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.

Outbound SSL Connection Settings

- **Use SSL**. Using SSL without **Force SSL** checked will attempt to use a TLS connection on port 25; if TLS is not supported then an attempt will be made to create an implicit SSL connection on port 465. If a TLS connection or implicit connection cannot be made then the message is delivered normally on port 25.
- **Force SSL**. This check box will attempt to use a TLS connection on port 25; if TLS is not supported then an attempt will be made to create an implicit SSL connection on port 465. If a TLS connection or implicit connection cannot be made then the message is **not** delivered. This method is useful for those who want to enforce a higher level of security.

Save. Click to save settings. A message at the top "Your changes have been saved" will confirm.

Queue Manager - Daily Count Report

Through the use of the queue manager, IMail Server has the ability to compile and send daily reports that detail server activity. These reports are sent once a day, 30 seconds after the date changes, to the e-mail address specified in the Daily Report Address text box located on the Queue Manager tab.

The following counts are included in the report:

- SpamContent. The number of statistical filtering matches.
- SpamPhrase. The number of phrase filtering matches.
- Virus. The number of viruses caught by IMail Anti-Virus.
- LocalDeliver. The number of local deliveries.
- RemoteDeliver. The number of remote deliveries.
- SpamFeatures. The number of e-mails containing the selected HTML features.

- SpamHREFDomain. The number of e-mails containing HTML links to one of the domains listed in the HREF domain black list.

Example Report

```
Date:   Fri, 3 Jan 2003 08:50:47 -0500
Message-Id: <7002211132.aa00253@host1.com>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
From: "Postmaster" <postmaster@host1.com>
Sender: <postmaster@host1.com>
To: user@Host1.com
Subject: IMail Daily Report

SpamContent     293
SpamPhrase     256
Virus          5
LocalDeliver   1281
RemoteDeliver    592

SpamFeatures    200

SpamHREFDomain    125
```

Troubleshooting the Spool Directory

Normally, IMail Server cleans up the .tmp and attached files as part of the delivery process. However, if there is an SMTP failure during delivery, these files may not be deleted. You can also run the *Spool Cleaner utility* (on page 96) (isplcln.exe) to delete old files.

A damaged or corrupt file in the queue can prevent mail from being received correctly. If you suspect that this is the cause of a problem you have, you can try moving all files from the Spool directory to a 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 are not sent may be damaged or corrupt files.

Related Topics

About the Spool Directory (Queue) (on page 94)

About Log Files (on page 411)

Beginning Character of Files in the Queue (on page 97)

File Extensions of Files in the Queue (on page 96)

SMTP

The SMTP service processes all incoming and outgoing messages. 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 POP3 or IMAP client. Spooling allows the transfer from client and server to occur in the background.

Related Topics

SMTP Settings (on page 392)

SMTP Control Access Options (on page 400)

SMTP Kill File Options (on page 401)

SMTP Accept List Options (on page 402)

SMTP White List (on page 403)

SMTP Domain Forwarding (on page 404)

Supported SMTP RFCs (on page 406)

SMTP Service Options

How to get here



Note: At the top of each Services page, the name of the Service, its Status (Running or Stopped), Start/Stop and Restart button appears. This allows you to Start, Stop, or Restart individual Services from your respective web pages, as well as from the **Service Administration** page.

The SMTP service processes all incoming and outgoing messages. Due to its openness, it is difficult to simultaneously block unwanted mail (spam) and keep your mail server available to its users. The following settings and options can be configured to help administer this protocol.



Important: After making changes, click **Save**, and restart the service.

- **Mail Relay Settings.** Select one of the following from the drop down list:
  - **No Mail Relay (Default setting).** Selecting this option from the drop down list enables the SMTP server to refuse to accept mail destined for other hosts (any host not on the IMail Server), unless the user authenticates. Select this option if

all of your users send and receive mail from the same host that IMail Server is on, or if they use web messaging to access mail. You will still receive mail for local users because a message destined for or originating from the IMail Server host does not use the relay function.

- **Relay Mail for Addresses.** Select this option from the drop down list to allow the SMTP server to transmit mail originating from local addresses and destined for other hosts. Likewise, the server will accept mail from other hosts that is destined for specified local addresses.
  - **Addresses.** This button is enabled when **Relay Mail for Addresses** is selected. Click the Addresses button. The *Relay Mail for Addresses* (on page 397) page appears.



Important: DomainKeys / DKIM Signature Verification will **not** be processed when an address exists in the **"Relay Mail for Addresses (on page 392)"**.

- **Relay for Local Users Only.** Select this option from the drop down list to check the "From" address of incoming mail and verify that it contains a valid IMail Server host name, then checks the host for the user ID.



Note: 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. If a user needs to use an alias for his/her e-mail address, the alias needs to be in the accept.txt file. You cannot use this option if you are using a "store and forward" setup to relay mail for another server. The accept.txt file is only used when the SMTP Relay Setting is set to Relay for Local.

- **Relay for Local Hosts Only.** Select this option from the drop down list to check the "From" address of incoming mail to determine that it contains a valid IMail Server host name, then checks that host for the user ID. It does not check user aliases. If the host name or User ID is not valid, the server does not relay mail.



Note: 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. If a user needs to use an alias for their e-mail address, the alias needs to be in the accept.txt file. You cannot use this option if you are using a "store and forward" setup to relay mail for another server. the accept.txt file is only used when the SMTP Relay Setting is set to Relay for Local.

- **Relay Mail for Anyone.** Select this option from the drop down list to allow the SMTP server to accept mail from any host that is destined for any other host, and redeliver that mail (i.e. become a mail gateway). This option is the least secure because it allows your server to be used by anyone to send mail to anyone. 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.



Note: If you select this option for mail relay, your server may be blacklisted for running an open relay. To remedy this, you should choose to *Relay Mail for Addresses.* (on page 397)

SMTP/Queue Manager Log Settings

- **Save Logs To**. Select the file type from the drop down list, that you want to use for logging SMTP events:
  - **No Log.** Selecting this option disables logging.
  - **SYSMMDD.txt.** Selecting this option causes all inbound and outbound mail to be logged in the file where MM is the month and DD is the day the log was written.
  - **Log Server.** Selecting this option causes messages to be sent to the log file specified on the Log Manager tab.
- **Debug Messages.** Select the check box to write debug messages to the log file.
- **Verbose Logging.** Select the check box to record more information than in standard logging. This can create very large log files; however, this can be helpful in troubleshooting problems.

SSL Settings



IMPORTANT! Enabling SSL or TLS will **only** accept SSL and TLS connections. This will **not** initiate SSL and TLS connections.



Note: IMail Server uses OpenSSL Command Line Tool (v0.9.8e) which supports up to 4096-bit RSA and 2048-bit DSA. OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.

- **Enable SSL.** Select the check box to enable a dedicated port that accepts only SSL- encrypted connections from the SMTP service. You can change the default port used by the SSL Listener in the SSL port box.
- **SSL Port.** Enter the port used by the dedicated SSL Listener to accept connections. The default SMTP SSL port is 465; the valid range is from 1 - 32,000.
- **Enable TLS.** Select the check box to enable the SMTP service to accept SSL/TLS connections over the SMTP port through use of the STARTTLS command.

Dictionary Attack Options



Note: All settings related to Dictionary Attack blocking default to 0.

- **Max Invalid Recipients Per Session.** Enter the maximum number of invalid recipients the server will accept before the session is dropped and the IP address of the sender is added to the Control Access table.

An invalid recipient is an addressee that is not valid for that server when the client issues a RCPT to command.

- **Soft Error Limits.** Enter the number of errors that may occur on a session before error responses are delayed.
- **Hard Error Limits.** Enter the amount of errors that may occur on a session before the session is dropped and the IP address is added to the Control Access table.
- **Minutes to Deny Access.** Enter the number of minutes to deny a sender access after a session is dropped.
- **Error Delay Seconds.** Enter the amount of time in seconds to delay error responses in the Soft Error Limits scenario.

  Example of an error response:

  'anyuser@anywhere.com' on 7/6/2005 11:59 AM

  550 Connection denied after dictionary attack

Security Options

- **Copy to Mail Address.** Enter the full e-mail address to which you want to send a copy of each message. This option will not function unless the **Enable Copy All Mail** check box is selected.
  - **Enable Copy All Mail.** Select this check box to enable copying of all mail.
- **Allow Remote Mail to Local Groups.** Select this check box to allow the SMTP server to accept mail addressed to a group that has been defined using IMail Administrator. The SMTP server re- sends the message to users in the group.
- **Check Valid Sender.** Select this check box to require that the user's mail address (user@host) is specified in the MAIL FROM or REPLY-TO line of an incoming mail message.
- **Auto Deny Possible Hack Attempts.** (Set by default) When checked it will assume that sending more than 512 characters in a command other than the SMTP DATA command is an attempt to "hack" into your server. The remote IP address will be temporarily placed into the "deny access" (Control Access) file, until the services are restarted.

  Auto Deny with the use of **extended SMTP** will allow 1600 characters in a command other than the SMTP DATA command.



Note: You will not see the address in the Control Access list, but it is reported in the log file.

- **Disable SMTP "VRFY" Command.** Select this check box to deny a remote host to test for valid user IDs. The SMTP VRFY command is used to verify a user ID on a host, and as such it can be used from a remote host 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 returns the message: `502 Command not implemented.`

If you disable the SMTP VRFY command, when IMail Server receives an SMTP VRFY request, it will return the message: 502 Command not implemented

Note: When using peer servers, do not select Disable SMTP "VRFY" Command. A peer server needs to use this command to verify a user that is on the other peer. See *Setting Up Peering* (on page 244) for more information.

- **Require CRAM-MD5 Authentication**. This setting when set will force encryption authentication when logging in to SMTP services.

Advanced Options

Warning: The default advanced settings should be appropriate for most installations. If you need to change these settings, be aware that they can change the operation of the server.

- **Max Recipients Per Message.** Enter the maximum number of addresses that can receive a single message. The default is 0.

Note: Max Recipients Per Message option does not apply to authenticated users.

- **Delay Between Recipients.** Sets a delay (Seconds), between message recipients, for relayed external mail. This prevents spammers from consuming all of the CPU time. However, the setting slows mail server performance. The default is 0.

- **Host Delimiters.** To change the default characters, enter the character(s) to use to delimit the host name. Each character is seen by IMail Server as equivalent to the @ in e-mail addresses. Any of the defaults can be used between the user ID and the virtual host name in the POP3 or IMAP4 login user ID. By default, the characters used are: @ % * : $ and &.

Note: IMail Web Messaging requires the @ character for the host delimiter.

- **Mailbox Delimiter.** Enter the character that will be used to delimit the mailbox name in a user ID. If nothing is entered, the default delimiter is - (dash).
- **Max Connections.** Enter the maximum number of connections handled by the SMTP Service. Use the default of 0 (zero) for an unlimited number of connections.
- **Port.** Enter the port that the SMTP service listens on. The default SMTP port is 25. The valid range is from 0-32000.



Note: If you update the port here, it will automatically update in the Client as well.

- **Hello Message.** To change the SMTP service welcome message, enter the new message in this text box. The text is limited to 400 characters or less. If over 400 characters are entered, the default message is used. To revert to the default message, delete the custom message text from the **Hello Message** box.
- **Delivery application.** To replace the mail delivery application with an external program, enter the full pathname of the file in this text box.
- **Enable Extra Port.** Select to enable an extra port.
  - **Extra Port.** If you've chosen to enable an extra port, enter its number here.
  - **Force AUTH on Extra Port.** Select this check box to force SMTP authorization on an extra configured port.
- **Disable SMTP AUTH.** Select this check box to disable SMTP authentication. SMTP Auth provides a means of authenticating the user ID and password of a user sending mail. This is handled transparently by the mail server and client. When the mail client connects to the mail server, the server tells the client the authorization methods it can use. The client then sends the user ID and password to the server and the server verifies them. If a user issues the AUTH command when Disable SMTP AUTH is selected, SMTPD responds with the "502 command not implemented" message.
- **Enable SMTP to Listen on All IP.** Select this check box if you want to have IMail Server listen on all available IP addresses and configured ports on the server.

Save. Click the save button at the bottom of the screen. A message at the top "Your changes have been saved" will confirm.

Related Topics

Control Access (on page 400)

Kill File (on page 401)

Accept List (on page 403)

White List (on page 403)

SMTP Delivery Application Utility (on page 443)

Supported SMTP RFCs (on page 406)

Relaying Mail for Addresses

How to get here

You can specify the IP address or range of hosts and subnets that you want to relay mail for. IMail Server considers these addresses to be local. If mail is received from any of the specified addresses, IMail Server will accept the mail that is destined for other hosts. Likewise, IMail Server will accept mail from other hosts that is destined for the specified addresses.



Important: DomainKeys / DKIM Signature Verification will **not** be processed when an address exists in the **"Relay Mail for Addresses (on page 392)"**.

- **Allow these addresses to skip AntiSpam filters.** Select this option to exempt these addresses from undergoing any spam tests.
- **IP Addresses.** This column displays the IP addresses for which you want to relay mail. Click the IP address link to edit the relay address. The *Edit Relay Address* (on page 399) page appears.
- **Subnet Mask.** This column displays the range of hosts and subnets for which you want to relay mail.
- **Add.** Click to Add Relay IP Addresses. The *Add Relay Address* (on page 398) page appears.
- **Delete.** Click this button after selecting the check box to the left of the IP address you wish to delete.
- **Save.** Click to save your settings. An "Update Successful" message and the time of the update appears.

Related Topics

SMTP Settings (on page 392)

Adding Relay Addresses

How to get here

Use this page to add a single computer or group of computers to treat as local to the IMail Server.

- **Add a single computer.** Click to add a single computer to treat as local to the IMail Server.
- **Add a group of computers.** Click to add a group of computers to treat as local. The subnet mask appears automatically in the Subnet Mask field, below.

  Example:

  If you have a class C address space of 156.21.50.0, enter the (group) IP address of 156.21.50.0 in the IP Address text box, and if it is not automatically entered, 255.255.255.0 in the Subnet Mask text box. This will allow all 254 systems to be considered the same as the local system and they can use the mail server to send mail, without having to enter each IP address individually.
- **IP Address.** Enter the IP address to add a single computer to treat as local to the IMail Server.
- **Subnet Mask.** Enter the subnet mask for the group to be considered local.

Important: You must restart the SMTP service for the changes to take effect.

- **Save.** Click to save your settings. An "Update Successful" message and the time of the update appears.
- **Cancel.** Click **Cancel** to not save any changes. The settings will remain the same.

Related Topics

SMTP Settings (on page 392)

Relay Mail for Addresses. (on page 397)

Editing Relay Address

How to get here

Use this page to edit a single computer or group of computers considered as local to the IMail Server.

- **Single Computer.** Click to edit a single computer to treat as local to the IMail Server. Your cursor appears in the IP Address text box.
- **Group of Computers.** Click to edit a group of computers to treat as local. Your cursor appears in the Subnet Mask text box.
- **IP Address.** Edit the IP address for a single computer considered as local to the IMail Server.
- **Subnet Mask.** Edit the subnet mask for the group considered as local to the IMail Server.

Important: You must restart the SMTP service for the changes to take effect.

- **Save.** Click to save your settings. An "Update Successful" message and the time of the update appears.
- **Cancel.** Click **Cancel** to not save any changes. The settings will remain the same.

Related Topics

SMTP Settings (on page 392)

Relay Mail for Addresses. (on page 397)

DomainKey Relay For Addresses Note

Important: DomainKeys / DKIM Signature Verification will **not** be processed when an address exists in the **"Relay Mail for Addresses (on page 392)"**.

SMTP Control Access Settings

How to get here

Important: After saving changes you must restart the SMTP service for the changes to take effect. To do this, click the **Services > SMTP Tab** to navigate to the SMTP Settings page. Click the **Restart** button.

There are two ways to control who connects to this service. You can either grant access to everyone, except specific computers or subnets that you specify, or you can deny access to everyone, except specific computers or subnets that you specify.

- **DENY all computers from communicating with this server except.** Select this option from the list drop-down box to allow access to specific computers or subnets. Click **Add**, will bring up a pop-up window with options for entering a single computer's IP address to allow access or a group of computer IP address' and Subnet Mask.
- **ALLOW all computers to communicate with this server except.** Select this option from the list drop-down box to deny access to specific computers or subnets. Clicking **Add**, will bring up a pop-up window with options for entering a single computer's IP address to deny access or a group of computer's IP address and Subnet Mask.

IP Address List

- **IP Addresses.** IP address(es) of a single or group of computers that are being allowed or denied SMTP access.
- **Net Mask.** Subnet mask of the computer group being allowed or denied SMTP access.
- **Expires.** Date the IP Address will expire and no longer be on the control access list.
- **Comments.** Space for IMail Administrator to enter comments pertaining to IP Address entered.

Add (on page 400). Click this button to add computers or computer groups you want to grant or deny access to the SMTP service.

Edit. Click this button after selecting an IP address to modify in the Control Access list.

Delete. Click this button after selecting an IP address to delete from the Control Access list.

Related Topic

Add / Edit the SMTP Control Access (on page 400)

Add/Edit SMTP Access Control

How to get here

Use the Access Control Add page to add a single computer or group of computers to the Access Control List.

- **Add a Single Computer.** Select this option if you want to allow or deny access to a single computer. If you select this option, you may enter text into the IP address text box.
- **Add a Group of Computers.** Select this option if you want to allow or deny access to a group of computers. If you select this option, you may enter text into the Subnet Mask text box.
- **IP Address/Range.** Enter the IP address of a single computer that you want to allow or deny SMTP access.
- **Net Mask.** Enter the subnet mask of the computer group that you want to allow or deny SMTP access.
- **Expires**. (Optional) Click the Calendar button to set an expiration date. Default is set to **Never Expires**.

  --OR--
- **Never Expires**. (Checked by Default) IP Address will never expire.

 **Important:** You must restart the **SMTP service** for the changes to take effect.

SMTP Kill File

How to get here

The SMTP server uses the Kill File to deny access to the IMail Server. It allows you to specify mail addresses or hosts from which you do not want to accept mail.

IMail Server checks the incoming message's "Mail From" user@host> line in the SMTP envelope. When it receives mail from an address listed in the kill file, IMail Server returns the message: 501 unacceptable mail address

- **Existing Entries in the Kill File.** To add, delete, or edit an entry, place your cursor in the text box, and modify as necessary, all addresses from which you do not want to accept mail.

Save. Click this button to save your entries or changes.

Related Topic

SMTP Kill File Examples (on page 401)

SMTP Kill file Examples

The kill.lst file is used by the SMTP server to deny access to the mail server. It allows you to specify mail addresses or mail hosts that you do not want to accept mail from. The kill.lst file is located in the IMail top directory and applies to the primary host and all virtual hosts. To create or edit the kill file, click the **Edit kill file** button. The kill.lst file appears in Windows Notepad, or if no kill.lst file exists, one will be created.

Adding Entries

In the KILL.LST file, enter one entry per line in either of the following formats:
userid@host

Examples:

To deny access from a user mail account

fred@widget.com

To deny access to all users from the mail host widget.com

@widget.com

@*partialhost

The following will reject all mail mail from widget.com, bluewidget.com, and nifty.widget.com.

@*widget.com



Note: The SMTP kill file is separate from the *kill files for Lists* (on page 208).

SMTP Accept List

How to get here

The Accept List lets you name remote hosts and users that you want the IMail Server to accept as local hosts and users.



Note: SMTP Accept List will only function correctly with settings for Relay for Local Users, and Relay for Local Hosts.

- **Existing Entries in the Accept File.** To add, delete, or edit an entry, place your cursor in the text box and modify as necessary all addresses from which you want to accept mail.



Warning: Using **Relay for Local Host Only** will relay only Host names in the **Accept List**, ignoring any E-mail addresses. Using **Relay For Local Users Only** will relay only User names in the **Accept List**, ignoring any Host name entries.

Save. Click this button to save your entries or changes.

Related Topics

SMTP Accept List Examples (on page 403)

SMTP Accept List Examples

The accept.txt file lets you name remote hosts and users that you want the IMail Server to accept as "local" hosts and users. IMail Server does this by checking the "from" address in the SMTP conversation and comparing it against the entries in the accept.txt file.

Adding Entries

Enter one IP address , host name, or user per line. Do not use spaces or punctuation.

Examples:

To enter hosts:

mail1.acme.com

mail5.foo.com

To enter users:

fred@mail1.acme.com

bob@mail5.acme.com



The Accept List must have an exact match for the respective host or e-mail address. It does not accept wild cards or partial matches.

SMTP White List

How to get here.

Use the SMTP White List page to create a list of IP addresses and ranges that are trusted.

- **IP Addresses.** This column lists the trusted IP addresses.
- **Net Mask.** This column lists trusted ranges of IP addresses.

Add. Click the button to add an IP address or range of IP addresses to the SMTP White List.

Edit. Select an IP address to modify and click **Edit**.

Delete. Click this button after selecting an IP address to delete from the SMTP White List.

Important: You must restart the SMTP service for the changes to take effect. To do this, click the **Services > SMTP Tab** to navigate to the SMTP Settings page. Click the **Restart** button.

SMTP Domain Forwarding

How to get here

Domain Forwarding will redirect all outgoing e-mail sent to a specific domain name to another IP Address. The Domain Forwarding page maintains all domain names that are to be forwarded in a binary file called **"domfwd.dfw"** which is located under the `"..\IMail"` folder.

Note: Domain Forwarding ignores e-mail sent for local delivery.

- **Domain Name**. This column lists domains to be forwarded
- **IP Address.** This column lists the IP address to forward to.

Add. Click the button to add a Domain Name to be forwarded.

Delete. Click this button to delete Domain Name

Example 1:

`"domain.com"` is setup to be forwarded to `"192.168.1.1". A`ll e-mail going to `"domain.com"` will be redirected to its corresponding user with the same domain name but on "192.168.1.1". So, an e-mail addressed to: dude@domain.com would be re-routed to dude@domain.com at 192.168.1.1.

Domain Name	IP Address
domain.com	192.168.1.1

Example 2:

Administrator would like to forward e-mail to a faxing service. Domain Forwarding can be set where the domain name is in the format of `"phonenumber.domain.com"` and the IP Address is the Faxing Service. E-mail received by the faxing service, extracts the phone number and uses it for the fax machine. Using a wild card to capture the phone number, Domain Forwarding would be as follows:

Domain Name	IP Address
*.domain.name	192.168.2.2

Important: Wild card will only work at the beginning of the domain name.

Wild Card Examples:

*.domain.com *wolf.domain.com	**Valid** usages of wildcard
wolf.*.com wolf*.com were*wolf.com	**Invalid** usages of wildcard

Related Topics

Adding to Domain Forwarding (on page 405)

Editing Domain Forwarding (on page 406)

Adding to Domain Forwarding

How to get here

Use the Domain Forwarding page to redirect all outgoing e-mail sent to a specific domain name to another IP Address.

Domain Forwarding generates a binary file ("..\IMail\domfwd.dfw") containing domain names that are to be forwarded.

- **Domain Name.** Enter add a domain name to be redirected.
- **IP Address**. Enter the IP address that the stated domain will be redirected.

Important: You must restart the Queue Manager services for the changes to take effect.

- **Save**. Click Save to save above settings to Domain Forwarding list.
- **Cancel**. Click Cancel to return to Domain Forwarding page without saving.

Important: Wild card capability will only work at the beginning of the domain name.

Examples:

*.domain.com *wolf.domain.com	**Valid** usages of wild card
wolf.*.com wolf*.com were*wolf.com	**Invalid** usages of wild card

Editing Domain Forwarding

How to get here

Clicking on a Domain Name or IP Address link will allow modification to **Edit** the following:

- **Domain Name.** Use this text box to change the domain name to be forwarded.
- **IP Address.** Use this text box to change the forwarding IP address for stated domain.

Important: You must restart the SMTP service for the changes to take effect. To do this, click the **Services > SMTP Tab** to navigate to the SMTP Settings page. Click the **Restart** button.

Save. Click **Save** after you have made your changes. Then restart the SMTP service as mentioned above.

Cancel. Click **Cancel** to not save any changes and return to Domain Forwarding page.

Supported SMTP RFCs

The SMTP Server supports the following Request for Comments (RFCs):

- RFC 2821 and 2822 SMTP
- RFC 1869 SMTP Service Extensions
- RFC 1870 SMTP Service Extensions 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 provides support for "ETRN host.name" and "ETRN @domain .name."

- RFC 2222 SMTP Service Extension for Authentication. IMail supports PLAIN, LOGIN, and CRAM-MD5.
- RFC 2487 supports TLS negotiation via the STARTTLS command.

Web Calendaring (Old)

IMail Web Calendaring provides users with a web interface that lets them schedule tasks, record notes, set appointments, and receive e-mail reminders that contain the date, time, and description of the appointment. They can also send e-mail requests to other people to invite them to scheduled appointments.



Note: The New Web Calendar for the Web Client requires no services. This Web Calendar service was kept to allow a link to the old web calendar available in the Web Client. This link (located in the upper right corner of the Web Client) will only display as long as the Web Calendar Service is running. The new Web Calendar uses the WorkgroupShare databases and does not require services.

Web Calendaring supports Microsoft Internet Explorer version 6.0 or higher. Users can log on to **IMail Web Calendar** by logging into their web client and clicking on **Calendar** in the folder tree.

Related Topics

Web Address For IMail Web Calendaring (on page 410)

Web Calendaring Settings (Old)

How to get here



Important: After making changes, click **Save**. Navigate to the Service Administration page and restart the service.



Note: The New Web Calendar for the Web Client requires no services. This Web Calendar service was kept to allow a link to the old web calendar available in the Web Client. This link (located in the upper right corner of the Web Client) will only display as long as the Web Calendar Service is running. The new Web Calendar uses the WorkgroupShare databases and does not require services.

Use **Web Calendaring Settings** to specify the Web Server Port , Directory, Maximum Work Threads, SSL and Thread Pooling Settings for the Web Calendaring Server.

- **Web Server Port.** Enter the port on which the Web Calendaring server operates. By default the web port is set to 8484, but you can change it to any unused port. If you change the port, the Web Calendaring server must be stopped and restarted. If you do not have another web server on the same system, you can use the normal web port of 25.



Tip: If you use a non-standard port number (anything other than 25), users will need to specify the SSL port in the logon web address.

- **Web File Directory.** Enter the the path to the Web Files Directory. This directory contains the files used to create web pages for IMail Web Calendaring. If you change this directory, you must stop and restart the web server. Use **Browse** to locate the directory if it resides locally.
- **Max Work Threads.** Enter the value to set the maximum number of work threads that can be simultaneously used by IMail Web Calendaring. This setting to constrains the load on your web server. If an HTTP request requires a work thread and the maximum has already been reached, Web Calendaring returns a "server not available" message. This option does not require **Enable Thread Pooling** to be selected.
  - **Ignore Source Address in Security Check.** Select this check box if you want the web server to ignore the IP address that requested the page. This is useful with firewalls and service providers that use dynamic IP addresses (such as AOL). (Normally, the web server checks the IP address that requested the page against the IP address from which the user logged on.)
  - **Enable Keep Alive.** Select this check box if you want to create a persistent TCP connection between the Web Calendaring server and a browser (if the browser supports it). If this option is cleared, 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. Using Enable Keep Alive can improve performance by reducing overhead per request, but it also means that fewer resources are available for other processes.



Caution: If you use **Enable Keep Alive** and **Enable Thread Pooling**, then 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.

SSL Settings

- **Enable SSL.** Select this check box to use Secure Sockets Layer to encrypt communications with clients, and to accept SSL connections in addition to normal connections.
- **SSL Port.** Enter the Web SSL Port on which the Web Calendaring server listens for an SSL-based HTTP request if you enabled SSL. If you used the default Web Server Port (8484), you can assign any TCP port number here -- the default is 8485. If you used the standard web server port (port 80), then set the SSL port to the standard SSL port 443.
- **Force SSL.** Select this check box to set the Web Calendaring server to accept only SSL- based HTTP connections; normal HTTP connections are not accepted.

Thread Pooling Settings

- **Enable Pooling.** Select this check box to create a thread pool for handling HTTP requests from clients. IMail Web Calendaring creates up to 64 Max Work Threads to process requests. If this option is cleared, IMail Web Calendaring creates a thread to handle each request (either persistent or normal) and after handling that request, destroys the thread. IMail 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, then additional HTTP requests are denied. Also, threads reserved for use by IMail Web Calendaring are not available to other processes running on your server.
- **Thread Check Time.** Enter the interval (in seconds) used by IMail Web Calendaring to check the status of the thread pool. If the current number of work threads is less than Max Work Threads, new threads are created. This option is used only when thread pooling is enabled. The default value is 10 seconds.
- **Thread Exit.** Select this check box to close a thread after the HTTP request is processed completely. This option is used only when thread pooling is enabled. IMail Web Calendaring creates a replacement for closed threads on the next poll time, which is set in Thread Check Time. When this option is cleared, the thread is kept open and made available to process another request.

Save. Click to save your settings. An "Update Successful" message and the time of the update appear.

Setting Access to Web Calendaring

IMail Web Calendaring provides access to calendaring functions. You can assign access to IMail Web Calendaring for each individual mail account or globally for all users.

To set access to IMail Web Calendaring for an individual user mail account:

1. Click the **Domain** tab.
2. In the Domains list, select a domain. The Domain Properties appear.
3. In the left navigation bar, click **User Administration**. The Username list appears.
4. Click a user in the **Username** list. The User Properties appear.
5. Select the Allow Web Access option, then click **Save**.

To allow web access to all existing users:

1. Click the **Domain** tab.
2. In the Domains list, select a domain. The Domain Properties appear.
3. In the left navigation bar, click **User Administration, then click Standard User Settings**. The Standard User Settings appear.
4. Select the Allow Web Access option, then click **Save**.



Note: If you change an option in the User Properties page after you have set a Standard User Setting (global setting), the change overrides the global setting.

Web Address For Web Calendaring

By default, the 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. For example, if your IMail Server host is named mailhost1.ipswitch.com , then the Web address is:

http ://mailhost1.ipswitch.com :8484

Users can access the IMail Web Calendaring logon page by entering the address in the browser address field.

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

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 25. In this case, users do not have to specify the port with the web address. For example, you could enter: http://mailhost1.ipswitch.com

Important: If you use a non-standard port number (anything other than 25), users must specify the port in the logon web address.

Important: Some firewalls may block port 8484, in which case you need to change the port number for Web Calendaring.

Related Topics

Configuring the IMail Web Calendaring Server (on page 407)

Setting Access To IMail Web Calendaring (on page 409)

Setting Up SSL for Web Calendaring

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 only the intended recipients can read them.

To set up SSL for IMail Web Calendaring:

1. Use the IMail SSL Configuration Utility to set up the SSL certificate and public/private key pair. From the **Start** menu, select **Programs** > **IMail Server** > **IMail SSL Configuration Utility.** See the SSL Configuration utility's Help for more information.
2. In the IMail Administrator's *Web Calendaring Server Settings page* (on page 407), click **Enable SSL**.

CHAPTER 11

Logging

In This Chapter

About Logging 411
Log Manager 412
Sys Log Access Control 412
IMail Log Analyzer 414
Using the IMail Installation Log File 414
Enabling Web Client Logging 415

About Logging

The generic format of a log file entry is:

```
Date - Time - Thread or Process ID - Virtual IP Address - Message
```

Example: 06:26 09:16 SMTPD(0015052C) [127.0.0.1] connect 127.0.0.1 port 2358

Typical Log Files

Following are examples of typical log files:

- File names in the form of logMMDD.txt contain messages sent to IMail's log server .
- File names in the form of sysMMDD.txt are messages from services that have their log file format set to sysMMDD.txt.
- The W1yymmdd.log is the daily log file for the Web Administration server (when the Web Administration capability is enabled in the Monitor server).
- The 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* (on page 370) (such as POP3 or IMAP).

- **No Log**. Select this option to disable the logging of events.
- **SYSMMDD.TXT.** Select this option to send system 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* (on page 94).
- **Log Server.** Select this option to send event information to the Log file indicated on the *Log Manager* (on page 412) page.

Important: If you have all or many of your services logging to the Log Manager page and your computer sees a lot of traffic, the Log Manager file can become very large. You can disable logging for individual services where you don't need the log information. Normally, logging is only necessary if you are having problems with a service.

Related Topics

About the Spool Directory (Queue) (on page 94)

Log Manager

How to get here

The **Log Manager** page shows the log files in the IMail *spool directory* (on page 94). Log files are named with the format logMMDD.txt where MM is the month and DD is the date.

To view a log, click the link of the file you want to view, the page will open using Windows Notepad.

- **File Name.** This column displays the log files in the IMail spool directory. Click ▲ or▼ to sort the list. To view a log file, select the link under the file.
- **Size (kb).** This column displays the size of each log file. You can click ▲ or▼ to sort the list.
- **Date Created.** This column displays the date and time the log file was created. You can click ▲ or▼ to sort the list.

Delete. To delete a log file, select the check box corresponding to a Log file in the list to the right. Then click the **Delete** button.

Access Control (on page 412). To manage (by allowing or denying) Sys log access to other computers or client users.

Related Topics

About Log Files (on page 411)

Sys Log Access Control

How to get here

The Access Control page allows you to manage (allow or deny) Sys log access to other computers or client users, and contains listings of IP addresses that are either granted or denied access.

Important: You must restart the Sys logger service for the changes to take effect.

- **Deny all servers from communicating with this server except**. Choose this option if you want to grant access to a single specific computer or group of computers.

Note: This is an exception command; for example: deny access except to... 123.100.100.80.

- **Allow all servers to communicate with this server except.** Choose this option if you want to deny access to a single specific computer or group of computers.

Note: This is an exception command; for example: grant access except to.. 123.100.100.80.

Important: To edit an existing IP address or subnet mask, click the link under the IP address. The **Add Access Control** page appears with the existing information. Edit the information and click **Save**. Click **Cancel** if you no longer want to edit the IP address.

- **IP Address.** This column lists the IP Addresses allowed or denied access to the server.
- **Net Mask.** This column lists the Subnet Masks related to the IP Addresses allowed or denied access to the server.

Add. Click this button to access the Add Access Control page to grant or deny access to either a single computer or a group of computers.

Edit. Click this button to edit, after selecting from the list.

Delete. Click this button to remove an existing entry, after selecting from the list.

Save. Click to save your settings. A message "Your changes have been saved" will appear.

Related Topics

Adding to Access Control (on page 413)

Add / Edit Sys Log Access Control List

How to get here

Use the Access Control Add to add a single computer or group of computers to the Access Control List.

- **Add a Single Computer.** Select this option if you want to allow or deny access to a single computer. If you select this option, you may enter text into the IP address text box.
- **Add a Group of Computers.** Select this option if you want to allow or deny access to a group of computers. If you select this option, you may enter text into the Subnet Mask text box.
- **IP Address.** Enter the IP address of a single computer that you want to allow or deny Sys log access.
- **Net Mask.** Required only for a Group of Computers. Enter the subnet mask of the computer group that you want to allow or deny Sys log access.

 **Important:** You must restart the Sys logger service for the changes to take effect.

IMail Log Analyzer

Analyze is a log file analysis tool which compiles reports based on your IMail Server log files. It sorts through the log files and separates the information into reports, enabling you to browse statistical information quickly and easily. You can select from up to 19 different reports that extract information such as:

- the number of SMTPD connections
- the number of IMAP errors
- the number of web logins
- the number of web hits

To navigate to the IMail Log Analyzer

1. Click **Start > Programs > IMail Server > IMail Log Analyzer**.
2. The **Analyze** dialog appears. Click the **Help** button at the bottom of the dialog for assistance.

Using the IMail Installation Log File

The IMail installation wizard generates an install log file to help you troubleshoot software installation issues. If you selected the default installation folders, the log file is located in C:\install-log-mm-dd-yyyy.txt.

During installation each action that occurred with respect to permissions or IIS is prefixed with "***".

Permissions are logged as follows:

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program Files\Ipswitch\IMail" /T /E
/G IUSR_WIN2K3- SRVR:F
```

```
processed dir: C:\Program Files\Ipswitch\IMail

processed file: C:\Program Files\Ipswitch\IMail\ActivationStub.exe

processed file: C:\Program Files\Ipswitch\IMail\AVReadMe.htm

processed file: C:\Program Files\Ipswitch\IMail\IMailLogo.jpg

processed file: C:\Program Files\Ipswitch\IMail\css_releasenotes.css
```

Tip: If you want to search the log file for failures, search the log file for the strings **"No Mapping" or "!!!."**

The first line is the command string used to set the permissions. If this fails, instead of seeing "processed" lines in the log file, you will see:

```
*** C:\WINDOWS\system32\cacls.exe "C:\Program
Files\Ipswitch\Collaboration Suite" /T /E /G IUSR_WIN2K3- SRVR:F
```

No mapping between account names and security IDs was done.

IIS settings in the log file are not as detailed. If the item is not prefixed with "!!!" followed by "Failed," then it was successful. For example, the first line in the following example is a success:

```
*** Disabling anonymous rights on "IIM /Status.asp".

*** Disabling anonymous rights on "IIM/StartStopServices.asp".
```

The following line, disabling the anonymous rights on IIM/StartStopServices.asp, failed because it is followed by an "!!! Failed.":

```
!!! Failed to disable anonymous rights on "IIM/StartStopServices.asp".
```

Enabling Web Client Logging

The following procedure allows you to verify (by enabling URI queries in IIS) when a user is logged in, if that login was successful, and when the user logged out.

Note: IIS log files are stored in the following directory: %WINDOWS%\System32\LogFiles\

How to place user login messages in the IIS logs:

1. Go to **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**. The IIS Manager window appears.
2. On the left pane, select the Web site upon which the client resides, right-click, and select **Properties.** The Web Site Properties window appears.
3. The **Enable Logging** option should already be selected. Click the Properties button next to the **Active log format** list box. The Logging Properties dialog displays. Click the Advanced (or Extended) Properties tab. Select the **URI Query** Option.
4. Click OK for each dialog until all dialogs are closed.



Note: If you need more information on enabling logging for IIS, read the following KB: *http://support.ipswitch.com/kb/IM-20051206-DM01.htm* (http://support.ipswitch.com/kb/IM-20051206-DM01.htm)

Examples of what the user data will look like in the IIS logs:

```
14:55:27 127.0.0.1 POST /cypress/login.aspx
Login+Attempt:+[Marc]Login+Successful:+[Marc]+Language+Used:+en-US 302

14:57:01 127.0.0.1 POST /cypress/Login.aspx
Login+Error:+[Marc]+Failed+to+authorize+user. 200

15:23:31 127.0.0.1 GET /cypress/Logout.aspx Logout:+[Marc] 200
```

CHAPTER 12

Command Line Utilities

In This Chapter

Adding Aliases using "addalias.exe" Utility 417
Adding a Virtual Host (adddomain.exe) 421
Adding Users (adduser.exe) 422
Rename a User (RenameUser.exe) 428
Overview (antispamseeder.exe) 429
Registry Backup 431
Web Site Updater (IClientUpdater.exe) 434
Initializing and Synchronizing LDAP Databases (iLDAP.exe) 435
Cleaning the Spool Directory (Isplcln.exe) 436
Deleting Old Messages (immsgexp.exe) 436
Populating the LDAP Database (ldaper.exe) 438
Sending Mail to All Users (mailall.exe) 439
Checking the Registry (regcheck.exe) 440
SMTP Delivery Application (smtp32.exe) 443
Self-Signed SSL Certificate(sslutility.exe) 443
Creating Config_CommonAddrBook.cgi 445
Command Line Installations (Silent Installs) 445

Adding Aliases using "addalias.exe" Utility

Addalias.exe is a utility for adding, modifying, and deleting batches of e-mail aliases stored in a text file. You can also import an existing Windows NT group into IMail and create a group alias. If you invoke Addalias.exe with no command line options (by entering only `addalias` at the MS-DOS prompt), you can manually input command lines, then press **Enter** after each line. Make sure that you press **CTRL-Z** to exit the utility when you are done. *Example* (on page 191)

Basic Command Syntax

```
addalias [-h hostname] [-cX] [-{a|d|m}] alias [=destination]
```

Command	Function
-a aliasname	Adds an alias if the alias does not exist. aliasname is the name of the alias you want to add. Only one alias may be added in a single command line.
-cX	Specifies an alternate delimiting character, which replaces the default delimiter (the equal sign). Spaces are not allowed. (Using -c in a text file affects all lines in the file.)
-d aliasname	Deletes 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	Specifies the virtual domain for the alias. The primary domain is used if no e-mail domain is specified. (Using -h in a text file affects all lines in the file.)
-i groupname	Imports an NT group as a group alias if the alias does not already exist. groupname is the group that you want to import. Only one alias can be added in a single command line.
-l	Lists current aliases. This argument may not be used in a text file.
-m aliasname	Modifies or adds an alias even if the alias exists. aliasname is the alias you want to modify. Only one alias may be modified in a single command line.
-?	Displays a summary of argument options.



Important: Windows 2000 and Advanced Server Users. You can import NT groups as an alias only for local and global groups. You cannot import NT groups with Microsoft Active Directory Services (ADS) Universal groups.

Addalias.exe Examples

Adding an Alias to the Default (primary) E-mail Domain (on page 189)

Adding an Alias to a Specific Domain (on page 189)

Deleting an Alias (on page 190)

Importing an NT Group as a Group Alias (on page 420)

Return codes

Addalias.exe 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 IMail Server from another mail system if the other mail server program can create a delimited text file of aliases. *Example* (on page 191)

Adding Alias to a Domain Using "addalias.exe"

Adding an Alias to a Specific Domain Using the addaliase.exe Utility

The following example adds an alias of newalias to the e-mail domain named `secondhost.com` and resolves to e-mail:

```
addalias -h secondhost.com -a newalias e-mail
```

Adding Alias to Primary Domain Using "addalias.exe"

The following examples add an alias of newalias to the default (primary) e-mail domain which resolves to e-mail:

```
addalias -c: -a newalias:email

addalias -a newalias=email

addalias -c: newalias:email

addalias newalias=email

addalias newalias email
```

Deleting an Alias using "addalias.exe" Utility

The following examples delete an alias:

```
addalias -d oldalias

addalias -h another.net -d alias1
```

Related Topics

`Adding an Alias using Addalias.exe` (on page 188)

Addalias Text File Example

Addalias.exe Text File Example

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, enter:

addalias < test.txt

The < symbol tells addalias to use test.txt as output.

You then get the following messages:

```
current host is wks003.augusta.ipswitch.com

added [wks003.augusta.ipswitch.com ] test1 -> me

added [wks003.augusta.ipswitch.com ] test2 -> test1

added [wks003.augusta.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
```

Import NT Group as Group Alias using addalias.exe



Important: Windows 2000 and Advanced Server Users. You can import NT groups as an alias only for local and global groups. You cannot import NT groups with Microsoft Active Directory Services (ADS) Universal groups.

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)**.

The following example takes an existing Windows NT group and converts it into an IMail group alias:

```
addalias -h NThost.com -i groupname
```

Adding a Virtual Host (adddomain.exe)

AddDomain.exe is a utility for adding virtual domains. It can be used to simply add a single domain, but is especially useful in a batch file to add multiple domains.

Basic Command Syntax and Example

Usage:

```
adddomain -h Hostname -i IPAddress -t TopDir

[-a Aliases -u IM | NT | External -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -m

[-t TopDir -a Aliases -x MaxMBXSize -s MaxMBXMsgs -r MaxUsers]

adddomain -h Hostname -i IPAddress -t TopDir -u External

[-e DLLFilename -o ODBC_DSN -n TableName]

adddomain -h Hostname -delete

adddomain -f Filename
```

Examples:

1. In the following example, since the -e, -o,or -n options are not specified, the external database relies on the default “values %“Imail_top dir”%odbcuser.dll , IMAILSECDB, and [default] accordingly:

   adddomain -h newhost1 -i virtual -u external

2. The following command populates an external database with settings of C:\mydll.dll, IMAILSECDB, and [default]:

   adddomain -h newhost2 -i virtual -u external -e C:\mydll.dll

3. The following example changes an existing host (notice the -m for modify) to use an ODBC Data Source Name (DSN) of MyNewDSN. If the other fields of -e and -n were previously set, they will be preserved. If the other fields of -e and -n were not previously set, they will be set with the default values:

   adddomain -h ExistingHost -m -u external -o MyNewDSN



Note: The -e, -o, and -n commands must be used in conjunction with -u EXTERNAL.

4. If you need to specify a DSN other than ‘IMailSecDB,’ or you need to specify a userID and password (required when setting up a DSN to connect to an SQL database), use the -o switch :

adddomain -h ExistingHost -m -u external -o IMailSecDB;UID=MyUser;

PWD=MyPassword

5 The following example shows how to add a new virtual host (or virtual host with an IP) using an external database:

adddomain -u external -t C:\IMail\newdomain_com -i virtual

-o IMailSecDB;UID=sqluser;PWD=sqlpassword -n table_name

6 Adddomain.exe supports the following command line options:

Command	Function
-h	Fully qualified host name; must match the IMail official host name
-i	IP address or virtual IP address for an IP-less host
-t	Path (full or relative) to the top directory for the domain
-m	Command to modify existing settings instead of creating new ones
-a	Alias list for a host
-u	User data base to use (IMail, NT, or external)
-e	Path to external database implementation DLL
-o	External database ODBC system Data Source Name (DSN)
-n	External database table name
-x	Default max mailbox size (in kbytes).
-s	Default max number of messages for mailbox.
-f	Path to the file containing the settings to modify
-r	Maximum number of users allowed on this host.
-delete	Removes the virtual host.



Note: AddDomain.exe does not warn when assigning already claimed 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 4 and 15 characters.

If you invoke adduser with no command line options (by typing only adduser at th e 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.



Note: Using the adduser.exe utility to create users does not apply the default user settings as defined in IMail Administrator.

Basic Command Syntax

```
Adduser.exe [-h hostname] [-k userid] [-m userid] [-u userid]

[-p password] [-n name] [-f filename] [±chgpass] [±web]

[±active] [±info]
```

Return codes

Adduser.exe returns 1 if it performed at least one of the requested operations; adduser returns 0 if it failed.

Disabling Web Options

New users have all 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.

Examples:

Adding 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 test 01

Deleting a user ID.

Adduser -k -u test01

Adduser -h another.net -k test01

Related Topics

Using a Text File (on page 190)

Command Options (on page 424)

adduser.exe Options

Adduser.exe Command Options

Command	What it Does
-h hostname	Specifies the user's virtual host , where hostname is the name of the host. The primary host is used if no host is specified. Using -h in a text file, affects all lines in the file.
-k userid	Deletes a user id, where userid is the id you want to delete. Only one user id may be deleted in a single command.
-m userid	Modifies a user id, where userid is the id you want to modify. Only one user id may be modified in a single command.
-u userid	Adds a user id, where userid is the id you want to add. Only one user id may be added in a single command.
-n "name"	Specifies the full name of the user in double quotes, where name is the user's full name.
-p password	Specifies a password for the user. If you omit this command, the default password is 'password.'
-q	Disables alias duplicate check.
-cX	Specifies an alternate delimiting character represented by X. adduser.exe replaces the default delimiter (a comma) with the specified delimiter. Spaces are not allowed. Using -c in a text file, affects all lines in the file.
-f filename	You can put multiple commands into a text file for one execution of adduser.exe. Use this command to specify the name of the file containing the commands. All commands are valid for the text file, but - h and -c persist across multiple lines.
-chgpass	Disables the user's ability to change his/her password.
+chgpass	Enables the user to change his/her password.
-web	Disables the user's ability to use Web messaging.

+web	Enables the user to use Web messaging.
-active	Disables the user’s ability to log on.
+active	Enables the user to log on.
-info	Disables the display of the user's information in LDAP queries.
+info	Enables the display of the user's information in LDAP queries.
-?	Displays a summary of argument options.
# : ;	Comments (for use in a text file)

Example Text File (Adduser.exe)

Example Text File (Adduser.exe)

#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 file above:

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

Using a Text File (adduser.exe)

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 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 wks013.augusta.ipswitch.com -f addfour.txt
```

You then get the following messages:

```
current host is wks013.augusta.ipswitch.com

OK: added userid to host wks013.augusta.ipswitch.com

OK: added smith to host wks013.augusta.ipswitch.com

OK: added test1 to host wks013.augusta.ipswitch.com

OK: added jones to host wks013.augusta.ipswitch.com
```

Note that the user named test1 will have "password" (the default) as his password.

Example File (on page 425)

Rename a User (RenameUser.exe)

"RenameUser.exe" is a command line utility for renaming only one Username. This utility can only be used on an IMail or external database. RenameUser.exe cannot be used for domains using Windows NT or Active Directory as user database.

If you invoke "RenameUser" with no command line options (by typing only renameuser at the MS-DOS prompt), you will be shown the syntax required for usage.



Note: Renaming a username will also rename all associated lists, aliases, and collaboration user names.

Basic Command Syntax

```
RenameUser.exe [old_user@domain_name] [new_user]
```

Return Errors

- **The user does not exist.** The username does not exist within the domain entered. Be sure that the Username is correctly spelled.



Important: RenameUser will only allow changing a Username within the same domain.

- **The domain does not exist**. Be sure that the Username and Domain name are correctly spelled.

Example:

Renaming "flip@mydomain.com" to "flop@mydomain.com"

```
renameuser flip@mydomain.com flop
```

Overview (antispamseeder.exe)

The antispamseeder.exe utility, located in the IMail top directory, is used to manage the spam and non-spam word counts contained in the antispam-table.txt file. You can use this utility to modify the antispam-table.txt file in the following ways:

- Re-assign the word counts contained in the `antispam-table.txt` file, when e-mail is incorrectly identified as spam (false positive), or vice versa. This increases the likelihood that such messages will be correctly identified in the future.
- Create a new antispam-table.txt file that applies only to a specific host.
- Add new words to the `antispam-table.txt` file.
- Delete words from the `antispam-table.txt` file that do not occur very often to decrease the size of the file.
- Enter wildcards (i.e. g* *d) into the `antispam-table.txt` file so that statistical filtering will identify such words as spam.



Note: If any of the procedures listed below are performed by a secondary host, that host will either need to copy antispamseeder.exe to the secondary host's directory, or access antispamseeder.exe from the primary IMail domain 's directory.

Procedures:

Resolving incorrectly identified e-mail (on page 339)

Creating a host's antispam-table.txt file (on page 340)

Customizing a host's antispam-table.txt file (on page 342)

Adding new words to the antispam-table.txt file (on page 337)

Modifying the word counts in the antispam-table.txt file (on page 343)

Deleting infrequent words from the antispam-table.txt file (on page 338)

Merging Antispam-table.txt files (on page 336)

Creating URL Domain Black Lists (on page 344)

Simultaneously Merge Domain Links List and Antispam- Table.txt Files (Simultaneously_Merge_Domain_Links_List_and_Antispam_Table_txt_Files.htm)

Identifying wildcards in e-mail (on page 346)

Related Topics

Antispamseeder Parameters (on page 335)

Understanding the Antispam-table.txt file (on page 430)

Merging Antispam-table.txt Files Example

Suppose that at installation, you chose to store the updated word statistics in the `antispam-table-ini.txt` file, and now you want to merge them with your existing `antispam-table.txt` file. Assuming that your host is named "Host1", enter the following command:

```
antispamseeder.exe -tantispam-table-ini.txt -hHost1
```

Understanding the antispam-table.txt file

The `antispam-table.txt` file contains the word counts that content filtering uses to determine if a message is spam. Each word is assigned three values. The first value is the statistical value assigned by the antispam engine. The second value is the number of times that the word has occurred in non-spam e-mail messages. The third value is the number of times that the word has occurred in spam e-mail messages.



Note: The `antispam-table.txt` file was created using e-mail messages and words that were received at Ipswitch. You may find that the words and values contained in it are not entirely appropriate for your use. In this case you can customize the file based on your needs by using the *antispamseeder.exe utility* (on page 333).

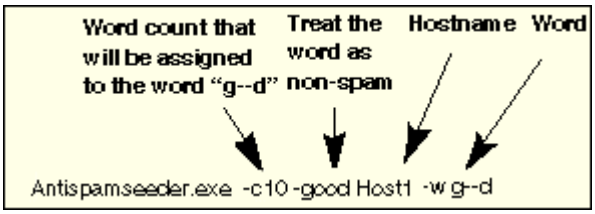
Antispamseeder.exe Wildcard Example 2

If you want the antispam engine to identify the word "2Sexy" as spam, add it to the antispam-table.txt file by entering the following command, replacing domain.com with your domain name:

```
antispamseeder.exe -spam -w-sexy -c100 - hdomain.com
```

This command adds the word "-sexy" to the antispam-table.txt file as if it had occurred 100 times in spam e-mail. The word will now be treated as a spam indicator by the content filters.

If you want the antispam engine to identify the word"g00d" (with zeros) as spam, you must enter the word into the antispam-table.txt file by running the following command, substituting dashes for the non-alphabetic characters. In this example, " host1" is the hostname and "g- -d" is the word you want to be recognized as spam.



Once you run the above command, the antispam engine will recognize any variable of the word "g- -d" as spam, such as g00d, g**d etc. This command does not change the word count for the word "good" because it does not contain any non-alphabetic characters.

Antispamseeder.exe Wildcard Example 1

If you want the antispam engine to identify the word 2Sexy as spam , add it to the antispam-table.txt file by entering the following command, replacing domain.com with your domain name:

```
antispamseeder.exe -spam -w-sexy -c100 - hdomain.com
```

This command adds the word "-sexy" to the antispam-table.txt file as if it had occurred 100 times in spam e-mail. The word will now be treated as a spam indicator by the content filters.

Registry Backup

In This Section

Back Up IMail Registry (on page 105)

Restoring IMail Registry (on page 106)

Backing Up System Files (on page 107)

Backing Up User Mailboxes (on page 107)

Back Up IMail Registry

There are two methods of saving the IMail registry keys. Select one that is fits best.

Important: This will only backup user data for domains that use the IMail User Database.

Backing Up Registry with Command Line

To backup the registry keys for IMail using **command line** use the following steps.

1. Click **Start > Run > "cmd"**. This will open a DOS window.
2. At the DOS prompt enter the following command all on one line:

```
regedit /e c:\imail\imail.reg
HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail
```

3. Entering a different path or file name is up to the administrator.

This will copy the complete IMail registry "hive" to the c:\imail directory folder.

Backing up Up Registry Manually

To backup the registry keys **manually** using export with the following steps:

1. Click on **Start > Run >** type "**regedit**" and click OK.
2. Go to the path: `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`
3. Select "IMail" Registry key
4. Right click and select "Export".
5. Select the desired path, and name the file.
6. The "selected branch" field should show the following:
7. `HKEY_LOCAL_MACHINE\Software\Ipswitch\IMail`
8. Click **Save**.

This will save all domain data, user names and user passwords for all domains that use the IMail user database.

Related Topics

Restoring IMail Registry (on page 106)

Backing Up IMail Server System Files (on page 107)

Backing Up User Mail (on page 107)

Restoring IMail Registry

There are two methods of restoring the IMail registry keys. Select one that is fits best.

Restoring using Windows Explorer

1. Go to Windows Explorer and double click on the exported .reg file
2. A prompt asking if you are sure that you want to add the information in "path name".reg file to the registry. Click "Yes" if the path name looks correct.
3. A prompt telling you it was successfully entered into the registry.

Restoring using "regedit"

1. Make sure a copy of the registry file is on the server.
2. Click on **Start > Run >** type "**regedit**" and click OK.
3. Click File > Import
4. Browse to the copy of the registry file on the server.

The current IMail registry keys will be overwritten with the selected file.

Related Topics

Back Up IMail Registry (on page 105)

Backing Up IMail Server System Files (on page 107)

Backing Up User Mail (on page 107)

Backing Up IMail Server System Files

IMail Server stores its system files in the \IMail directory, unless you have given it a different name. You can make a backup copy of the IMail Server directory tree.

Related Topics

Back Up IMail Registry (on page 105)

Restoring IMail Registry (on page 106)

Backing Up User Mail (on page 107)

Backing Up User Mail

Users' mail is stored in directories below `\IMail`, usually under `IMail\users`, but each domain may have mail stored, under `\IMail\domain\users`, if default paths were selected.

Daily backups should include these directories.

Related Topics

Back Up IMail Registry (on page 105)

Restoring IMail Registry (on page 106)

Backing Up IMail Server System Files (on page 107)

Web Site Updater (IClientUpdater.exe)

IClientUpdater.exe is a utility designed for users that have multiple IClient web sites for branding purposes. This utility will search through all web sites looking for the IClient.config file, and will allow the user to update web sites that were created for branding.

Warning: IIS will be stopped and restarted to avoid locked files.

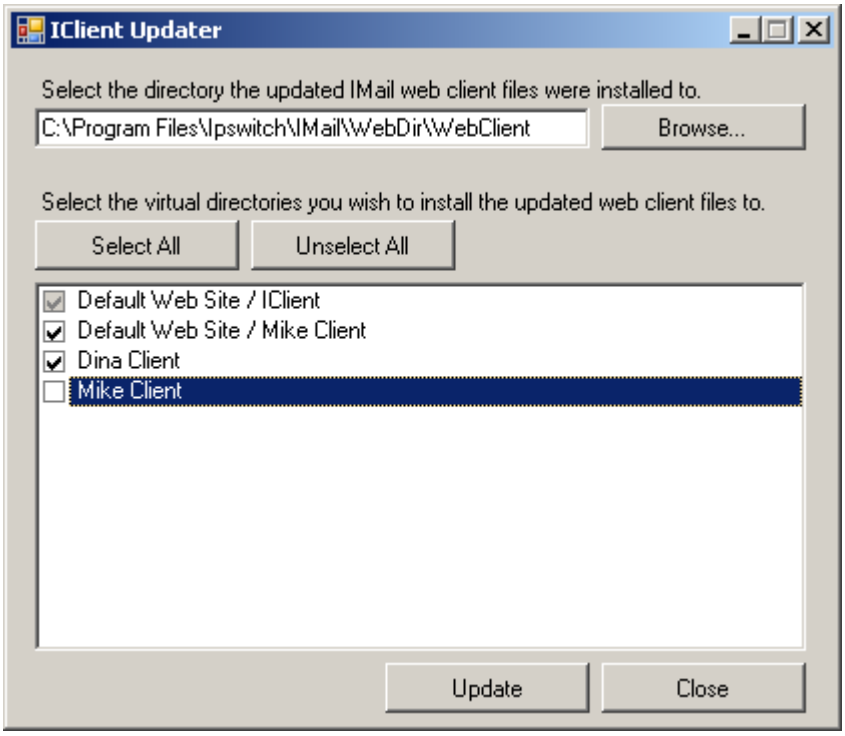
Select the directory the updated IMail web client files were installed to. The text box displays the default path that the Install updated.

Note: `"web.config"` file will not be overwritten, to protect branding.

Browse. Use the Browse button to modify this path.

Select All. By default all web sites found will be selected. Uncheck the web sites that you do not want updated.

Unselect All. Click **Unselect All** to uncheck all web sites.



Update. Click update to copy the contents of the new IMail web client to the selected web sites.

Close. Click this button to close the utility without running the utility.

Initializing and Synchronizing LDAP Databases (iLDAP.exe)

iLDAP.exe is a utility to Init or Sync a specified LDAP domain or all the LDAP domains. This utility can be used in the case when the Web Administrator does not properly Init or Sync all the LDAP domains on a server. This issue sometimes occurs on servers running Microsoft Windows 2003 machines with over 30 domains.

Basic Command Syntax

```
iLdap -i|s[<domain>]
```

where domain is the domain you want to Init or Sync. All the domains are initialized or synchronized if no domain is specified.

Command	Function
-i	Initializes the specified LDAP database.

-s	Syncrhonizes the specified LDAP database.

Related Topics

Populating the LDAP Database Using Ldaper.exe (on page 381)

Cleaning the Spool Directory (Isplcln.exe)

Isplcln.exe is a command utility that 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: 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 deletes all log files that are thirty days old or older.

Command	Function
-x	The number of days old a file must be before it is deleted.
-y	The number od days old a log file must be before it is deleted.

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
      -m specific_mailbox
```

`-f fully_qualified_path_to_mailbox (cannot be used with -t and -m)`

The `"startdirectory"` will be scanned search only `"specific_mailbox"` and any message older than `"#of_days_to_save"` will be deleted.

Option -f gives capability to delete `"#of_days_to_save"` from a `"fully_qualified_path_to_mailbox"`.

Warning: -t option can not be used with the -f option.

Warning: -m option will be ignored if used with the -f option.

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).

Examples:

The following command deletes all messages in the `"C:\Program Files\Ipswitch\IMail"` directory that are more than 60 days old.

```
immsgexp -t"C:\Program Files\Ipswitch\IMail" -d60
```

The following command deletes all messages in the "spam" mailbox located in the c:imail directory that are more than 60 days old.

```
immsgexp -t"C:\Program Files\Ipswitch\IMail" -mspam.mbx -d60
```

The following command deletes messages in the `"sent"` mailbox of the User "jdoe" that are more than 90 days old.

```
immsgexp -d90 -f"C:\Program Files\Ipswitch\IMail\jdoe\sent.mbx"
```

immsgexp.exe command line options

Command	Function
-t	The directory containing the mailboxes from which messages will be deleted.
-d	The number of days that a message will remain on the server before it is deleted.
-m	The name of the mailbox from which messages will be deleted.
-f	Full path to the specific mailbox. **Warning -** Can not be used with the -t option. **Warning** - The -m option will be ignored when using this option.

Populating the LDAP Database (ldaper.exe)

`Ldaper.exe` populates the LDAP database with user properties for all users on a selected e-mail domain. This may be particularly helpful after you have added a large number of users at once using the *Adduser.exe utility* (on page 422).

Important: If you are upgrading from IMail Server prior to version 8.1, an LDAP database conversion occurs during installation. The conversion can take a lengthy amount of time depending on the number of domains to convert. If the LDAP data is not available after the upgrade, run the LDAP Convert utility to correct the issue. In the command line utility, type: ldaper /CONVERT /Y

Basic Command Syntax

ldaper [options]:

`Ldaper.exe` supports the following command line options. Options can be prefixed with a hyphen or a forward slash.

Option	Explanation
-H	Host name
-U	User ID
-P	Password
-GN	First name
-HN	Last Name (Sur Name)
-S	Street Address
-C	City
-ST	State
-CO	Country
-Z	Postal Code
-T	Telephone
-O	Organization
-OU	Organizational Unit (Department)
- CONVERT	Converts LDAP dbases prior to version 8.1 to the new OpenLDAP dbase schema
-Y	Required option with the CONVERT option
-LSTART	Keeps the LDAP service running

Related Topics

Init & Sync LDAP DB - iLDAP.exe utility (on page 382)

Adding Users Using Adduser.exe (on page 422)

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 system.

Basic Command Syntax

mailall -h hostname|ALL> -f sender -d [-s Subject] <FullPathToMessageFile>

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. When an e-mail is sent to the program alias, the executable program is invoked and the entire contents of the message is passed as the text for the "mailall.exe" message.

Command	Function
-h hostname	The -h parameter is required. Use it to enter the hostname.
-h ALL	The -h parameter is required. Use this command to specify all hosts on the IMail system.
-f sender	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	This is an optional parameter that specifies the content of the Subject field.
-d	Optional. Use -d to delete the source files when mailing is complete.
FullPathToMessageFile	This parameter is required.

Checking the Registry (regcheck.exe)

`Regcheck.exe` is run automatically during a repair or upgrade, and can also be run from the command line. Regcheck troubleshoots registry conflicts during upgrades and repairs.

Basic Command Syntax

```
regcheck
```

What do the RegCheck messages mean?

Message	Example	Translation
Missing primary domain %Official Host Name%	Missing primary domain imail.ipswitch.com	The hostname defined in the 'HostName' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global does not match a key in HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains.
Primary Host %Official Host Name% address is %IP Address%	Primary Host imail.ipswitch.com address is 192.168.1.1	This tells you the Primary Domain defined by the 'HostName' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global and its IP defined by the 'Address' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%OfficialHostName%.
Could not find address for primary host %Official Host Name%	Could not find address for primary host imail.ipswitch.com	The 'Address' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%OfficialHostName% does not exist.
Could not find Global HostName, host key check failed	Could not find Global HostName, host key check failed	The 'HostName' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Global does not exist.
Could not find IMail Global key,	Could not find IMail Global key, host key check failed	The Global key under the HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail does not exist.

Message	Example	Translation
host key check failed		
Could not find IMail Domains key, domain registry check failed	Could not find IMail Domains key, domain registry check failed	The Domains key under the HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail does not exist.
Dup Official %Official Host Name% Official %IP Address% and %IP Address%	Dup Official imail.ipswitch.com Official 192.168.1.1 and 192.168.1.2	There are multiple Address keys under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains that contain the same 'Official' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%IP Address%.
Domain / official mismatch: official - %Official Host Name% Address - %IP Address%	Domain / official mismatch: official – imail.ipswitch.com Address – 192.168.1.1	The 'Address' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%OfficialHostName% is %IP Address%, but other Address keys under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains contain the same 'Official' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%IP Address%.
Domain / official mismatch: missing address key in domain %Official Host Name%	Domain / official mismatch: missing address key in domain imail.ipswitch.com	The 'Address' value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% does not exist.
Address %IP Address	Address 192.168.1.3 Official key	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%IP Address% contains an 'Official' value of %Official Host Name% that does not contain a key under

Message	Example	Translation
% Official key %Official Host Name% domain does not exist	mail3.ipswitch.com domain does not exist	HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains.
Dup Address %IP Address % Domain %Official Host Name% and %Official Host Name%	Dup Address 192.168.1.1 Domain imail.ipswitch.com and mail2.ipswitch.com	The Address value for HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% and HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% are the same.
Dup TopDir Domain %Official Host Name% and domain %Official Host Name%	Dup TopDir Domain imail.ipswitch.com and domain mail2.ipswitch.com	The ‘TopDir’ value for HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% and HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% are the same.
Domain entry %Official Host Name% has no IP entry	Domain entry mail4.ipswitch.com has no IP entry	The ‘Address’ value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% references an address that does not contain a key under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains.
Domain IP / system IP mismatch - %Official Host Name% Address - %IP	Domain IP / system IP mismatch - mail4.ipswitch.com Address-10.10.10.1	The ‘Address’ value under HKEY_LOCAL_MACHINE\SOFTWARE\Ipswitch\IMail\Domains\%Official Host Name% references an address that is not bound to the NIC.

Message	Example	Translation
Address %		
System IP found - %IP Address %	System IP found - 192.168.1.4	The IP that is bound to the NIC.

SMTP Delivery Application (smtp32.exe)

The smtp32.exe is a command line utility that lets you:

- Start IMail queue runs
- Pass messages back to IMail for delivery

Smtp32.exe supports the following command line options:

Parameter	Function
smtp32	With no options, smtp32 will attempt to deliver all messages in the mail queue.
smtp32 queue_filename	Causes smtp32 to process the single messages pointed to by the queue_filename.
smtp32-qr	Causes smtp32 to attempt to deliver all messages in the mail queue.
smtp32 -v	Activates full display of the conversation (verbose)

Self-Signed SSL Certificate(sslutility.exe)

IMail ships with an SSL Configuration Utility that you can use to create your own 128-bit SSL certificate. You can use the self-signed certificate within IMail, or you can purchase a trusted SSL certificate from a registered CA. To create a self-signed certificate, use the following steps:

1 Open the IMail SSL Configuration Utility **Start > Programs > Ipswitch IMail Server > IMail Server > IMail SSL Configuration Utility** and click the **Certificate Creation** tab.

2 Click the **Browse (...)** button in the **Output Location** box to select the folder you want the certificate created in.

3 Enter information in all of the Certificate Information boxes:

- **City/Town.** City or town where you are located. (Ex. Augusta)
- **State/Province.** State or Province where you are located. (Ex. Georgia)
- **Organization.** Company or individual user name.
- **Common Name.** The hostname you enter here should be the hostname users use in their browsers to connect to Web Messaging/Calendaring.

  For example: If users normally connect to: `http://webmail.maildomain.com` then, enter `webmail.maildomain.com` into the **Common Name** field.
- **Pass Phrase.** Pass phrase that is to be used to encrypt the private key. It is important to remember this pass phrase. The pass phrase can be any combination of words, symbols, spaces, or numbers.
- **Pass Phrase Confirmation.** Re-enter the same pass phrase as above.
- **Country.** The country you are in. This must be a valid two letter country code. (i.e. US)
- **E-mail.** E-mail address of an administrator for the server.
- **Unit**. Name of organizational unit. (Ex. IT or Information Systems)

4 After all of the boxes are filled in correctly, click **Create** to generate the keys, certificate, and certificate signing request.



Note: If all of the boxes are not filled in, you cannot create the certificate.

5 Once the SSL Certificate has been created, you must select go to the **Certificate Selection** tab and point to the new certificate to be used in SSL connections to the IMail server.

- **Private Key**. Click browse and locate new key.
- **Certificate**. Click browse and locate new certificate.
- **Pass Phrase**. Enter pass phrase associated with new certificate.
- **Pass Phrase Confirmation**. Re-enter pass phrase.
- Click **"Apply"** to save settings.

Related Topic

Installing SSL Keys (on page 32)

Creating Config_CommonAddrBook.cgi

You can create a Public Contacts folder that can be used in IMail (no Outlook or Collaboration WorkGroupShare required).

To create contacts:

1. Open Notepad.
2. Enter your contacts in the following manner: contact name<space>-<space> contact e-mail address, separating each entry with a comma and no spaces.

   Example:

   ```
   Sam - SSmith@yahoo.com,Josie - jbrown@hotmail.com,HumanResources - hr@ipswitch.com
   ```
3. When you have finished, close the Notepad file and save it as Config_CommonAddrBook.cgi.
4. Add the file to the IMail\Web directory for your primary domain. For all non-primary domains the file should be added to the IMail\DomainName\Web folder.
5. When the user opens his/her e-mail in the Client, a Public Contacts folder appears.



To create a Public Contacts folder for a non-primary domain follow the steps 1 - 3 above. Create a "Web" folder within the non-primary domain. Add the new config_CommonAddrBook.cgi file in the new "web" directory.

Command Line Installations (Silent Installs)

Command Line installation is similar to silent installations as it is capable of installing IMail Server with no User Interface. This method allows new IMail Server installations to be started with command-line settings initialized to suit each computers need, requiring minimal if any interaction from the user.



Note: Silent Installs currently will only install using the IMail User Database.

See **example** at bottom of the page.



Warning: This command line utility will currently **not** work for repairs or upgrades. It was designed for new installations only.



Note: Activation on multiple computers will require multiple serial numbers.

Command Line Options

Non-Interaction	
--no-ui	Runs the install without interactive dialogs. Default setting if omitted: All dialogs for IMail installation will display.

Activation	
--serial-num	 Specifies the **serial number** to activate.  **e.g. --serial-num="aa9bb99ccc9ddd8drs9321"**  **Warning:** The installation will fail without a valid serial number that is 23 characters in length.

IIS Configuration	
--webadmin-ip	Setup will install the admin and client web applications to a web site using this IP address. If an IIS site does not exist for the given IP, it will be created. Can be used with **webadmin-port.** Default setting if omitted: IP Address from the Default Web Site
--webadmin-port	Setup will install the admin and client web applications to a web site using this port. If an IIS site does not exist with the given port, it will be created. Can be used with **webadmin-ip**. Default setting if omitted: "80"
--restart-iis	Setup option for restarting IIS upon completion of install. Default setting if omitted: "yes"

Installation Directory	

--install-dir	Specifies directory path for installation. Default setting if omitted: `c:\Program Files\Ipswitch\IMail`

Domain Configuration	
--domain	Setup to use given domain as the primary domain. Default setting if omitted: Computer_Name
--admin-id	Setup will use given "Userid" to create Admin User. Must be used with `"admin-pwd"` Default setting if omitted: "Administrator"
--admin-name	Setup will use given "Full Name" to for creating the Admin userid. Must be used with `"admin-pwd"` Default setting if omitted: "IMail Administrator"
--admin-pwd	 Setup will use given password for the Admin UserID.  This setting is required by `"admin-id"` and `"admin-name"`, but can be used alone.  Default Setting if omitted: System Administrator is not created  If this setting is omitted a System Administrator is not created.



SSL	
--install-ssl-keys	Setup will install default SSL keys unless "no" is set for this setting. Default setting if omitted: "yes"

Service	

Configuration	
--svc-start	Selecting services to automatically start. ▪ queuemgr - Queue Mgr ▪ imap4d32 - IMAP ▪ pop3d32 - POP ▪ slapd - LDAP ▪ syslogd - Sys Logger ▪ IMServer - Instant Messaging Default setting if omitted: `"smtpd32"` only
--smtp-logging	Setup will enable "Verbose Logging" for SMTP Log Setting by date. e.g. --smtp-logging="verbose" Default setting if omitted: Not checked.
--smtp-listen-all	Setup will enable "Listen on all IP's" an SMTP option. e.g. --smtp-listen-all Default setting if omitted: Not checked.

Example of Silent Install

```
imail-setup.exe --no-ui --serial-num="aa9bb99ccc9ddd8drs9321"
--webadmin-port="8383" --restart-iis="no" --install-dir="c:\IMail"
--domain="mydomain.com" --admin-id="sysadmin" --admin-name="IMail Admin"
--admin-pwd="password" --install-ssl-keys="no"
--svc-start=queuemgr,imap4d32,pop3d32,syslogd --smtp-logging="verbose"
--smtp-listen-all
```

Above example will install as follows:

- No UI will display for new installation with the serial number `"aa9bb99ccc9ddd8drs9321"`
- The Web Admin & Web Client applications will default to port `"8383"` using the IP Address of the default website.
- IIS will not be restarted.
- Installation path will be `"c:\IMail"` with primary domain name being `"mydomain.com"`.
- A system admin will be created called `"sysadmin"` with a Full Name of "IMail Admin" and password = `"password"`.
- No default SSL keys will be installed.
- The following services will be restarted upon successful installation: SMTP (is always started), Queue Manager, IMAP, POP3, and Syslog
- SMTP logging will be set to "Verbose Logging, with "Listen on All IP's" enabled on SMTP.

-

CHAPTER 13

Using IMail Web Messaging (Web Client)

In This Chapter

What is Web Messaging? 451

Access and Login to IMail Web Messaging Client 451

Low Bandwidth Web Messaging Lite 453

LBW - Enable Cookies 453

User Impersonation by System Administrators 454

Changing the Web Client Default Directory (setting a redirect for Web Messaging) 455

Configuring Web Messaging Email List Auto-Refresh Frequency 455

Accessing Spell Check Dictionary 456

Setting Up SSL for IMail Web Messaging 457

What is Web Messaging?

IMail Web Messaging (Web client) lets users send and receive mail using a web browser. Users can log on to IMail Web Messaging from a browser on any computer with a supported browser and manage e-mail without installing e-mail client software.

IMail Web Messaging directly accesses the server to manage mail, and no longer requires IMAP. After logging in, users can manage e-mail from the browser, organize e-mail into folders (mailboxes), maintain an address book (contacts) and auto-synchronize it with Microsoft Outlook contacts (if the WorkgroupShare Client has been installed), and set delivery rules for incoming mail.

When a user creates a mailbox in IMail Web Messaging, the mailbox is created on the mail server and mail folders and messages reside on the server.

Access and Login to IMail Web Messaging Client

Web Messaging Access

To launch the Web Client, in your browser address box, type the IP address or URL of the IMail Web Server followed by the **IMail Web Messaging** path.

Example:

http ://123.100.100.80/IClient, then press **ENTER**. The Web Messaging login page appears.

Note: IMail Web Messaging directly accesses the server to manage mail, and no longer requires IMAP.

Web Messaging Login

Enter your **Username** and **Password** and then click **Login**. If the login information is correct, the client login page will appear.

Note:To login to **Web Messaging Lite**, check the **Use Web Messaging Lite** checkbox.

When logging in for the first time on a new computer a cookie is generated.

Note: *Cookies must be enabled* (on page 453) for a user to successfully login.

The cookie will remember all the settings below on their next login:

- **Language:** Web Messaging contains a list box for Languages, you can read messages composed with international characters in the following languages:
  - English
  - Chinese Simplified
  - Chinese Traditional
  - French
  - German
  - Italian
  - Japanese
  - Spanish
- **Use Web Messaging Lite:** This checkbox will log you into the low bandwidth client, designed especially for users with dial-up modems. This web client has *limited capability* (on page 453), and was not designed with all the advanced options and features that the regular web client offers.
- **Remember my username:** Select this check box if you wish the client to remember your username on the local machine, only.
- **Remember my password:** Select this check box if you wish the client to remember your password on the local machine, only.

Note: Username and encrypted password information are stored in cookies on your computer.

Low Bandwidth Web Messaging Lite

Web Messaging Lite allows users with low-bandwidth (dial-up) capability to access their mail quicker. To allow this capability, framesets, icons, and certain processes were removed to allow for faster load in a low-bandwidth environment. Users can log into Web Messaging Lite from any computer with a supported browser, and manage e-mail without installing e-mail client software.

The Web Messaging Lite has limited capability, and was not designed with all the advanced options and features that the regular web client offers.

Some of the features that have been removed are as follows:

- Rule maintenance has been removed, functionality still exists but to update your existing rules, login to the regular web client is required.
- Search capability was removed.
- Contact Groups maintenance has been omitted.
- Auto suggest has been disabled.
- Web Admin link has been omitted.

Note: Web Messaging Lite Help was designed for low-bandwidth capability. To keep the Help light certain processes were removed, such as the Index and Search features. To access these features login to the normal web client and click Help.

LBW - Enable Cookies

If after attempting to login to the IMail Server web interface you receive this error message:

"Your request could not be served because you have browser cookies disabled. Please enable cookies in your browser's settings, close your current web session and try again."

Enable cookies for Windows Internet Explorer:

1. Open Internet Explorer.
2. Select **Tools > Internet Options**.

3 Select the **Privacy** tab.
4 Select **Advanced**.
5 Select **Override automatic cookie handling**.
6 Click **OK** to save changes.

Enable cookies for Mozilla Firefox:

1 Open Firefox.
2 Select **Tools > Options**.
3 Select the **Privacy** tab.
4 Select the **Cookies** tab.
5 Select **Allow sites to set cookies**.

Click **OK** to save changes.

User Impersonation by System Administrators

IMail System Administrators have the capability to access any users within their IMail Server without having to know the users password. Impersonation gives System Administrators access to a users web client mailbox to check, verify or assist with issues that may arise.

The System Administrator once logged in can do the following:

- Delete mail messages
- Move mail messages
- Create / Modify mail folders
- Full access to contacts
- Full access to rules
- Preference modification



Important: System Administrator impersonation will not allow sending mail, as authentication will prevent the mail to process. Impersonation will also not allow access to the users web calendar.

Using the IMail Web Client Login Page for Impersonation

- Enter the **Username** to be accessed (full domain name may need to be entered)
- Enter "/" after the **Username** with no spaces
- Enter System Administrator **Username**
- Enter **System Administrator Password**, then click **Login**.
- If the login information is correct, the IMail main page opens.
- **Language:** If your version of Web Messaging contains a list box for Languages, you can read messages composed with international characters in English, Chinese Simplified, Chinese Traditional, French, German, Italian, Japanese, or Spanish. You choose the language to send messages in via the Preferences page.

- **Remember my username:** Select this check box if you wish the client to remember your username on the local machine, only.
- **Remember my password:** Select this check box if you wish the client to remember your password on the local machine, only.

Note: For security, it is recommended to not check any **Remember** check boxes.

Impersonate Example:

Username: jsmith@domain.com/sysadmin@domain.com

password: System Administrator password

Note: localhost login does not require full domain name when accessing primary domain users.

Changing the Web Client Default Directory (setting a redirect for Web Messaging)

To set a redirect so Web Messaging users do not have to use \IClient in the URL for Web Messaging:

1. Click **Start** > **Programs** > **Administrative Tools** > **Internet Information Services**. The IIS console opens.
2. Right-click **IClient** (usually located under **Web Site** > **Default Web Site**).
3. Select **Properties**. The IClient Properties dialog box opens.
4. In the **Execute Permissions** list, click **Scripts only**.
5. Copy the directory path in the **Local Path** box.
6. Click **OK**.
7. Right-click **Default Web Site**.
8. Select **Properties**. The Default Web Site Properties dialog box opens.
9. Click the **Home Directory** tab.
10. Paste the directory path you copied from the IClient dialog box **Local Path** box into the Default Web Site Properties dialog box **Local Path** box.

Configuring Web Messaging Email List Auto-Refresh Frequency

You can change the setting for how often the Web Messaging (Web Client) e-mail message list auto-refresh occurs. In the IClient.config file (usually located in \Program Files\Ipswitch\Collaboration Suite\WebDir\WebClient), under the <appSettings> node,

change the value for the following AutoRefresh key:
`<add key="AutoRefresh" value="300"/>.`

This key contains a numerical value that corresponds to how often the auto-refresh occurs. By default this value is set to 300 seconds (5 minutes). Please note that the word “seconds” does not appear in the value. Only numerical values are valid for this key, for example: 300. If for any reason you want to disable the e-mail message list auto-refresh, set the value to 0.

Note: The AutoRefresh setting affects all Web Client users.

Accessing Spell Check Dictionary

Modifications to the Spell Check Dictionary are not recommended, except for line deletions. This file is named `"en-US.dic"` and exists under the `"WebDir\WebClient\dic"` directory.

Important: Any changes to dictionary files will be lost during an upgrade or re-installation.

If logging in with a different language the associated dictionary file is substituted as follows:

- en-US.dic = English - United States
- fr-FR.dic = French - France
- it-IT.dic = Italian - Italy
- de-DE.dic = German - Germany
- es-ES.dic = Spanish - Spain

For convenience to the administrator other language dictionary files exist.

- en-AU.dic = English - Australia
- en-CA.dic = English - Canada
- en-GB.dic = English - United Kingdom
- es-MX.dic = Spanish - Mexico

These files can be used in place of the default settings by renaming.

Example.

If administrator resides in Mexico and would like the dictionary to use "es-MX.dic". Complete the following steps:

1. Create backup copy of Spanish file. Rename es-ES.dic to es-ES.bak
2. Create backup copy of Mexico file. Make a backup copy of es-MX.dic to es-MX.bak

3 Rename es-MX.dic to "es-ES.dic".

This will allow capability to restore back to original setup.

Setting Up SSL for IMail Web Messaging

IMail Server and Web Messaging use the Microsoft Internet Information Services (IIS) Secure Sockets Layer (SSL) features to encrypt communications between the IMail Web client and server. To learn more about using SSL with IIS, see the IIS help information at *http://localhost/iisHelp/* (http://localhost/iisHelp/).

Index

A

About 1, 53, 90, 186, 256, 263, 351, 375, 376, 411, 430
About Domain Aliases 186
About Group Aliases 186
About Help 1
About LDAP Data 376
About LDAP Server 375
About Logging 411
About Program Alias 188
About Standard Aliases 186
About Virtual Mail Domains (Hosts) 53
About Your Spam Signature 263
Access 18, 359, 364, 409, 451, 456
  Default User Settings 98
  Web & Account Access - Global 137
Access and Login to IMail Web Messaging Client 451
Access Control 385, 400, 412
Accessing Spell Check Dictionary 456
Accessing the IMail Web Administration .. 18
Account Settings 143
Accounts, Orphan 140
Activating 19
Active Directory (AD) 52, 65
  Example, AD Builtin 52
ActiveSync78, See Mobile Synchronization
ActiveSync Domain Level Checkbox 149
ActiveSync -User Level Checkbox 149
Add / Edit Auto Responder Account 160
Add / Edit E-mail Alias 185
Add / Edit Sys Log Access Control List .. 413
Add Auto Responder Sub-Mailbox Responses 161
Add Collaboration User 354
Add User to Collaboration 147
Add/Edit DNS Black List 92, 273
Add/Edit POP3 Control Access 386
Add/Edit SMTP Access Control 400
Addalias Text File Example 191, 419
Addalias.exe Utility 188, 189, 190, 420
Adddomain.exe Utility 121
Adding 47, 190, 201
Adding a New Collaboration Group 356
Adding a New Contact to a Group 364
Adding a New IMail Domain 47
Adding a New Word to the antispam-table.txt File 337
Adding a Rule Condition 156, 206, 225
Adding a Subscriber by Forwarding 213
Adding a Virtual Host (adddomain.exe) . 121, 421
Adding Alias to a Domain Using 189, 419
Adding Alias to Primary Domain Using .. 189, 419
Adding Aliases using 188, 417
Adding an IMail User 143
Adding Attachment Blocking types 229
Adding Multiple Conditions for Domains . 226
Adding Multiple Conditions for Users 157
Adding Relay Addresses 398
Adding Rule for Domains 223
Adding Rule for Lists 204
Adding Rule for Users 154
Adding to Black List 277, 316
Adding to Domain Forwarding 405
Adding Users (adduser.exe) 422
Adding Users to a List 201
Additional Resources 19
adduser.exe Options 424
Adduser.exe Utility 422, 424
Administration 5, 6, 18, 124, 183
Administrators 109, 110, 216
Alert Administrator Email 255
Alias Administration 183
Aliases 183
  Addalias.exe Utility 188, 189, 190, 420
  Beeper, Alias 183, 185
  Domain, Alias 186
  Example, Setting Up Alias 30
  Group, Alias 185, 186
  Pager, Alias 185
  Program Alias 183, 185, 188
  Standard, Alias 185, 186, 187
Allow Access to Users and Groups 359
Allow remote mail to local groups 187
Antispam 259, 262, 267, 319
  Broken MIME Headers 301, 302
  Connection Checks 89, 274, 277
  Example, AntiSpam Table 430

Forwarding SPAM 266, 267
HTML Filtering..... 291, 292
Log Messages, Antispam..... 317, 319
Connect Filtering, Log Messages 319
Content Filtering, Log Messages . 326
Mailing Lists and Newsletters, Spam . 239
Phrase Filtering.....288, 289, 290
Premium Filter.....283
SPF 182, 261, 303, 304, 305, 313
Statistical Filter.....283, 284
URL Domain Black List.....299, 300
X-Header, Spam 297, 330
Antispam Configuration Overview.....262
Antispam FAQs.....267
Antispam Log Messages.....319
Antispam Logging 317
Antispam Overview 259
Antispamseeder Parameters 335
Antispamseeder Utility 333
antispamseeder.exe Utility.....333, 334, 337, 338, 339, 343, 346, 430
Antispamseeder.exe Wildcard Example 1 431
Antispamseeder.exe Wildcard Example 2 430
Antivirus 252, 254, 255, 256
Anti-virus 249
Anti-Virus
Antivirus 252, 254, 255, 256
BitDefender 249, 251, 252
Standard Anti-Virus (BitDefender) ... See BitDefender
Anti-Virus Administration (Symantec) 254
Archiving 73
Attachment Blocking 227
Attachments 25, 41, 242
Attachment Blocking 227, 229
Auto Responder 158
Auto Responder Variables.....162
Automated Response 158
Auto-Refresh Frequency.....455

B

Back Up IMail Registry.....105, 431
Backing Up IMail Server System Files...107, 433
Backing Up User Mail.....107, 434
Backups 105, 107
Restoring IMail Registry.....106
Bayesian Filter 283
Beeper, Alias.....183, 185
Beginning Character of Files in Queue.....97
Beginning Character of Files in the Spool 97

BitDefender 249, 251, 252
Black Lists 89, 90, 91, 92, 277
Blocking Message 230
Bouncing Spam Messages using Rules... 55
Broken MIME Headers 301, 302
Browser 5
  Cookies 451, 453

C

Calendars, Adding 359, 364
Certificate, SSL
  SSL Keys..... 32, 443
  SSL Setup . 373, 382, 392, 407, 410, 457
Change Password 125, 126
Changing Default Directory 455
Changing the IP Address of a Host..... 60
Changing the Web Client Default Directory (setting a redirect for Web Messaging)455
Changing the Word Count for a Word (Example) 348
Characteristics..... 232, 235
Check Registry - regcheck.exe 440
Checking the Registry (regcheck.exe) ... 440
Cleaning the Spool - Isplcln.exe..... 96
Cleaning the Spool Directory (Isplcln.exe) 96, 436
Collaboration 353, 365
  Groups, Collaboration 356, 357, 364
  Public Calendar..... 359, 364
  Public Contacts, Collaboration.. 359, 364
  Users, Collaboration..... 147, 353, 354
Collaboration Settings 365
Collaboration User Account Details 354
Collaboration User Folders and Access. 354
Collaboration Users..... 353
Command Line Installations (Silent Installs) 445
Command Line Utilities ... 96, 121, 141, 143, 188, 333, 381, 382, 417, 422, 440, 443, 445
  Backups..... 105, 107
Commtouch 371
Commtouch Premium Filter (Only Premium Versions)..... 280
Condition and Quantifier Syntax 234
Conditions 156, 218, 226
Config_CommonAddrBook.cgi..... 445
Configuring
  Configuring Antispam.....262
  Configuring Inbound. 153, 202, 219, 220, 230, 232
  Configuring Outbound 41, 219, 222, 230, 232
  Configuring Services.....367
Configuring an NT/AD database 52, 119
Configuring IMail Services 369
Configuring Sender Policy Framework (SPF) 304
Configuring Web Messaging Email List Auto-Refresh Frequency 455
Connect Filtering Log Messages 320
Connect Filtering, Log Messages 319
Connection Checks.....89, 274, 277, 313
Contacts, Adding.....445, 451
Content Filtering.... 182, 284, 288, 289, 291, 292, 303
Content Filtering Log Messages 326
Content Filtering, Log Messages 326
Control Access 385, 400, 412
Cookies 451, 453
CRAM-MD5.....392
Creating.....187
Creating a rule to filter messages listed in a black list.....278
Creating a URL Domain Black List .299, 344
Creating an Account.....143, 160, 422
Creating and Managing Lists 196
Creating Config_CommonAddrBook.cgi.445
Creating External User Database for a Mail Domain 68, 117
Creating Peer List 244
Creating Public Mailboxes 374
Creating Separate antispam-table.txt Files for Multiple E-mail Domains 340
Creating URL Domain Black List and Antispam-Table.txt Files.....346
Creating URL Domain Black List with antispamseeder.exe 344
Creating User Database 65
Customizing an E-Mail Domain's antispam-table.txt File 342
Customizing the Full Mailbox Notification Message 71

D

Daily Count Report.....390

Database 41, 65, 68
Database 41, 68
IMail Database 68, 422
NT Database31, 41, 52, 65, 66, 120, 420
Deceptive Text 296
Deceptive URLs 295
Default Subject Values for SPF..... 313
Default User Settings 98
Default X-Headers for Premium Filter Classifications..... 283
Deleting 120, 141, 148, 190, 338
Deleting Messages by Date 141
immsgexp.exe - Deleting Old Messages 141
Deleting a Collaboration Group..... 357
Deleting an Alias using..... 190, 419
Deleting an IMail Domain 120
Deleting an IMail User 148
Deleting an IMail User from Aliases/Lists148
Deleting Messages by Date 141
Deleting Messages by Date for User 152
Deleting Old Messages (immsgexp.exe) 141, 436
Deleting Words from Antispam-table.txt. 338
Delivery Rules153, 206, 218, 219, 220, 222, 236, 240
Deny Access ... 26, 208, 382, 385, 392, 400, 401, 412
Determining Which Rule Trapped a Message 240
Dictionary 456
Dictionary Attack Settings 392
Digest 192, 209, 210
Digest Scheduling 210
Directory 96
Disk Space, Monitoring 98, 148, 375
DKIM / DomainKeys..... 82, 83, 164, 171
DNS Black Lists..... 89, 90, 91, 92, 277
DNS Black Lists (Server Level)..... 89, 272
Do I need to alter the word tables in the antispam-table.txt file?..... 348
Domain 41, 54
Alias Administration..... 183
Attachment Blocking 227, 229
Domain Management... 47, 61, 110, 121, 182
Domain, Alias..... 186
Inbound Rules.....153, 202, 220
List Administrator 143, 201, 216
Outbound Rules.....222
Peering List.....244, 245, 246
Spam Filtering, Domain Level.....182
User Administration.....124, 126, 150
White List Administration 242
Domain (Host) Administrator.....110
Domain Administration.....109
Domain Administrator.....143
Default User Settings.....98
Domain Default User Settings.....130
Domain Default Web Preferences 132
Domain Forwarding.....404
Domain Properties 41, 111
Domain Selector Add / Edit.....165
Domain Selector List (Signatures) 164
Domain User Changes.....137
DomainKey Relay For Addresses Note ..399
DomainKey Result - Invalid DNS Selector 175
DomainKey Result - Invalid Signature 173
DomainKey Result - No Signature.....173
DomainKey Result - Pass.....177
DomainKey Result - Verification Failed ..176
DomainKeys / DKIM... 82, 83, 162, 164, 171
DomainKeys / DKIM Verification Settings 171
DomainKeys / DKIM Wizard 179
DomainKeys Default Subject Values 178
DomainKeys Result - DNS Unreachable 174
Domains.....110

E

Editing Domain Forwarding.....406
Editing Relay Address.....399
Email 26, 143
Embedded Comment.....296
Enable Content Filtering 303
Enabling Symantec Anti-virus Logging ...255
Enabling Web Client Logging.....415
Ensuring Delivery of Lists and Newsletters 344
Ensuring Mailing List and Newsletter Delivery.....344
Error Codes in the SMTP Log.....256
Example - Non-Spam Word Counts.....343

Example - Spam Word Counts 343
Example - Total Number Signatures / Message 178
Example 4 for Entering Inbound Rules in the Rules.ima file 238
Example for Entering Inbound Rules in the Rules.ima file 238
Example for Entering Outbound Rules in the Orules.ima file 239
Example for Entering Rules in the Rules.ima File 236, 238
Example HTML Feature Configuration... 297
Example of Active Directory 52, 120
Example of Peering 246
Example Text File (Adduser.exe) 425
Example, Install Log 38
Examples
  Example, AD Builtin 52
  Example, AntiSpam Table 430
  Example, Full Mailbox Notify 71
  Example, Install Log 38
  Example, Peering 246
  Example, Setting Up Alias 30
  Example, X-Header 297, 298, 330
  Examples, HTML Filtering 297, 298
  Examples, Rules 226, 231, 236, 238, 239, 240, 278
  Examples, URL Domain Black List .. 300, 301
Examples of Delivery Rules 236
Exclude List (definition) 288
Existing System Selectors 170
Exporting Domain Users to File 140
Exporting Users to File 136, 140
External Text File Example 231

F

False Positive Example 283
False Positives 239, 263, 283, 284, 349, 350
File Attachment Setting 25
File Attachment Settings 25
File Directory 151
File Extensions of Files in the Spool 96
File Extenstions 96, 97
Filtering 190, 261, 283, 288, 294, 295
Finding Orphan Mail Accounts 140
Flow of Processing 26
Folder Permissions and IIS Configuration 32
Forwarding SPAM 266, 267
Forwarding Spam Messages (Example) 267
Forwarding Spam to CommTouch 266
Full Mailbox Notification 41, 71
  Example, Full Mailbox Notify 71
Full Mailbox Notify Example 71

G

Global Properties 98
Global User Changes 137
Granting Access 366
Granting Access to a User's Personal Folders 355
Granting Access to Group 357
Granting Access to Public Folders 364
Granting to Users 143
Group
  Group, Alias 185, 186
  Groups, Collaboration 356, 357, 364

H

Hack Attempts, Denying 382, 392
Hand Held Devices ..... See Mobile Synchronization
Help 19
Helpful Definitions 25
Hosts 41, 53, 73, 110, 121, 123, 186
How Black Lists Work 91, 271
How Peering Works 246
How Rules are Stored and Processed 219
HTML Features Filter 291
HTML Filtering 291, 292
  Examples, HTML Filtering 297, 298
HTML Filtering Example of Scanning E-mail 298
HTML Online Editor 76
HTML or Plain Text Scan Example 301
HTML Scan Example 301
Hyperlinks 294

I

Identifying spam with double byte characters 336, 351
IIS
  IIS Configuration 32
  IIS Setup 19, 455
iLDAP.exe - Init & Synch LDAP DB 382

Image Tags 294
IMail Administrator Requirements 5
IMail Antispam Processing Order..... 263
IMail Antivirus powered by BitDefender - Settings 249
IMail Anti-virus powered by Symantec - Settings 252
IMail Database 68, 422
IMail Getting Started Guide Links 21
IMail Log Analyzer..... 414
IMail Processing Order..... 26
IMail User Selection 361
IMAP..... 373, 374
IMAP Settings..... 373
immsgexp.exe - Deleting Old Messages 141
Impersonation, Web Messaging..... 454
Import NT Group as Group Alias using addalias.exe..... 420
Importing NT Users 66, 136
Importing Windows NT Users 66, 138
InBound / Outbound Rules..... 218
Inbound Delivery Rules for Domains..... 220
Inbound Delivery Rules for Lists 202
Inbound Delivery Rules for Users 153
Inbound Rules 153, 202, 220
Information Manager 158, 160
Init and Synch LDAP - iLDAP.exe..... 382
Adduser.exe Utility 422, 424
Populating LDAP DB - ldaper.exe..... 381
Initializing and Synchronizing LDAP Databases (iLDAP.exe) 382, 435
Installation 22, 29, 30, 31, 32, 265, 347
Installing 29
Installing IMail Server Administrator..... 29
Installing Patches and Upgrades 22, 37
Installing SSL Keys 32
Installing Updated Antispam Files..... 265
Interaction with AntiVirus Scans..... 254, 256
Introduction to IMail Administrator..... 1
Invalid Tags..... 294
IP Address..... 47, 53, 60, 121, 123
IP Ignore List 372
IP Reputation, Commtouch ..... See Commtouch
IPhone ..... See Mobile Synchronization
isplcln.exe - Cleaning the Spool Utility..... 96

K

Kill File for a List.....208
Kill Files.....26, 208, 392, 401

L

LBW - Enable Cookies.....453
LDAP.....54, 150, 375, 377
Access Info Svcs for LDAP - Global ..137
Default User Settings.....98
LDAP Information.....150, 380
LDAP Service Settings.....377
LDAP Settings.....54, 217, 379
ldaper.exe - Populating LDAP DB.....381
List Administration.....192
List Command Syntax.....214
List Digest Subscribers 209
List Moderator 217
List Owner.....213, 216
List Owner Shortcuts for Subscribing and Unsubscribing.....213
List Subscribers.....201
List, Digest 209, 210
List, Open.....194, 195, 196
Lists.....194, 196, 201
List Administrator 143, 201, 216
Default User Settings.....98
List Moderator.....217
List Owner.....213, 216

List Rules 202, 206, 344
List, Digest 209, 210
List, Maximum Size 192
List, Open 194, 195, 196
Local List Administrator 216
Log Analyzer 414
Log Files 38, 256, 317, 411, 412
Log Manager 392, 411, 412
Log Messages, Antispam 317, 319
Setting Log Messages 89, 392
Logging 411
Logging for IMail Anti-virus powered by BitDefender 252
Logging into IMail Services 369
Login 18, 369, 451, 454
Low Bandwidth Web Client 451, 453
Low Bandwidth Web Messaging Lite 453

M

Mail Domain (Host) Configuration 41
Mail Processing 26
Mail Queue Considerations 256
mailall.exe - Mail All Utility 143
Mailbox Path 347
Mailbox Path - Antispamseeder 347
Mailing Lists 192, 194
Mailing Lists and Newsletters, Spam 239
Mailto
Hyperlink 295
Manage 110, 124
Managing Messages 375
Managing Collaboration Groups 356
Managing Lists 211
Managing Mailboxes 375
Managing Spool Manager 95
Managing the Client Disk Space Indicator 148
Maximum Size 41, 98, 143, 185, 192
List, Maximum Size 192
Max Mailbox Settings - Global 137
Merging Antispam-Table Text Files 336
Merging Antispam-table.txt files 336
Merging Antispam-table.txt Files Example 430
Message Area 236
Message Flow 26
Method 2 Example 59
Method 3 Example 60
Microsoft Exchange ActiveSync 78
Microsoft Exchange ActiveSync Users 136
Minimizing False Positives 350
Mobile Synchronization . 41, 73, 80, 98, 126, 130
Moderated Lists 194
Modify Subject for URL Domain Black List 347
Modifying the Subject for Broken MIME Headers 302
Modifying Word Counts of Existing Words 343

N

Nested Tables 293
New Contact for Public Contacts 361
New for Version 11.01 10
New Groups for Public Contacts 362
No List Message 212
Nobody Alias 187
Nolist.txt file 212
normalizing words 290
Normalizing Words 290
Notifications 252
NT Database 31, 41, 52, 65, 66, 120, 420

O

Open Lists 195
Order, Mail Processing 26
Orphan Accounts 136, 140
Outbound Delivery Rules for Domains 222
Outbound Rules 222
Overview 19, 94, 210, 218, 254, 303, 367
Overview (antispamseeder.exe) 333, 429
Overview of HTML Filtering 292
Overview of IMail Anti-virus powered by Bitdefender® 251
Overview of IMail Anti-virus powered by Symantec 254
Overview of Mail Digests 210

P

Pager 183
Pager Notification 351
Pager, Alias 185
Pager Problems 351

Password
Allow Password Change - Global 137
Change Password 126
Default User Settings 98
Password Complexity 41
Patches 19, 22, 32
Peer List 244
Peering List 244, 245, 246
Example, Peering 246
Permissions 32
Phrase Filter Options (Content Filtering) 289
Phrase Filtering 288
Phrase List 265, 267, 288, 289, 290
POP3 ..... 367, 382, 385
POP3 - Control Access 385
POP3 Settings 383
Populating LDAP DB - ldaper.exe 381
Adduser.exe Utility 422, 424
Init and Synch LDAP - iLDAP.exe 382
Server Black Lists 89
Populating the LDAP Database (ldaper.exe) 381, 438
Ports 56
Poster File for a List 207
Posters List 195, 207, 213
Posters List (Moderated Lists) 213
Poster's List (Subscribed List) 212
Premium Antispam (Commtouch) 371
Premium Anti-Virus (Symantec) ..... See Antivirus
Premium Options 182, 261, 262
Preparing Mailboxes for use with antispamseeder.exe 334
Processing Order 26
Program Alias 183, 185, 188
Public Calendar 359, 364
Public Contacts 445
Public Contacts, Collaboration .. 359, 364
Public Contacts Management 360
Public Folder Properties 358
Public Folders 358

Q

Queue ... 95, 96, 97, 256, 367, 370, 386, 387
Cleaning the Spool - Isplcln.exe 96
Queue Manager 386, 387
Queue Manager - Daily Count Report 390
Queue Manager Options 387

R

Receiving Mailing Lists and Newsletters that are identified as spam 239
Redirect Address 252, 254
Regcheck.exe - Checking the Registry ... 440
Registry 19, 31, 60, 440
Backups 105, 107
Check Registry - regcheck.exe 440
Restoring IMail Registry 106
Registry Backup 105, 431
Relaying Mail for Addresses .. 392, 397, 398, 399
Remote Administration Utility 5
Rename a User (RenameUser.exe) 428
Rename User ID 150
Rename Username 150
Reply To Addresses, Setting 136, 141
Requesting and Subscribing to List Information 214
Requesting List Information ... 195, 207, 209, 214
Resolving Incorrectly Identified E-mail 339
Restoring IMail Registry 106, 433
Restricted Post 194
RFCs 406
Rule with Multiple Conditions Example ... 226
Rules 55, 218, 220, 222
Examples, Rules 226, 231, 236, 238, 239, 240, 278
Inbound Rules 153, 202, 220
List Rules 202, 206, 344
Outbound Rules 222
Syntax, Rules 232, 234, 235, 236
Rules Syntax 232

S

Script tag 295
Searching 124, 211, 353
Searching Lists for a User 211
Self-Signed SSL Certificate - sslutility.exe 443
Self-Signed SSL Certificate(sslutility.exe) 443
Sending Mail 196, 214
mailall.exe - Mail All Utility 143
Sending Mail to a List 214
Sending Mail to All Users (mailall.exe) .. 143, 439

Sending spam to a specific folder in a user account 239
Server 18, 19, 451
Server Level Antispam Options (Black Lists) 270
Service Administration Overview 367
Services 367
Set 141
Setting Access to Web Calendaring 409
Setting Database Options 31
Setting Permissions 32
Setting Service Administration Options 370
Setting the Antispam Logging Options 319
Setting the E-Mail Domain Name (Official Host Name) 30
Setting the IP Address for a Virtual Host 123
Setting up a Dial-up Internet Connection . 57
Setting Up a Mail Gateway 61
Setting Up a Virtual Host Without an IP Address 123
Setting Up an Alias for a Host 30
Setting up an SPF record 305
Setting up IMail Server as a Backup Mail Spooler 62
Setting Up Peering 245
Setting Up SSL for IMail Web Messaging 457
Setting Up SSL for Web Calendaring 410
Setting User Properties 124, 126
Settings
  File Attachment Setting 25
  IMAP Settings 373
  Reply To Addresses, Setting 136, 141
Silent Install 445
SMTP ..... 187, 392, 400, 401, 402, 403, 406, 443, See Domain Forwarding
  CRAM-MD5 392
  SMTP Delivery Application - smtpd32.exe 443
  SMTP White List 403
SMTP Accept List 402
SMTP Accept List Examples 403
SMTP Control Access Settings 400
SMTP Delivery Application (smtp32.exe) 443
SMTP Domain Forwarding 404
SMTP Kill File 401
SMTP Kill file Examples 401
SMTP Service Options 392
SMTP White List 403
Spam Filtering (Domain Level) 182, 279
Spam Filtering, Domain Level 182
Spam X-Header Explanations 330
Spam, Preventing ..... 89, 90, 259, See Antispam
SPAM, See Antispam
  Forwarding SPAM 266, 267
Specify Corresponding Collaboration User 147
Spell Check 456
SPF 182, 261, 303, 304, 305, 313
SPF Filtering 303
SPF Result - Error 309
SPF Result - Fail 308
SPF Result - Neutral 311
SPF Result - None 311
SPF Result - Pass 312
SPF Result - Soft Fail 309
SPF Result - Temp Error 310
Spool Directory 95
  Cleaning the Spool - Isplcln.exe 96
Spool Manager 94
SSL Keys 32, 443
SSL Setup 373, 382, 392, 407, 410, 457
Standard, Alias 185, 186, 187
  Nobody Alias 187
Statistical Filter 283, 284
Statistical Filter Options (Content Filtering) 284
Statistical Filtering 283
Status, Services 367
Storing and Processing 219, 230
Storing Search Strings in an External Text (.rul) File 230
Subscriber - Mailing List 195, 196, 213
Subscriber Lists 195
Subscribing 195, 207, 209, 213, 214
Subscribing to a Digest 209
Support 19
Supported SMTP RFCs 406
Symantec's Scan Engine 254, 255
Synchronize and Initialize LDAP Utility 382
  Adduser.exe Utility 422, 424
  Populating LDAP DB - ldaper.exe 381
Synchronizing With Microsoft Exchange ActiveSync 80

Syntax Message 211
Syntax, Rules 232, 234, 235, 236
Sys Log Access Control 412
System .....73, 89, See Administration
System Admin Impersonation 454
System Administration..... 73
System Administrator 73, 109, 143
Default User Settings 98
System Default User Settings 98
System Default Web Mail Preferences .. 101
System Requirements 6
System Selector Add / Edit 85
System Selector List (Signatures)..... 83
System Settings 73
System Trailer 76
System WebMail Message..... 78

T

Table of Features 22
Testing a List 213
Testing a List-Server Mailing List 213
Text Patterns 235
The 207
Timer 62, 387, 392
Troubleshooting..... 349, 391, 440
Troubleshooting Antispam 349
Troubleshooting the Spool Directory..... 391
Types Of..... 53, 186, 194, 195, 261
Types of Antispam Filters..... 261
Types of List Server Mailing Lists 194

U

Understanding Anti-virus Entries in the Mail Queue 256
Understanding DNS Black Lists 90, 270
Understanding the antispam-table.txt file430
Unsubscribing..... 213, 214, 216
Updating Symantec Virus Definitions..... 255
Updating Virus Definitions 255
URL Domain Black List 299
URL Domain Black List Entry (Example) 300
URL Domain Black List Options.... 259, 261, 263, 265, 299
Examples, URL Domain Black List .. 300, 301
User
User Administration.....124, 126, 150
User Properties 126
User Utilities..... 66, 137, 140, 141, 150
Users, Collaboration 147, 353, 354
Users, Exporting To File 136, 140
Users, IMail 98, 124, 126, 136, 143, 150, 153, 422
User Administration.....124
User Impersonation by System Administrators.....454
User Mail Accounts 65
User Properties 126
User Utilities 66, 136, 137, 140, 141, 150
immsgexp.exe - Deleting Old Messages 141
mailall.exe - Mail All Utility 143
Public Contacts 445
Using a Text File (adduser.exe).....190, 427
Using Antispam Log Entries.....317
Using Antispamseeder.exe to identify wildcards.....346
Using Delivery Rules for a List-Server Mailing List.....206
Using ETRN to Retrieve Mail on a Dial-up Connection. 59
Using IMail Rules to Filter Spam.....220
Using IMail Web Messaging (Web Client) 451
Using Internet Information Services (IIS) Virtual Directories 19
Using the antispam-table.txt File.....347
Using the IMail Database.....68
Using the IMail Installation Log File ..38, 414
Using the Windows NT/Active Directory Database 65
Utilities
Backups 105, 107
Command Line Utilities.....96, 121, 141, 143, 188, 333, 381, 382, 422, 440, 443, 445

V

v10.5 Domain User Changes.....137
Vacation Message.....26, 70, 157, 158
Versions, IMail.....299
View 201, 202
Viewing
View Antivirus Logs.....256
Viewing Queue Manager ..... See Queue

Viewing Vacation Message Recipients 158
Viewing Anti-virus Log Files 256
Viewing Auto Responder Message Recipients 161
Viewing the Status of IMail Services 369
Viewing Vacation Message Recipients .. 158
Virtual Hosts 53, 121, 123, 219

W

Web Access 98, 126
Web & Account Access - Global 137
Web Address For Web Calendaring 410
Web Administrator and Client 3
Web Browser Support 5
Web Calendaring..... 18, 407, 409, 410
Web Calendaring (Old)..... 407
Web Calendaring Settings (Old) 407
Web Client Auto-Refresh 455
Web Messaging..... 110, 409, 451, 455
Web Site Updater (IClientUpdater.exe).. 434
Web.config settings 25, 148, 455
What is Web Messaging? 451
What should be in the phrase list? 290
White List Administration..... 242
White Lists
SMTP White List 403
White lists 242, 243
Wild Card Examples for Trusted Addresses 243
Windows NT Database... 31, 52, 65, 66, 420
Wireless..... See Mobile Synchronization
Word (defined for the antispam-table.txt file) 348
Word count 349
Word Value (definition)..... 288
Working with Individual User Accounts 70

X

X-Header Example 1 297
X-Header Example 2 298
X-Header, Spam..... 297, 330