

Message Security

Administration Guide

- [Google Message Security](#)
- [Google Message Discovery](#)

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
www.google.com

Part number: ADG_R645_95

June 6, 2012

© Copyright 2012 Google, Inc. All rights reserved.

Google, the Google logo, Google Message Filtering, Google Message Security, Google Message Discovery, Postini, the Postini logo, Postini Perimeter Manager, Postini Threat Identification Network (PTIN), Postini Industry Heuristics, and PREEMPT are trademarks, registered trademarks, or service marks of Google, Inc. All other trademarks are the property of their respective owners.

Use of any Google solution is governed by the license agreement included in your original contract. Any intellectual property rights relating to the Google services are and shall remain the exclusive property of Google, Inc. and/or its subsidiaries ("Google"). You may not attempt to decipher, decompile, or develop source code for any Google product or service offering, or knowingly allow others to do so.

Google documentation may not be sold, resold, licensed or sublicensed and may not be transferred without the prior written consent of Google. Your right to copy this manual is limited by copyright law. Making copies, adaptations, or compilation works, without prior written authorization of Google, is prohibited by law and constitutes a punishable violation of the law. No part of this manual may be reproduced in whole or in part without the express written consent of Google. Copyright © by Google, Inc.

Postini, Inc. provides this publication "as is" without warranty of any either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Postini, Inc. may revise this publication from time to time without notice. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

GD Graphics Copyright Notice:

Google uses GD graphics.

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000 Philip Warner.

Portions relating to PNG copyright 1999, 2000 Greg Roelofs.

Portions relating to libtiff copyright 1999, 2000 John Ellson (ellson@lucent.com).

Portions relating to JPEG copyright 2000, Doug Becker and copyright (C) 1994-1998, Thomas G. Lane.

This software is based in part on the work of the Independent JPEG Group.

Portions relating to WBMP copyright 2000 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd 1.8.4, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

Google Compliance Policies Notice:

Google assumes no responsibility in connection with the Compliance Policies lexicon-filtering feature, including any failure to recognize credit card or social security numbers that do not follow an applicable pattern as established in Postini's systems or any failure to encrypt a credit card or social security number.

Contents

About This Guide 15

Welcome to the Administration Guide	15
Related Documentation	16
Additional Documentation for the Email Security Service	16
Documentation for Related Products	18
Support Resources	18
Knowledge Base	18
Training	19
Community	19
Support Tools	19
Support Contact Information	19
How to Send Comments About This Guide	19

Chapter 1: Getting Started 21

Welcome to the message security service	21
Activation Summary	21
What Does Activation Give Me?	22
Best Practices Roadmap	22
Deployment Phases and Rollout	27

Chapter 2: How Email Security Works 29

Email Security Overview	29
Product Bundles	30
Features and Capabilities	31
Service Architecture	34
Real-Time / Reliable Spam Detection	35
Timely Configuration Changes	36
Message Processing Order	36
User Validation	42
Outbound Architecture Overview	44
Data Center Backup / Redundancy	44
Data Center Synchronization and Switchover	45
Notifications About Continuation Events	45
Secondary Data Center: Feature Summary	46

Chapter 3: The Administration Console 49

- About the Administration Console 49
- Administration Console Security 49
- Logging In 49
- Administrator Passwords 50
- Using Home Page 52
- Navigating the Administration Console 57
 - Navigating the Organization Hierarchy 57
- Troubleshooting the Administration Console 59

Chapter 4: Organization Hierarchy & Design 61

- About the Organization Hierarchy 61
- Hierarchy Requirements & Configurations 63
- Plan Your Organization Hierarchy 68
- What Settings Are Made Where 73

Chapter 5: Organization Management 81

- About Organization Management 81
- View Your Organizations 81
- Manage Organization Settings 86
- Create an Organization 91
- Find an Organization 92
- Set an Organization's Message Limits 93
- Organization General Settings 94
- Handle Mail to Unrecognized Addresses 98
 - When users are passed through without filtering 100
- Move an Organization 100
- Download Organization Settings 101
- Delete an Organization 102
- Troubleshoot Organizations 102

Chapter 6: Users and Quarantines 103

- About Users and Quarantines 103
- Set and View User Limits, Enable Alerts 103
- View All Your Users 107
- Search for Users 111
- Manage Default User Templates 114
- Add / Delete / Move Users 120
- Add Users Automatically to an Org 126
- Enable Web Autocreate 128
- Add Users Automatically (Automatic Account Creation) 129
- Manage a User's Settings 131
- Manage Quarantined Messages 135
- Manage User Aliases 140
- User General Settings 142
- Set User Password Policies 144
- Reset a User's Password 145
 - User Password Page 146
- Protect Your Mailing and Distribution Lists 147

Suspend a User	148
Reset a User	149
Download Users and Settings	150
Troubleshoot Users	152
Health Check: Update User Settings	154
Chapter 7: Administrators	157
About Administrators and Authorization	157
Administrators and the Organization Hierarchy	157
Limiting Authority	158
Create Administrators and Manage Authorization Records	162
Types of Administrators	166
Descriptions of Privileges	198
Troubleshooting Authorization	204
Chapter 8: Directory Sync	205
About Directory Sync	205
Features and Capabilities	206
Requirements	206
Directory Sync Concepts	208
Special Users	210
Special users that might be unintentionally deleted	210
Special users that might be unintentionally added	211
Planning Directory Synchronization	211
Configuring Your Directory Server	215
Setting Up Directory Sync	215
Directory Sync Settings	216
Operation Limits	220
Advanced Filtering	221
Synchronizing	223
Validation	224
Commit Changes	225
Viewing Current Settings	226
Enable Automatic Synchronization	227
Reporting	228
Synchronization Authorization	228
Troubleshooting Directory Sync	229
Chapter 9: Domains	233
About Domains	233
View Your Domains	234
Add a Domain for Filtering	236
Changing MX Records for a Domain	238
Domains with the Same User List	238
Add a Domain Alias	239
Subdomain Stripping	240
Add a Catchall Account (Legacy Feature)	241
How Domain Settings Interact	242
Edit a Domain	243
Move a Domain	243

Delete a Domain 244

Chapter 10: The Message Center 247

About the Message Center 247
 Message Center: Features Overview 248
Message Center and Message Center Classic 250
 Switching to Message Center 251
Enable / Disable Message Center Access 252
 Where User Access Is Configured 253
Control What Users Can View and Modify 255
Prevent Users from Opening Quarantined Messages 261
The Message Center & Notifications 262
Log In To The Message Center 264
Set Message Center Passwords 265
Message Center Language Settings 266
Message Center Security 266
Brand Your Message Center 267
Message Center Documentation and Help 270
Troubleshoot the Message Center 270

Chapter 11: Quarantine Summary & Notifications 273

About Notifications 273
Configuring Notifications for an Organization 273
User Settings for Notifications 279
Disabling and Redirecting Notifications 280
About Quarantine Summary 282
Configuring the Quarantine Summary 284
Customizing the Quarantine Summary 286
Quarantine Summary & Message Center Localization 288
 Setting Languages Using Batch commands 289
Troubleshooting: User Notifications 290

Chapter 12: Spam Filters 293

About Spam Filters 293
Configure Spam Settings for an Organization 297
Enable and Adjust Spam Filters 301
Fine-Tune Spam Filters 303
Phishing Attacks 304
Botnet Attacks 304
Early Detection Filtering 304
Outbound Spam Scanning 305
Troubleshoot False Positives 306
Troubleshoot Spam that Gets Through 306
 When Spam Still Gets Through 309

Chapter 13: Virus Blocking 311

Levels of Protection 311
About Virus Blocking 314

Virus Definition File Updates	315
McAfee Virus Definition Files	316
Authentium Virus Definition Files	316
Configure Inbound Virus Blocking	316
Troubleshooting Virus Blocking	322
Health Check: Update Virus Settings	324
Chapter 14: Content Manager	329
About Content Manager	329
How Content Manager Works	333
View Content Manager Filters and Policies	337
Configure Content Manager	338
Create or Edit a Content Manager Filter	340
Set Up a Compliance Policy	345
Reorder Content Filters and Policies	347
Delete and Disable Content Filters	348
About Using Regular Expressions	349
How to Use Content Manager in a Spam Outbreak	364
Content Manager Tips and Best Practices	365
Troubleshoot Content Manager	369
Chapter 15: Approved and Blocked Sender Lists	387
About Sender Lists	387
Editing Sender Lists in the Administration Console	391
Editing Sender Lists in Message Center	393
Size Limits for Sender Lists	394
Using Batch Commands for Approved/Blocked Lists	395
Deciding Which Approved Senders to Add	396
Quarantine Redirect and Approved/Blocked Senders	397
Message Headers for Approved/Blocked Senders	397
Troubleshooting: Approved/Blocked Senders and Mailing Lists	397
Health Check: Approved Senders List Cleanup	400
Chapter 16: Attachment Manager	403
About Attachment Manager	403
Configure Attachment Manager	406
Create / Edit Attachment Manager Filters	409
Troubleshoot Attachment Manager	414
Health Check: Update Settings for Executable Attachments	415
Chapter 17: Industry Heuristics	417
About Industry Heuristics	417
Configuring Industry Heuristics	418
Chapter 18: Configuring Inbound Servers	421
About Inbound Servers	421
Creating an Email Config	422
Events	423
Troubleshooting: Inbound Servers	427
Transport Layer Security (TLS)	428

Transport Layer Security for Inbound Mail	428
Setting Up Inbound TLS	434
About Policy Enforced TLS	438
Features and Benefits	439
Requirements	439
How Policy Enforced TLS Works	440
Inbound Policy Enforced TLS Mail Flow	440
Outbound Policy Enforced TLS Mail Flow	441
Mail Between Message Security Service Customers	442
Set Up Policy Enforced TLS	442
Certificate Validation	445
Scope of Certificate Validation	445
Certificate Validation Settings	446
TLS Alerts	448

Chapter 19: Connection Manager 453

About Connection Manager	453
Automatically Blocking Attacks	453
Manual IP Block Configuration	457
Pass Throughs: Preventing Attack Blocking	459
Attack Blocking Details	460
Network Effect Protection	460
Interpreting the Connection Manager View Page	461
Connection Manager Events	462
Troubleshooting: Connection Manager	463
Health Check: Update Connection Manager Settings	463

Chapter 20: Delivery Manager 465

About Delivery Manager	465
How Delivery Manager Works	465
Interpreting the Delivery Manager View	466
Dual Delivery	468
Requirements	468
How Dual Delivery Works	468
Alerts	470
Using Dual Delivery with Gmail	471
Sample Uses	471
Dual Delivery and Split Delivery	473
Use Google Apps Gmail	473
Use Cases	473
System Requirements	474
Setup	474
Setting up Delivery Manager	475
Email Servers and Load Balancing	476
Fail over	478
Overflow	478
Verifying Email Flow	479
Delivery Manager Events	479
Delivery Manager Alerts and Event Types	480
Troubleshooting: Delivery Manager	480

Chapter 21: Spool Manager	481
About Spool Manager	481
How Spool Manager Works	481
When and How Messages are Spooled	482
Allocating Spool	483
Configuring the Spool Manager	484
Interpreting the Spool Manager View	486
Alerts and Events for Spool Manager	487
Alerts	487
Events	488
Troubleshooting: Spool Manager	488
Chapter 22: Administrator Alerts	489
About Alerts	489
Setting Up Alerts	489
Alert Descriptions	491
Chapter 23: IP Ranges and Security	495
About IP Ranges and Security	495
Setting Up Secure Mail Delivery	495
Configuring for All Domains	496
Configuring for Partial Domains	496
IP Range	498
RPF: Tools to Help Prevent Spoofing	498
Setting Up IP Lock with Batch Commands	505
Chapter 24: Configuring Outbound Servers	507
About Outbound Services	507
Outbound Concepts	508
Setting Up Outbound Filtering	511
Handling Undeliverable Bounce Messages	515
Interpreting the Outbound Overview Page	516
Outbound Services	517
Compliance Footer	518
Formatting the Compliance Footer Text	520
Transport Layer Security for Outbound Mail	521
Setting Up Outbound TLS	522
Configure TLS for Outbound Servers	524
Troubleshooting Outbound Spam Scanning	527
Troubleshooting: Outbound	529
Chapter 25: Test Tools & Mail Flow Troubleshooting	531
About Test Tools & Mail Flow Troubleshooting	531
SMTP Message Test	531
Successful Results for SMTP Test	532
Error Messages and Next Steps	534
MX Record Test	534
Successful Results for the MX Record Test	535
Error Messages and Next Steps	536
Health Check: Firewall Test	537

Run a Firewall Test	538
Successful Results for the Firewall Test	538
Error Messages and Next Steps	539
Latency Test	539
Interpret Latency Test Results	540
Traceroute Test	541
Interpret Traceroute Test Results	541
Reinjection Test	542
Successful Results for the Reinjection Test	543
Error Messages and Next Steps	543
Troubleshoot Incoming Email Delivery	544
Troubleshooting Instructions	544

Chapter 26: Reports 551

About Reports	551
View a Report	551
Inbound and Outbound Reports	553
Summary Reports	553
Traffic Reports	555
Spam Reports	560
Email Authentication Reports (SPF Check)	565
Virus Protection Reports	566
Attachment Manager Reports	569
Content Manager Reports	572
Message Encryption Reports	576
Archiving Reports	577
Quarantine Delivery Reports	579
TLS Reports	580
Troubleshooting Reports	583

Chapter 27: Message Log Search 585

About Message Log Search	585
About the Data	586
Administrative Privileges for Message Log Search	586
Run a Log Search	587
Log Search Fields	592
Common Log Search Scenarios	606
Troubleshoot Log Search	610

Chapter 28: Batch Processing and EZCommand 611

About Batch Processing	611
Batch Validation	611
Submitting Batch Commands for Processing	611
When To Use Batch	612
About EZCommand	612
Setting Up EZCommand	613
Troubleshooting: Batch	614

Chapter 29: User Authentication 615

About User Authentication	615
---------------------------	-----

PMP Authentication 615
Cross-Authentication 616
Troubleshooting: Authentication 620

Chapter 30: Configuring Single Sign On (SSO) 623

Overview 623
Requirements 623
Recommendations 624
Configure SSO 625
Troubleshooting SAML Assertion Data 630
 SAML Post Response HTML 630
 Decoded SAML Post Response 632
SSO Reference 634

Appendix A: Interpreting Header Fields 637

About Header Fields 637
Received Header Field 638
X-pstn-levels Header Field 638
 Spam Scores 639
X-pstnvirus Header Field 640
X-pstn-settings Header Field 641
 Determining Whether or Not the Message is Spam 642
 X-pstn-2strike Header Field 642
 X-pstn-xfilter Header Field 642
 X-pstn-neptune Header Fields 643
 Industry Heuristics Header Fields 643
 General Transport Heuristics Header Fields 644
X-pstn-addresses Header Field 645
X-pstn-disposition Header Field 646
X-pstn-nxpr and X-pstn-nxp Header Fields 646
Attachment Manager and Content Manager Header Fields 646
 Attachment Manager Header Fields 646
 X-CM Header 646
Analyzing Header Fields 647

Appendix B: Customizing Notifications 649

About Customizing User Notifications 649
Customizing Notifications 649
 Editing User Notifications Text 649
 Editing Text with Tokens 652
Default Notifications with Tokens 654

Appendix C: Usage Details 671

About Usage Details 671
 How are Statements Calculated? 671
Viewing Usage Details 671
Interpreting Usage Details 672

Appendix D: Configuring Intradomain Filtering 677

About Intradomain Filtering 677

About This Guide

Welcome to the Administration Guide

This guide contains detailed information for setting up and administering your email security service. It's intended for administrators of the Postini email security service, and assumes that you are familiar with administering email services for an organization.

This guide is for customers of both Postini Email Security for Enterprises and Postini Email Security for Service Providers.

For a summary of what's new in this release, see the *Release Notes*:

In this guide, you'll find information about:

- Best practices for setting up and using your email security service
- How the email security service works
- Managing user accounts and account permissions
- Setting up your organization hierarchy
- Setting up and customizing notifications to users
- Providing users with access to Message Center
- Configuring spam, virus, message attachment, and content filters
- Setting up approved and blocked senders lists
- Configuring inbound email flow, load balancing, security, disaster recovery, and alerts
- Configuring outbound email filtering, bounced-message handling, and Transport Layer Security (TLS)
- Using Directory Sync, which lets you import user account information from your directory server
- Generating usage reports

Note: This guide does not include information about using other Postini products and services. For this information, refer to the documentation for those products and services. For details, see "Related Documentation" on page 16.

Related Documentation

For additional information about your email security service and optional products, refer to the following related documentation. These documents are also available at the Postini Help Center at:

<http://www.google.com/support/appsecurity>

For more information, see "Support Resources" on page 18.

Additional Documentation for the Email Security Service

Document	Description
<i>Email Security Release Notes</i>	The latest information about new features in this release, known issues, and resolved issues. If you are a direct Postini customer, please log in to the Support Portal to view the Release Notes; otherwise, please contact your vendor.

Document	Description
<i>Email Security Quick Reference Guide</i>	One-page quick reference guide for the email security service
<i>Message Center Documentation</i>	On this page, you'll find the <i>Message Center Quick Start</i> user guide and email templates for introducing the service to your users.
<i>Message Security Activation Guide</i>	Instructions for preparing for activation of your message security service, completing the online activation form, and testing your activation.
<i>Message Security Help Center</i>	Message Security documentation in the Google help center.
<i>Directory Sync Server Edition Administration Guide</i>	Instructions for downloading, installing and running Directory Sync Server Edition, a utility that runs in your server environment and pushes user data to your email security service.
<i>Directory Sync Configuration Guide</i>	Instructions for setting up your network environment and directory server for Directory Sync Hosted Edition, an optional feature of your email security service that lets you import user account information to your email security service.
<i>Outbound Services Configuration Guide</i>	Step-by-step instructions for setting up your network environment and mail server for Outbound Services, an optional feature that allows filtering of outbound messages.
<i>Batch Reference Guide</i>	Instructions for using batch commands to programmatically perform configuration tasks, including creating, deleting, and modifying organizations, users, domains, and aliases.
<i>Authorization Reference Guide</i>	Reference for authorization settings of general types of administrators, and detailed information for each authorization privilege. It's intended for administrators familiar with administering email services for an organization.

Documentation for Related Products

These documents are available on the Postini Support Portal.

Document	Description
<i>Encryption Services Administration Guide</i>	Information about advanced TLS and encryption features for your organization's email communications.
<i>Postini Message Archiving Administration Guide</i>	Instructions for setting up and administering Message Archiving to provide long-term, immutable storage of your organization's electronic communications.
<i>Postini Message Archiving User's Guide</i>	Instructions for retrieving and exporting email messages, IM conversations, and IM file transfers from your corporate message archive.
<i>Postini Web Security & Compliance Administration Guide</i>	Instructions for administering Postini Web Security & Compliance, a web-filtering service.

Support Resources

If you are a direct Postini customer, you can access additional documentation and the following support resources and services on the Postini Support Portal:

<http://support.postini.com>

Otherwise, please contact your vendor for support.

For the current status of the message security service, and for announcements of system maintenances, see the following pages:

Postini Current Status page: <http://www.postini.com/webdocs/postinistatus>

Apps Status Dashboard: <http://www.google.com/appsstatus>

Knowledge Base

The comprehensive knowledge base contains answers to the most commonly asked questions, information about error messages, configuration tips for outbound servers, and much more.

Training

To learn more about using the email security service and best practices, you can register for free instructor-led webinars on the Postini Support Portal or view recorded self-paced training sessions.

Community

The Postini Community Forum was created to provide an environment for the exchange of ideas and information about Postini configurations, observations on the current threat environment, or the Communications Security and Compliance space at large.

<http://community.postini.com>

The forum is designed with Postini clients and partners in mind, but is accessible to anyone on the internet. Anyone can browse the forum freely, but registration is required to respond or post. The forum is moderated by Postini employees. Please see the forum Terms and Services for complete guidelines for forum use.

Support Tools

On the Postini Support Portal, you can:

- Use the Header Analyzer to determine why your email security service quarantined specific email messages or allowed them to pass through the filters
- Join mailing lists for technical talk new groups and technical tips

Support Contact Information

In you encounter a problem with your email security service, or have questions about your service, you can find the following on the Postini Support Portal:

- An online problem submission form
- Technical support phone numbers
- Marketing support contact information
- Sales representative contact information
- Billing and invoice support information

How to Send Comments About This Guide

Postini values feedback. If you have comments about this guide, please send an email message to:

postini-doc_comments@google.com

In your email message, please specify the section to which your comment applies. If you want to receive a response to your comments, ensure that you include your name and contact information.

Chapter 1

Getting Started

Welcome to the message security service

Once you have activated service for at least one of your domains, you can begin to add users, customize protection for those users, and tailor your own administrative environment.

Important: Before continuing, please make sure that you've inserted new DNS MX records for at least one domain, and run the appropriate mail flow and DNS tests, as instructed in the . Users won't begin to receive protection until their domain is directing mail flow to the service's data center, and the users themselves have been added to the service.

Activation Summary

During the Activation process, you completed the following steps:

- Created an administrator account.
- Configured one email server and one domain.
- Chose some basic spam and virus protection settings.
- Performed mail flow tests, changed your domain's DNS records to route mail through the message security service, and verified that the new records propagated successfully throughout the Internet.

What Does Activation Give Me?

Successful completion of the activation process provides you with:

- Access to the Administration Console
- An email server configured for mail flow, an account-level organization, and a user organization associated with one domain
- One administrator account, which has email filtering and virus protection. Email for all other addresses will flow through to your email server without being filtered.
- Email flowing through the message security service for one domain

Best Practices Roadmap

Following these steps ensures that you get the best performance and the most effective filtering from the message security service.

- **Review your Health Check settings.**

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration. Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust.

- **Configure additional domains to ensure that all domains are filtered by the message security service.**

If you have multiple domains, you need to add these domains to the message security service. Also, if you have multiple interchangeable domains (for example, jumboinc.com, jumboinc.corp.com, jumboinc.net) set up domain aliasing.

See “Domains” on page 233 for steps to add domains and domain aliases.

- **Lock down the firewall for each of your email servers so that spam and viruses can't circumvent the message security service.**

Some virus and spam senders specifically target mail servers using low-priority DNS MX records or by looking up a server directly using a common naming convention like *mail.yourdomain.com*. To prevent malicious sender bypassing the message security service, we highly recommend that you add *all of your domains to the service*, then configure your email servers to accept mail only from the service's data center.

See “IP Ranges and Security” on page 495 for the email security IP addresses to use when locking down your firewall.

If you have traffic routing to multiple email servers at your site, you will need to create additional server configurations.

See “Configuring Inbound Servers” on page 421 for detailed procedures on adding email servers and setting up load balancing and failover if you have multiple email servers.

- **Determine service requirements for your organization.**

Review the requirements for your organization's users and email policy, and design your organizational hierarchy. For example, decide which users should have access to the Message Center, and whether obvious spam is blackholed or quarantined. For smaller groups of users, this is a relatively simple and quick task.

See “Organization Hierarchy & Design” on page 61 for information on organizations.

- **Configure the default user settings for spam filtering, virus blocking, and the Message Center and Quarantine Summary (if available with your service package). For best practices and recommendations for your settings, click the Health Check tab in the Administration Console.**

Verify that the default user settings are appropriate (you set these up during Activation).

- “Manage Default User Templates” on page 114
- “Spam Filters” on page 293
- “Virus Blocking” on page 311
- “The Message Center” on page 247

- **Set up Message Center and Quarantine Summary notifications.**

Configure and customize the notification messages for your users. The default Welcome notification is sent immediately to new users; you can also customize this notification with more information.

The Quarantine Summary sends users a convenient daily digest of the quarantined messages, and is highly recommended.

The Message Center can also be branded and customized with your logo and layout requirements.

See “ The Message Center” on page 247 and “About Quarantine Summary” on page 282.

You can also set your users’ preferred language for the Quarantine Summary notifications and Message Center. See “Set Permissions for an Organization” on page 255 for instructions.

- **Determine your user authentication method and add users.**

You can add a small group of users as a pilot group before rolling out to your company. For information on user authentication, see “ User Authentication” on page 615.

Following are the options for adding and managing groups of users:

- Add/Move/Delete Users in the Administration Console. See “Add / Delete / Move Users” on page 120.
- Batch commands in the Administration Console
See “ Batch Processing and EZCommand” on page 611.
- Automatic Account Creation, an automated feature to add new users who receive valid mail
See “Add Users Automatically (Automatic Account Creation)” on page 129.
- Directory Sync, a feature that lets you import user data from your LDAP server. See “ Directory Sync” on page 205.

- **Add additional administrators and set permissions.**

You can create accounts for administrators and support staff, and set authorizations for different levels of access.

See “Create Administrators and Manage Authorization Records” on page 162.

- **Configure alerts to be sent to your wireless device.**

We recommend you set up alerts for Delivery Manager and Spool Manager. If your email server becomes unavailable, the message security service can send you a notification.

See “ Administrator Alerts” on page 489.

- **Set up disaster recovery through the Spool Manager.**

Spooling of email is an optional feature. For more information about your service package and options, contact your account manager or vendor.

Note: Most customers have spooling automatically set up during the activation process.

See “Spool Manager” on page 481 for the procedure.

- **Consider enabling Blatant Spam Blocking, if it is not already enabled.**

Blatant Spam Blocking, which is enabled by default for new accounts, automatically deletes most obvious junk messages. This feature can stop more than half of all spam, by detecting the most blatant spam messages, and automatically blocking or *blackholing* (deleting) them. Blatant Spam Block reduces the amount of spam you must manage and your users see in their Message Center.

See “Configure Spam Settings for an Organization” on page 297.

- **If necessary, set up Connection Manager for automatic attack blocking. Set the “Virus Outbreak” sensitivity to Very High.**

Connection Manager, which detects and blocks attacks against your email servers based on sending IP behaviors, is highly recommended for all customers. For new accounts, Connection Manager protection is turned on and set to “Normal” sensitivity against all attacks (Directory Harvest Attacks, Spam Attacks, and Email Bombs). Be sure to set Virus Outbreak sensitivity to “Very High.” (Click the Health Check tab in the Administration Console for additional recommendations and best practices.)

If you are using a mail server that issues asynchronous bounces (such as Microsoft Exchange), enable the Directory Harvest Attack feature to handle these bounces once you have set up a majority of your users.

See “Automatically Blocking Attacks” on page 453.

- **Configure inbound services.**

Set up the following inbound services for your organizations and users:

- “Approved and Blocked Sender Lists” on page 387.
 - “Content Manager” on page 329 (if available with your service package)
 - “Attachment Manager” on page 403 (if available with your service package)
 - “Industry Heuristics” on page 417 (if available with your service package)
- **Protect against Directory Harvest Attacks with Connection Manager or Non-Account Bouncing.**

There are two common methods for protecting against Directory Harvest Attacks: Non-Account Bouncing and Connection Manager. Connection Manager includes a setting called Asymmetric Bounce. These are two similar but very distinct settings on your server.

Non-Account Bouncing is an organization setting, set in your user organization. If enabled, Non-Account Bouncing rejects mail to any address not registered in Perimeter Manager.

It is important to add every address, alias and mailing list before you enable Non-Account Bouncing. Users not added will never receive outside mail.

Connection Manager is set on the email config level, as an Inbound Servers setting. It includes the ability to detect Directory Harvest Attacks. If a sender sends email to many invalid addresses in a short period of time, Connection Manager will block all mail from that sender.

Usually, Connection Manager bases this decision on SMTP error codes from your server, but some servers (including Microsoft Exchange) do not send these codes. In this case, you can enable Asymmetric Bounce. If Asymmetric Bounce is enabled, Connection Manager compares the recipient addresses on incoming email to your registered user list. If a enough recipients are not on your user list, Connection Manager blocks email from that sender.

Add your users before enabling Asynchronous Bounce. If you have not added your users, Connection Manager may block valid senders. However, unlike Non-Account Bouncing, you don't need to add every user. If you have added 90% of your users added, it is safe to enable Asynchronous Bounce.

Both Non-Account Bouncing and Connection Manager (with Asynchronous Bounce) will protect your server from the heavy load of a Directory Harvest Attack, and both require that you have added users. Non-Account Bouncing is a complete block of all unregistered accounts, while Connection Manager blocks a sender when a threat is detected.

After you have added all users, aliases and mailing lists to the message security service, and established a policy for adding new users, consider enabling Non-Account Bouncing.

Non-Account Bouncing blocks all mail send to addresses not listed in the message security service. This provides protection against directory harvest attacks, but will block all mail to addresses not registered in the message security service.

See “Manage Organization Settings” on page 86.

- **Create an emergency plan and familiarize yourself with your support options.**

You must have a plan in place to follow in the event that you experience mail flow issue:

- a. Be sure that you have set up a support contact with your provider for emergency service. If you have access to the support portal, set up a support portal account.
- b. Sign up for service update lists. Contact support for more information.
- c. Set up an internal process for the unlikely event of a service outage (for example, changing MX records and firewall settings).
- d. Be aware of the troubleshooting procedures for mail flow and filtering. For troubleshooting mail flow problems, see “ Test Tools & Mail Flow Troubleshooting” on page 531 and “ Spam Filters” on page 293.

Deployment Phases and Rollout

For the smoothest deployment possible, you should go through the following four phases:

1. Activation

This gives you access to the Administration Console, with one administrative account, one organization, and one server.

2. Pilot

Add a small group of users and possibly add additional administrators. Set up your service configuration and filters, and follow the “Best Practices Roadmap” on page 22.

In planning your deployment, we recommend you review “Plan Your Organization Hierarchy” on page 68.

3. Rollout

Add your remaining users and organizations, and set the filter configurations and access levels as required.

4. Maintenance

Ongoing support of your users and servers. This may required adjusting filter settings, managing users and domains, and adding new or configuring existing email servers.

Chapter 2

How Email Security Works

Email Security Overview

The message security service lets a company, service provider, or other organization easily provide real-time spam and virus filtering, attack blocking, and email-traffic monitoring across a user deployment of any size. Users receive comprehensive protection against unwanted and malicious email, while administrators can easily tailor service for users' needs and policies.

The service blocks a wide range of email attacks at the connection level, filters spam and viruses, and can approve, block, or divert messages based on sender address or domain, origin IP address, attachment size or file type, text content, and more. It does this without requiring you to install additional software or hardware. Instead, users' incoming email is processed at our highly secure and reliable data center *before* reaching your server. Within milliseconds, spam and viruses are separated from legitimate messages. Legitimate messages are delivered to recipients without delay, while suspicious messages are deleted, or sent to a Quarantine where you have the option to review or deliver them to the user.

Administrators can arrange users into groups to easily tailor their service while still maintaining control across an entire deployment. They can also give users varying degrees of control over managing their own service. The service includes a number of tools for administrators to monitor, secure, and regulate server connections and email delivery.

Product Bundles

Different versions and service levels are available. Some service capabilities described in this administration guide are available only for certain versions. Other features are optional add-on features that can be purchased separately. The table below shows which capabilities are available with your product bundle. For more information about product options, please contact your account manager.

Email Security Feature	Postini Service Provider Edition Google Message Filtering	Postini Enterprise Edition Google Message Security	Google Message Discovery
Spam Filtering	Yes	Yes	Yes
Virus Blocking	Yes	Yes	Yes
Message Archiving	No	No (available as optional upgrade)	Yes
Connection Manager	Yes	Yes	Yes
Delivery Manager	Yes	Yes	Yes
Reports	Yes	Yes	Yes
Message Center	Yes	Yes	Yes
Quarantine Summary	Yes	Yes	Yes
Blatant Spam Blocking	Always On	Configurable	Configurable
Directory Harvest Attack, Spam and Virus Attack protection	Always On	Configurable	Configurable
Spool Manager	Yes with Service Provider Edition. Not available with Google Message Filtering.	Yes	Yes
Attachment Manager	No	Yes	Yes
Content Manager	No	Yes	Yes
Transport-Layer Security (TLS)	No	Yes	Yes
Policy-Enforced TLS (TLS settings configured by domain)	No	Optional for Enterprise Edition Yes for Google Message Security	Yes
Industry Heuristics	No	Yes	Yes
Directory Sync	Yes	Yes	Yes

Email Security Feature	Postini Service Provider Edition Google Message Filtering	Postini Enterprise Edition Google Message Security	Google Message Discovery
Outbound Services (Attachment Manager, Content Manager, Virus Blocking, Compliance Footer)	No	Yes	Yes
Message Encryption	No	Optional	Optional
Postini Web Security & Compliance	No	Optional	Optional

Features and Capabilities

Your service provides a wide range of protection and administrative capabilities via several service components. The following topics provide an overview of these components, and are a good introduction to understanding the full power of the service. These components are described in greater detail elsewhere in this guide.

Attack Blocking and Connection Protection

Protection against email attacks, where an outbreak of harmful traffic originates from a single server, is provided by Connection Manager. This blocks a wide range of attacks, including Directory Harvest Attacks (DHA) and denial-of-service (DoS) attacks, and it protects against significant spikes in spam or virus activity. Attacks are detected and blocked in real time, at the time the offending IP address attempts to connect with your email server. When an attack or unwanted probe is detected, the source IP address is temporarily blocked, during which time all messages received from that address are bounced back to the sender. See “Connection Manager” on page 453 for more information.

Spam, Virus, and Content Filtering

Messages passing through the message security service are evaluated by several filters that can approve, block, or divert a message based on criteria you specify. These include:

- **Virus Blocking** Detected viruses can be deleted or sent to a separate *Quarantine*, depending on your preference.
- **Spam Filtering** Not only can you set a level for how aggressively to filter spam overall, but individual category filters let you filter more aggressively for sexually explicit or racially insensitive content, get-rich-quick offers, or commercial offers, depending on your organization's tolerance or policies.
- **Attachment Manager filters (optional feature)** Messages can optionally be filtered based on the size or file type of any attachments (optional feature) some service packages).
- **Content Manager filters (optional feature)** Messages can also be filtered based on key words or phrases in the message header or body (available only with some service packages).
- **Sender lists** You can allow or block messages based on the sender's email address or domain.
- **Industry Heuristics (optional feature)** Messages can be filtered specifically for users in the legal or financial industry (available only with some service packages).
- **Message limits** You can limit the number of daily messages received by a user or group of users.

See the appropriate topic in this guide for details about each of these filters.

Message Quarantine and Retrieval

Messages caught by a particular filter can be processed in any of a number of ways according to your users' preference. This is determined for a particular group of users by the filter's *disposition*. Depending on the filter (spam, virus, attachment, and so on), a variety of dispositions are available. For example, you might opt for a message to be bounced back to the sender, deleted with no return message sent, or placed in a separate *Quarantine* where you can later review it and optionally forward it to the user.

By quarantining spam, for example, an administrator and optionally users themselves can review suspected spam and retrieve messages that are actually legitimate. See "Manage Quarantined Messages" on page 135 for more information.

Scalable / Custom User Management

With the message security service, you can easily maintain common services, filter settings, and email policies across your entire user base, while also tailoring service for individual groups of users. You do this by arranging users in a hierarchy of *organizations* (or *orgs*, for short).

For example, you might apply a general policy against anyone being able to receive mp3 sound files, set everyone's spam filtering to moderately aggressive, and provide a master list of approved senders. Users in Sales, however, might want more lenient filtering, and Marketing might need to receive mp3 files after all. These users can be placed in a separate organization that inherits its configuration from a master or *parent* org, thus retaining desired common settings. Each org can then be tailored as necessary for its users, only.

Service can also be tailored, as appropriate, for individual users. For example, some users might want to add their own personal allowed and blocked senders.

See "About the Organization Hierarchy" on page 61 for more information.

Scalable Administration

Your service makes it easy to manage protection across a large user base, and also delegate specific management tasks among administrators. High-level administrators can maintain control over the entire deployment, while others can be given authority to manage specific organizations (user groups). You can also control what tasks an administrator can perform. For example, a Customer Care representative might be authorized to assist users in basic ways, say, by adding them to the service and managing their filters and sender lists. A more technical administrator might be able to perform more advanced tasks such as blocking traffic from an IP range or configuring a mail server. While a policy maker can set policies for what types of messages users can receive.

See "Create Administrators and Manage Authorization Records" on page 162 for more information.

User Access

You can optionally allow a given group of users to manage their own spam, viruses, and other filtered messages, by enabling access to the *Message Center*. Users can log in to the Message Center in any Web browser to see what messages are being filtered and why. They can also look for falsely quarantined messages and forward any legitimate messages to their own Inbox.

In addition, users can be given permissions to view or modify certain aspects of their own service at the Message Center. With the appropriate permissions, they can turn spam or virus filters on or off, set spam filter levels, manage their own sender lists, and more.

See "About the Message Center" on page 247 for more information.

Disaster Recovery

Protection against email loss if your email server goes down is provided by *Spool Manager*. Should your server become unavailable due to a crash or network connectivity problem, Spool Manager automatically *spools* incoming traffic to a backup server, where it is stored until communication with your server is re-established. When your server becomes available again, Spool Manager *unspools* the traffic back to your server so it can be delivered. See “Spool Manager” on page 481 for more information.

Note: Depending on your service package, you might need to purchase spooling separately. Contact your account manager for information.

Graphs, Reports, and Other Administrator Tools

The Administration Console provides several tools that help service administrators monitor email activity, filter effectiveness, server performance, and events such as an email attack or a server outage:

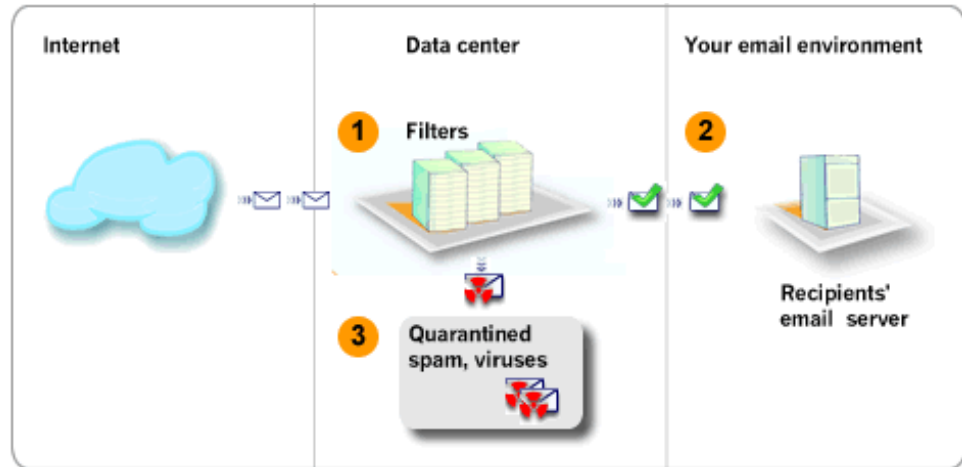
- **Graphs** The Home page and several server-related pages display a variety of real-time graphs reporting at-a-glance statistics on the number of messages recently delivered, blocked, quarantined, or spooled, recent attacks or server outages, successful and failed connections, and more.
- **Reports** You can track email activity and filter effectiveness by generating any of several reports on the Reports tab. Data in these reports includes the number of messages delivered or quarantined for a user, organization, or domain, the number of messages being forwarded from Quarantines to users' Inboxes, the number of messages caught by a particular filter (spam category, virus blocking, sender list, etc.), and more.
- **Server event tracking** Get detailed information about recent attacks, server outages, and spooling events, on an Events page. Information includes the IP source of an attack, and the time and duration of any outage or spooling.
- **Administrator alerts** Report significant events to administrators, such as a server outage or spooling, as soon as they occur, by sending automated email notifications.
- **System test tools** Quickly test and trace mail flow, test server latency, verify your MX record configuration, troubleshoot mail flow problems, and test your firewall, using a set of tools, available for each organization.

Service Architecture

Because the message security service is hosted, actual detection and filtering of suspicious mail occurs not in your email environment, but at our external *data center*. This is a robust and secure cluster of servers that sits between your users and the Internet, and is wholly managed by our personnel.

To set up service for users, you need only register your mail servers, domains, and users with the service. Then you configure their filtering and services. You can do this all from a standard Web browser, without having to install or maintain any separate hardware or software.

Once service is set up, all incoming traffic to users is filtered at the data center according to your configuration—*before* it reaches your server. Within milliseconds, heuristics-based anti-spam and virus engines separate spam and viruses from legitimate messages. Legitimate messages are delivered to users without delay, while suspicious mail is either deleted or diverted to a Quarantine where you or your users can review it.



Service architecture (1) Users' email arrives from the Internet as usual, and is filtered at the data center, before reaching your server. **(2)** Legitimate messages are delivered to users without delay. **(3)** Spam and viruses are diverted to a Quarantine.

Note: The data center accepts incoming email in SMTP format on port 25.

Real-Time / Reliable Spam Detection

Messages are filtered before they reach your email server, without being written to an intermediate disk or delayed in a queue. Instead, a pass-through spam detection engine works in-line with SMTP traffic to scan, score, and perform any resulting disposition as messages travel the public Internet.

As a result, the sender receives acknowledgement of successful delivery only after the message is indeed delivered and acknowledged by your email server. If your server becomes unavailable, the message security service returns the message "451 unable to reach the *domain name*". This 400 class error message indicates a temporary failure to the sending server, which then re-sends the message repeatedly, until either your email server comes back up and the message is delivered, or until the delivery times out. In the latter case, the sender receives notice that the delivery failed and can resend the message.

Timely Configuration Changes

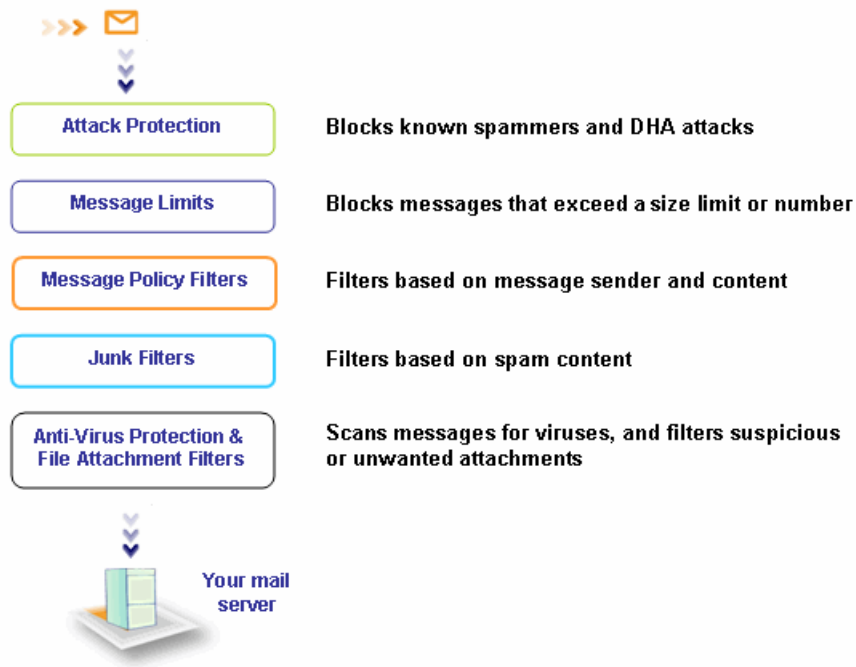
When you make a change to your service configuration, for example by adjusting a filter, the change takes effect the next time any sender's server opens a connection with your email server. Assuming that your server receives a fairly constant stream of incoming traffic, most changes can go into effect within seconds or minutes of being submitted.

Existing connections are not affected by the change. But as connections typically last only a few seconds, this causes no appreciable delay in most changes taking effect.

Message Processing Order

The order that filters and checks are applied to messages passing through the message security service ensures that no potentially harmful traffic can reach your servers, while allowing desired traffic to get through in all other cases. For example, no filter can approve an email attack or virus, but remaining traffic from approved senders can't be treated as spam.

Below is an overview of the protection and filtering provided by the message security service:



Each message processed by the service is delivered, blocked, or sent to a separate Quarantine based on a specific sequence of rules.

MESSAGE FILTER	WHEN THE FILTER IS TRIGGERED...
Attack Protection	Message is bounced
Message Limits	Message is bounced
Message Policy Filters	Message is bounced or quarantined, or allowed to skip Junk Filters
Junk Filters	Message is quarantined or deleted
Anti-Virus Protection	<p>All messages that are quarantined or pass through the filters are scanned for viruses.</p> <p>Virus-infected messages can be deleted or quarantined</p>

When you set up the message security service, you choose:

- **Which protections to turn on or off** We highly recommend that you enable attack protection, junk mail filters and virus protection (typically these services are enabled during your activation).
- **Message filters** Add message filters and message limits based on your organization's messaging policies. For example, you can create a filter that quarantines all MP3 files, or allows all messages from a trusted partner to bypass the Junk filters and go directly into your inbox (unless the message contains a virus).
- **How the filters process the message** You can set the *message disposition* for the some filters. For example, you can configure the filters to quarantine junk message, but delete all virus-infected messages.
- **Filter policies for groups of users or individual users** Some filters rules are set for user organizations, while others can be set per individual user, or you can even allow users to adjust some of their own settings. For example, you can allow users to add to their individual list of approved senders.

The next section describes in detail each filter component, the processing order, the options for message dispositions, and where to find more information on each filter.

- Enabling SPF Check (available with *Google Message Security* only) helps protect against domain spoofing of incoming emails. With this feature turned on, the message security service checks the SPF record to determine whether a message comes from an authorized mail server for that domain. Messages are accepted or rejected based on the response in the SPF record. By default, this feature is turned off. (For details and instructions about enabling SPF Check, see “RPF: Tools to Help Prevent Spoofing” on page 498).
- If the incoming message claims to be from a domain that you have specified for source IP validation, the system checks to see if the sender’s IP address matches the domain’s range of IP addresses. If it doesn’t, the email is rejected with the error `550 IP Authorization check failed - psmtp`. This blocks messages from spammers trying to “spoof” a sender address by trying to make it appear that it’s from your own domain.

For more information about Connection Manager, see “Automatically Blocking Attacks” on page 453.

2. Message size

By default, the maximum message size is 200MB; messages exceeding the maximum message size are bounced.

The message size is set per organization in Attachment Manager; see “Create / Edit Attachment Manager Filters” on page 409 for details.

3. Daily message limit

If the recipient is a registered user or alias, the system then checks to see if a daily message limit has been set for that user. If the limited has been reached, the message is bounced.

The daily message limit is set per organization in an organization’s General Settings; see “Organization General Settings” on page 94.

4. Content Manager

Content Manager scans email messages for specific content—*words*, *phrases*, or *text patterns*—and then takes an action on any messages that contain that content. You can define custom filters to deliver, bounce, or delete messages, and optionally copy them to various quarantines. For messages that you choose to deliver, you also have the option to have them bypass junk filters.

5. User Senders List

The Users Senders lists allow individual users to define lists of approved or blocked senders, based on the sender’s address or domain.

If the sender is on the user’s Approved Senders or sent to an Approve Mailing List, the message is allowed to bypass spam filtering regardless of any spam-like content.

Messages from Blocked Senders are quarantined regardless of message validity or whether the message could be considered obvious spam, which is automatically deleted by the Blatant Spam Blocking feature.

If Virus Blocking is enabled, the message, even if from an approved or blocked sender, is *always scanned* for viruses before delivery to a user's inbox. If a virus is found, then the message is either quarantined or deleted.

6. Organization Sender Lists

The Organization Sender Lists allow administrators to define lists of approved or blocked senders (based on the sender's address or domain) for a group of users. If the sender is on the organization Approved Senders or sent to an Approve Mailing List, the message is allowed to bypass spam filtering regardless of any spam-like content.

Messages from Blocked Senders are quarantined regardless of message validity or whether the messages could be considered obvious spam and automatically deleted by the Blatant Spam Blocking feature.

If Virus Blocking is enabled, the message, even if from an approved or blocked sender, is *always scanned* for viruses before delivery to a user's inbox. If a virus is found, then the message is either quarantined or deleted.

Notes:

- Organization approved senders can optionally override Attachment Manager and Content Manager filtering.
- The user sender list has precedence over the organization sender list. For example, if the sender is on an individual user's approved list and also on the organization blocked sender list, the message bypasses the spam filters, and is delivered to the user's inbox (if the message does not contain a virus).

7. Blatant Spam Blocking

Next, Blatant Spam Blocking examines the message and calculates the message's spam score. If the score is below 0.00001 (a perfectly valid message has a score of 100), the message is overwhelmingly deemed spam, and blocked. By detecting the most obvious spam, Blatant Spam Blocking can remove more than half of all spam before it reaches your email server. Neither you nor your users ever see it.

If the sender is on an applicable Approved Senders list, the message continues being processed, regardless of spam-like content.

For more information on Blatant Spam Blocking, see "About Spam Filters" on page 293.

8. Junk-Mail (Spam) Filters

Next, the message reaches the user's junk-mail filters. These include a general Bulk Email filter that sets a baseline threshold for filtering all types of junk mail, and category filters that can provide more aggressive filtering for specific types of junk mail. The message's junk-mail score is evaluated against the threshold set by each filter.

If the final threshold exceeds the junk-mail score, the message is considered junk mail, and then quarantined or otherwise processed as determined by the *spam disposition*.

If any Industry Heuristics (any optional feature) filters are enabled for the user's organization, this spam score is further adjusted to filter legal or financial content less aggressively, or to allow the message if it's from a network of trusted senders within either of these industries. This may cause a message that would otherwise be quarantined to go through.

For more information, see "About Spam Filters" on page 293, and "About Industry Heuristics" on page 417.

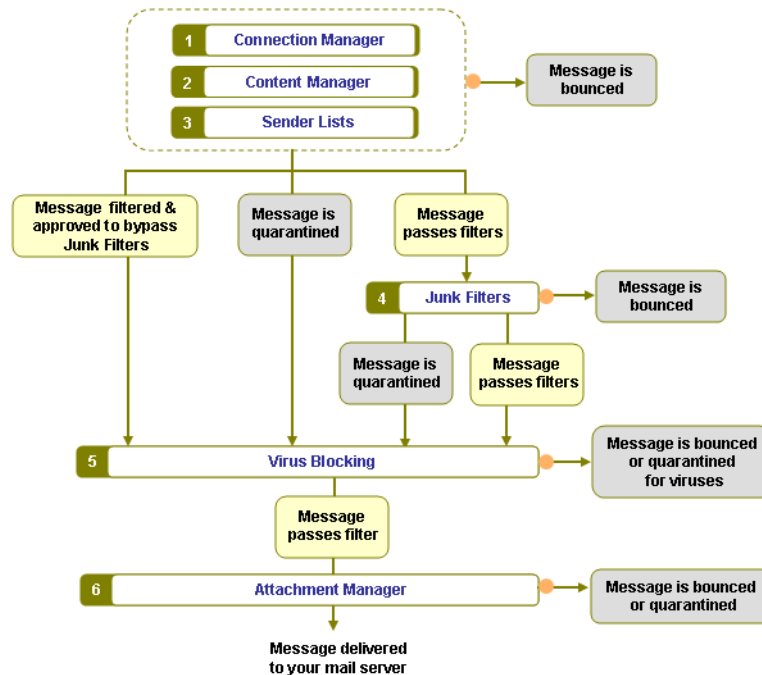
9. Virus Blocking

Virus Blocking scans the message and the message attachments for viruses. If a virus is detected, the message is deleted, quarantined, or otherwise processed, as determined by the applicable *virus disposition* (even if it's from an approved sender).

Virus Blocking checks all messages that pass through other filters or are quarantined. The diagram below shows the details of the interaction between Virus Blocking and the other filters.

10. Attachment Manager

Attachment Manager filters messages based on the size or file extension of any attachments. Each filter within Attachment Manager can have its own *disposition*, or method of processing filtered messages. Attachment filters override content filters. You can configure Attachment Manager so that approved senders bypass attachment filters.



For more information, see “About Virus Blocking” on page 314.

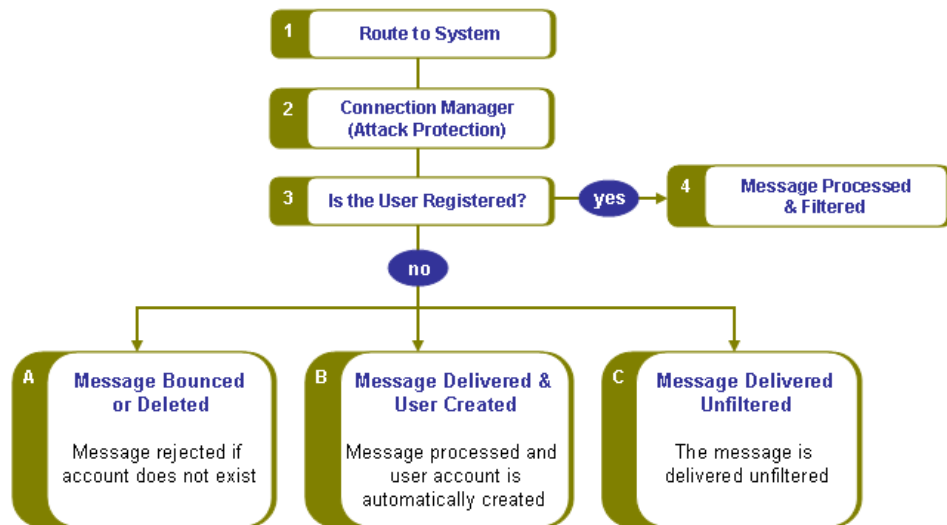
After passing through the filtering, the message is delivered to the recipient on your email server.

User Validation

A user is an email account on your mail server that’s been registered with the message security service. Once users are added to the service, their email begins to be filtered. You can associated email aliases or a mailing list address with a registered user so that mail sent to those addresses is also filtered.

This section describes user validation (how the system checks whether the message recipient is a registered user), options for processing messages for unregistered users, and methods for creating user accounts.

This diagram show how the message security service processes an incoming message:



1. Message routed to its domain’s service configuration

After being evaluated against other customer data, the message is routed to the data-center system that manages your service configuration. This is determined based on the recipient’s domain (the part of the email address that comes after the @ sign). For example, a message sent to joe@jumboinc.com is routed to the system configured to process messages for the owner of the domain jumboinc.com.

2. Connection Manager provides attack protection

If the message was sent to a domain that's registered in the message security service, Connection Manager checks to see if the sending IP is associated with malicious sender. Connection Manager also protects against directory harvest attacks where the attacker sends many SMTP "rcpt to" commands to a server in an attempt to check common user names. Connection Manager automatically blocks any messages from attackers.

3. The system checks whether the recipient is a registered user

Next, the message security service checks to see if the address is associated with a registered user or aliased to a registered user. You can also check whether the recipient is associated with a recognized user by domain sub-stripping (for example, email addresses with either the domain, **jumboinc.com** and a subdomain **sales.jumboinc.com** are recognized as registered) or a domain alias (for example, addresses to either **jumboinc.com** and **jumboinc.net** are recognized as registered).

If the recipient is a registered user, the message continues to be processed, according to that user's filters and other settings.

You have a number of options to handle messages sent to unregistered users:

a. Message is bounced

If the recipient is unregistered, and you do not want the message delivered unfiltered to your server, you can enable:

- **Non-Account Virus Blocking:** If a message that contains a virus is sent to unregistered recipient, the message is automatically deleted. This protects your domains from viruses, even if all of your users are not registered. If the messages doesn't contain a virus, it's delivered to your mail server unfiltered. For more information, see "Configure Inbound Virus Blocking" on page 316.
- **Non-Account Bouncing.** With Non-Account Bouncing, all messages sent to unregistered users are bounced. For more information, see "Handle Mail to Unrecognized Addresses" on page 98.

b. Message is processed and user created (autocreate methods).

The message security service can automatically create user accounts.

- **Automatic Account Creation:** Messages are delivered unfiltered to the recipient until the recipient receives three valid messages (contains no spam content or viruses) within two weeks. Then the user account is created, and the user's messages are filtered as normal.

For more information about this method for automatically creating user accounts, see "Add Users Automatically to an Org" on page 126.

c. Message is delivered unfiltered

You can choose to have messages sent to unregistered users delivered to the mail server without any filtering.

Outbound Architecture Overview

You can set up filtering of your outbound mail (messages sent outside of your organization) to ensure secure mail connections, enforce messaging policies and add virus protection. Following is the processing order for outbound mail flow.

Please see “Outbound Concepts” on page 508 for details on outbound services.

1. Outbound Encryption

The outbound mail service offers options for encryption with TLS (Transport Layer Security). Based on your settings, a TLS connection is attempted. See “Transport Layer Security for Outbound Mail” on page 521 for more information.

2. Outbound Virus

The outgoing message is scanned for viruses, and can be quarantined if a virus is detected.

3. Outbound Attachment Manager

Outbound Attachment Manager prevents or allows certain file types (such as MP3s or executables) to be sent out from your network.

Messages can be bounced, quarantined, or allowed to bypass Attachment Manager.

4. Outbound Content Manager

Outbound Content Manager provides administrators with the ability to filter outgoing messages based on key words and phrases found in specific areas of a message.

Messages can be bounced, quarantined, or allowed to bypass Content Manager.

5. Insert Compliance Footer

Outbound messages can be configured with a compliance footer. The compliance footer will be added to the last existing text portion it encounters. In the rare event of an empty text portion, the footer will not be added.

Data Center Backup / Redundancy

During normal operations, the message security service filters and processes your email through a cluster of servers at its *primary data center*. This facility filters messages, maintains Quarantines, and hosts Administration Console functionality. Serviced by a tier-one network provider, this data center is located in a physically secured facility with SAS70 certification, and contains multiple layers of redundancy for network connectivity and power.

In the rare event that the primary data center becomes unavailable—referred to as a *continuation event*—your traffic is automatically routed to the *secondary data center*. This center is in a geographically separate location and serviced by a different tier-one provider, making it highly unlikely that it would be affected by the same event that disabled the primary data center.

The secondary data center has the same capacity and capabilities of its primary counterpart. During a continuation event, your email traffic is directed to the secondary data center, and *there's no change to your email flow or level of protection*. However, depending on the type of continuation event, some features may be unavailable. Following are the two types of events that trigger the switchover from the primary to the secondary data center:

- **Mail flow continuation event:** The mail flow function fails over from the primary to the secondary data center. Users can access the Message Center and Administration Console, and the noticeable effect on users' experience is minimal. Most configuration settings can be changed/updated during a mail flow continuation event.
- **Full continuation event:** All functions fail over from the primary to the secondary data center. During a full continuation event, the Administration Console, Message Center, and some features are not accessible.

Please see “Secondary Data Center: Feature Summary” on page 46 for the full list of functions supported during a continuation event.

Data Center Synchronization and Switchover

To ensure that the secondary data center's configuration is up to date, its databases are synchronized with the primary data center at an interval of less than a second.

How synchronization is affected by a continuation event:

- Mail flow continuation event: Database synchronization continues as normal or slightly slower between the primary and secondary data centers.
- Full continuation event: The secondary data center uses the settings made since the last synchronization. During the continuation event, no configuration changes can be made until the primary data center is back online.

Technical details: When the secondary center is enabled, routing for the message security service's domains are switched from the primary data center load balancer to the secondary center's load balancer. Routing occurs with Border Gateway Protocol (BGP), a protocol used by large networks as a way to exchange routing information.

Notifications About Continuation Events

The service status for the message security service is available in the Apps Status Dashboard:

<http://www.google.com/appsstatus>

The dashboard offers a single location for the latest service status and options for RSS feeds so you can set up event notifications.

Secondary Data Center: Feature Summary

The secondary data center is designed to continue processing messages and delivering legitimate email to users as usual. All spam and virus filters, IP blocks and delivery mechanisms remain in effect. During a continuation event, however, some service features are not available. Below is the status of the service's features while the secondary data center is enabled:

Feature	Mail flow Continuation Event	Full Continuation Event
Incoming Legitimate Messages	Delivered.	Delivered.
Spam & Virus-infected Messages	Quarantined or blocked as usual	Quarantined or blocked as usual
Message Center	Available. There may be a slight delay in receiving quarantined messages.	Unavailable. Messages can be viewed when the primary center is enabled.
Quarantine Summary	Unavailable. Will be sent when the primary center is enabled.	Unavailable. Will be sent when the primary center is enabled.
Notifications	Only virus notifications are sent. A virus notification is sent for each virus received, even if virus notifications are set for a single notification per day. All other notifications will be sent when the primary center is enabled.	Unavailable. All notifications are sent when the primary center is enabled.
Administration Console	Administrators can use the Console, with the exception of limitations described in this table.	Unavailable. Administrator logins will return message error indicating that Web access is temporarily unavailable.
Spam filters	Active.	Active, but settings cannot be changed.
Virus blocking	Active. Virus pattern definitions continue to be checked for updates approximately once a minute.	Active, but settings cannot be changed. Virus pattern definitions continue to be checked for updates approximately once a minute.
Add/Delete/Move Users	Available.	Unavailable.
Autocreate Methods	Web Autocreate: Available Automatic Account Creation: Unavailable	Web Autocreate: Unavailable Automatic Account Creation: Unavailable
Batch & EZ commands	Available.	Unavailable.

Message Number & Size Limits	<p>Active.</p> <p>When primary center is available, message counts don't include message delivered during the continuation event.</p> <p>Note: Message Limits set to zero are ignored.</p>	<p>Active but settings cannot be changed.</p> <p>When primary center is available, message counts don't include message delivered during the continuation event.</p> <p>Note: Message Limits set to zero are ignored.</p>
Delivery Manager	Active but settings cannot be changed.	Active but settings cannot be changed.
Connection Manager	<p>Existing blocks remain active until they expire (up to one hour).</p> <p>New manual blocks can be added.</p>	<p>Existing blocks remain active until they expire (up to one hour).</p> <p>Blocks cannot be added/removed.</p>
Administrator Alerts	Traffic, Delivery Manager, and Spool Manager alerts are not sent.	Traffic, Delivery Manager, and Spool Manager alerts are not sent.
Spooling	<p>If the primary data center is spooling or unspooling while the secondary data center is enabled, spooling and unspooling is still active.</p> <p>New spooling events will not be triggered automatically, but can be triggered manually.</p>	<p>If the primary data center is spooling or while the secondary data center is enabled, spooling continues.</p> <p>New spooling is not possible, and spooling can not be stopped until the primary data center is enabled.</p> <p>Unspooling is not possible during a full continuation event. Spooled mail can be delivered when the primary data center is enabled.</p>
Directory Sync	Available.	Unavailable.
Traffic & Delivery Graphs	Unavailable. When the primary data center is enabled, graphs don't display information from when the secondary data center was enabled.	Unavailable. When the primary data center is enabled, graphs don't display information from when the secondary data center was enabled.
Reports	Reports can be generated, although updates may occur slightly less frequently.	Unavailable.
Outbound Message Filtering	Outbound messages processed as usual. No changes to outbound settings can be made.	Outbound messages processed as usual. No changes to outbound settings can be made.
Support Portal	Available.	Available.

Chapter 3

The Administration Console

About the Administration Console

The Administration Console is a secure web-based interface used to manage and configure the message security service, and administer organizations, users, and email server configurations.

This chapter provides an overview of the Administration Console, information about logging in and passwords, and a description of the Home page.

Administration Console Security

The Administration Console provides a secure web interface during the entire session. Each session maintains an audit log to ensure that each task is tracked. Both the Administration Console and Message Center use SSL to encrypt the ID and password information. All pages on the Administration Console and the Message Center are HTTPS secured.

Cookies are only used to identify and validate users. The system does not track history or session information in cookies. The only persistent cookie contains the email address of the user who last logged in to the Administration Console. All other cookies expire within 40 minutes or when the browser is exited.

Logging In

To access the Administration Console, you must have completed the activation process.

Note: If other administrators in your organization need an Administration Console account, contact support to add the administrator. For information about managing administrators, see “Administrators” on page 157.

Logging in to the Administration Console

1. Open a web browser and go to

`http://login.postini.com/exec/login`

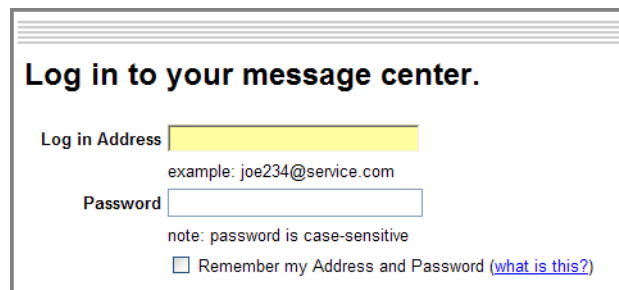
If you are a direct Postini customer, you can also go to

`http://www.postini.com/support/`

and click the Administration Console link.

2. Enter your login address and password (though the title of the page refers to accessing the Message Center, you can also access the Administration Console). You receive your login information from your vendor.

Note: If you incorrectly type your password, there is a five-second delay before the Administration Console will accept another login attempt.



Log in to your message center.

Log in Address
example: joe234@service.com

Password
note: password is case-sensitive

Remember my Address and Password ([what is this?](#))

3. If you have administration privileges, the next page has links to the Administration Console and Message Center. Click the Administration Console link.
4. You will see the Administration Console Home page. See “Using Home Page” on page 52 for information on the fields and graphs on this page. Once logged in to the Administration Console, clicking the logo in the upper left corner displays the Home page.

Administrator Passwords

You will be prompted to change your password after your first login. To prevent cracking programs from guessing your password, the message security service requires a password that is difficult to guess. Once you have set Password Policies at the organization level, administrators inherit the policies set for that org.

Your password must:

- Contain at least six characters
- Have complexity

To be complex, the password cannot include your email address and must contain at least three of the following four groups:

- lowercase
- uppercase
- numbers
- symbols

Note: For customers who signed up before May 2007, your password must:

- Contain at least six alphabetical letters
- Contain at least five unique alphabetical letters
- Not be a dictionary word
- Not be sequential letters
- Not contain an email address

Furthermore, the message security service checks for common password tricks that crackers use:

- Verifies that the password meets requirements when all numbers are removed
- Verifies that the password meets requirements when typical suffixes are removed. These include “ing”, “er”, “es” and “y”.
- Verifies that the password meets requirements when common cracker substitutions are applied. For instance, “@” and “a”, “1” and “L”.

With this criteria, many simple passwords will not be accepted. For example, “JOHN123” would be rejected because there are only four letters. Another example of an unacceptable password is “CR@CK3R”, because after substitution, the word “cracker” is a dictionary word.

Note: Users attempting to sign in with batch or API cannot use a single quote (‘), a double quote (“), a comma (,), or a backslash (\). If these characters are used in a password, and the user attempts to log in for a batch or API connection, the user will receive an error. The error text will be either:

```
Password did not meet the minimum requirements.'
```

or:

```
No such user.
```

Resetting or changing the administrative password

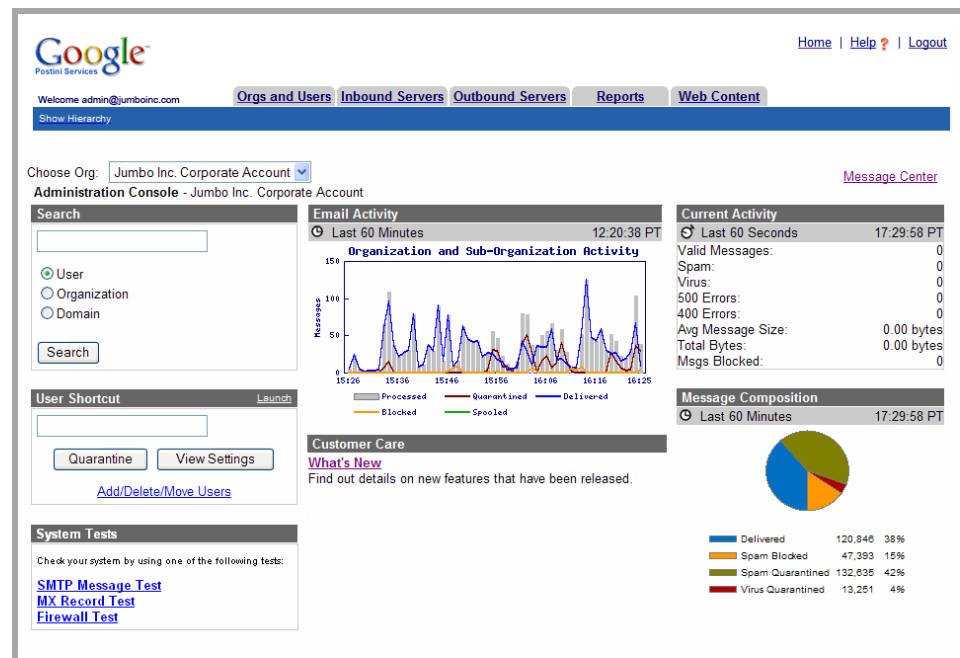
There are three ways to change or reset your password.

- In the Message Center, click the Account Settings link in the right-hand corner of the page, and then click the Set or Change your Password link. For details, see “Set Message Center Passwords” on page 265.
- If you forgot your password, enter an incorrect password in the login page. The next page has a Forgot Your Password link. Click this link and a temporary password will be emailed to you.
- If you have permissions, you can change or reset your administrator password in the Administration Console.

Using Home Page

After logging in to the Administration Console, you will see the home page. This page can be accessed at any time by clicking the logo in the upper-left corner.

A shortcut to the Message Center is provided by the link in the upper-right corner of the page. Your administrator ID (email address) appears in the left corner.

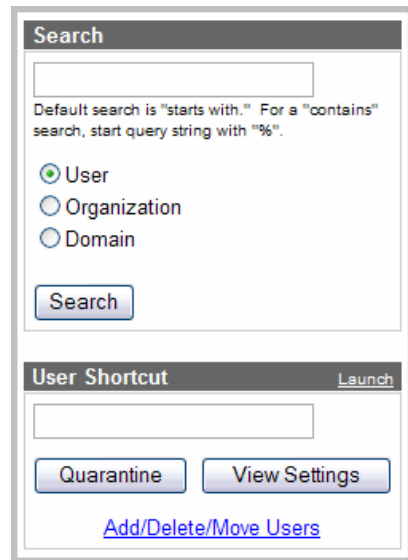


The Home page provides shortcuts to search functionality, an overview of account activity, and links to helpful information.

Search and User Shortcut

The Search and User shortcut boxes provide fast access to users, orgs, and domains. You can search using a partial name. Search results include aliases.

To quickly access a user's quarantine or view settings, enter their email address in the User Shortcut field and click the Quarantine or Settings button, or click Launch to open a floating User Shortcut window that controls your main Administration Console window.



The image shows two stacked panels. The top panel, titled "Search", contains a text input field, a help text line stating "Default search is 'starts with.'" For a 'contains' search, start query string with "%".", and three radio buttons labeled "User", "Organization", and "Domain", with "User" selected. A "Search" button is at the bottom. The bottom panel, titled "User Shortcut", has a "Launch" button in the top right, a text input field, and two buttons labeled "Quarantine" and "View Settings". A blue hyperlink "Add/Delete/Move Users" is at the bottom.

Systems Tests

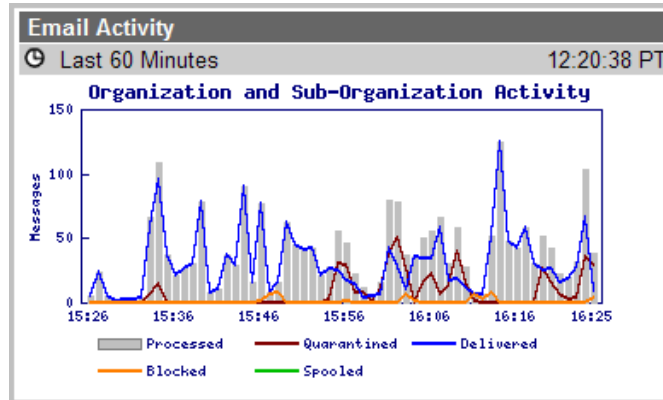
Use the System Tests to test mail flow, verify your MX record configuration or check that email traffic cannot bypass the message security service. Additional tests to trace mail flow and test server latency are available in Delivery Manager.

Refreshing Graph and Chart Information

The information displayed in graphs, charts, and boxes on the Home page is updated regularly but does not refresh automatically. Use the browser's refresh button to update the data on the Home page.

Email Activity

The Email Activity graph shows an at-a-glance summary of important email statistics from the last 60 minutes. The number of processed messages, quarantined, delivered, bounced, and spooled (if any) is displayed.



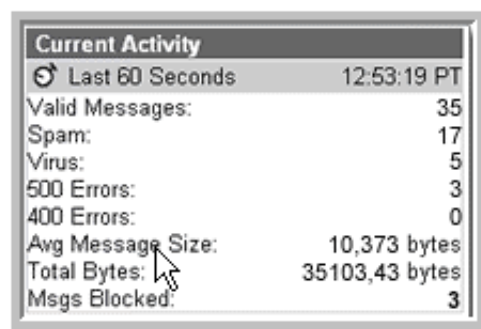
Current Activity

The Current Activity box shows activity over the last 60 seconds.

A count of valid, spam, and virus messages is displayed. The number of 500-series errors (fatal) and 400-series errors (deferred) are displayed, along with the average message size, total bytes, and number of blocked messages.

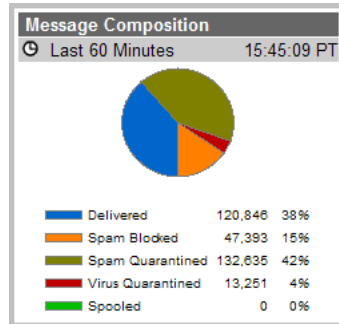
The Current Activity box shows the following information:

Activity Information	Meaning
Valid messages	Total count of valid messages that were passed on to your mail server.
Spam	Total count of messages quarantined as spam.
Viruses	Total count of messages quarantined as viruses.
500 Errors	Total count of messages rejected with 500 errors. A 500-series error is a standard email code (with an error number between 500 and 599) that indicates a mail message has been rejected. This could happen for many reasons, including Content Manager rules, invalid recipients, or blatant spam bouncing.
400 Errors	Total count of messages deferred with 400 errors. A 400-series error is a standard email code (with an error number between 400 and 499) that indicates a mail message has been deferred and that the sending server should try again later. This may happen due to a server error, special spam filtering deferrals, or a temporary error.
Avg Message Size	The average size of messages sent through the service.
Total Bytes	The total size of all message sent through the service.
Msgs Blocked	The number of messages that have been blocked or bounced by the service.



Message Composition

The Message Composition box displays a pie chart summary of the number of delivered messages, virus messages quarantined, spam quarantined, spam blocked (by Attachment Manager or Content Manager), and spooled messages. This information is a summary of the activity that has taken place over the last 60 minutes.



Customer Care

The Customer Care section of the Home page gives an update on new features and support.

Customer Care

[What's New](#)
Find out details on new features that have been released.

[Support Options](#)
This document is a description of the support services available to customers. Included are descriptions of our support portal, documentation, case submissions, online knowledge base, service levels, and emergency phone numbers.

Navigating the Administration Console

The tabs at the top of the Administration Console provide the following functions:



- **Orgs & Users:** Creating and managing your organizational hierarchy and users. See “ Organization Management” on page 81 and “ Users and Quarantines” on page 103 for more information.
- **Inbound Servers:** Information and settings for inbound email servers, and for access and protection of your mail server. See the “ Configuring Inbound Servers” chapter for more information.
- **Outbound Servers:** Information and settings for outbound email servers. Note, this is an optional feature and may not be accessible. Please contact your account manager for more information about your service package. See “ Configuring Outbound Servers” on page 507 for more information.
- **Reports:** Reports and logs for mail filtering activity. See “ Reports” on page 551 for more information.

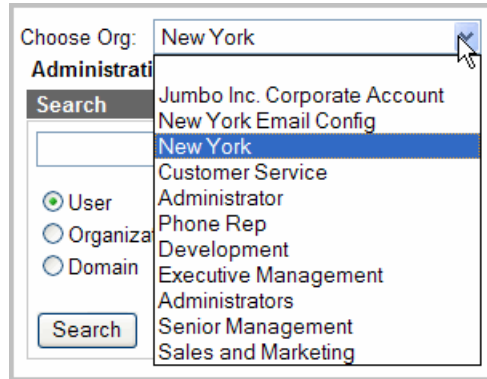
Navigating the Organization Hierarchy

Your email servers and users are grouped into an organizational hierarchy (information about organizations is described in detail in the “ Organization Hierarchy & Design” chapter). You have two ways to navigate and view your organization information and settings.

Choose Org Pull-Down List

Choose an organization or email server config from the Org Pull-down List. For example, if you chose Customer Service, you would go to the Customer Service organization settings in the Orgs & Users tab.

The pull-down list displays a maximum of 45 organizations. To navigate very large numbers of organizations, use the Show Hierarchy panel described below.

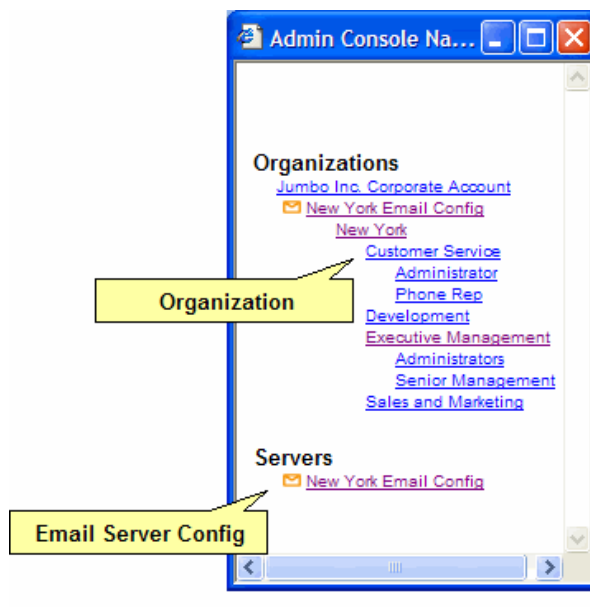


Show Hierarchy Panel

Click the Show Hierarchy link in the menu bar to display the Hierarchy panel. The Hierarchy panel helps with visualization of large numbers of organizations and email servers.

The Hierarchy panel is divided into two sections:

- **Organizations:** This reflects the organization of your account. When you click an organization, you go to pages that allow you to administer organizations, users, and component settings.
- **Servers:** This shows only your email server configurations. When you click a servers link, you go to pages to that allow you to administer email server settings, such as editing the mail hostname or blocking an IP address.



Troubleshooting the Administration Console

How do I get another administrator account for a co-worker?

You can create an administrator account by creating a new authorization record for a user. See “Create Administrators and Manage Authorization Records” on page 162 for more information.

I’m logging in to the Administration Console for the first time. The system asks me to change my password, but it is not accepting any new password I type in. Why not?

To prevent easily-cracked password, the message security service has very strict guidelines for administrative passwords. See “Administrator Passwords” on page 50.

Chapter 4

Organization Hierarchy & Design

About the Organization Hierarchy

To best manage users, you can divide them into groups called *organizations* (or *orgs*, for short). An org can be configured to give its users specific services or management control, such as a support address, email policy, or administrator. You can also create sub-organizations (or *sub-orgs*) below an org to create a finer level of control within a larger group. The resulting hierarchy is called your *organization hierarchy*.

There are three types of organizations:

- *Account organization*, which resides at the top of the hierarchy and is used for billing.
- *Email server config*, which maps to, and provides information about one of your email servers.
- *User organization*, which provides a group of users with common settings, services, and administrative control.

To view your orgs and manage their settings, see “About Organization Management” on page 81.

Account Organization

At the top of the organization hierarchy is your Account org, named “*Your_Company Account*.” The Account org is set up when your account is created and used primarily for billing.

You shouldn’t add users to the Account org (except optionally you can add a Default User, whose settings act as a template for new users but doesn’t itself send or receive mail), nor should you add domains to this org.

You can make general policy settings for the Account org, and these settings are inherited by new orgs created later. But none of your changes will be copied to existing orgs. Normally, the Account org needn’t be modified at all.

Email Config

An email server configuration (or *email config*, for short) is a special kind of organization used to manage an email server. Typically, it resides directly below the Account org in the hierarchy, although it can reside elsewhere within the hierarchy.

An email config is where you map the message security service to your email server, set up failover and load balancing, set up spooling, turn on attack blocking, and manually block or allow traffic from an IP address.

As with the Account org, you shouldn't add users or domains to an email config.

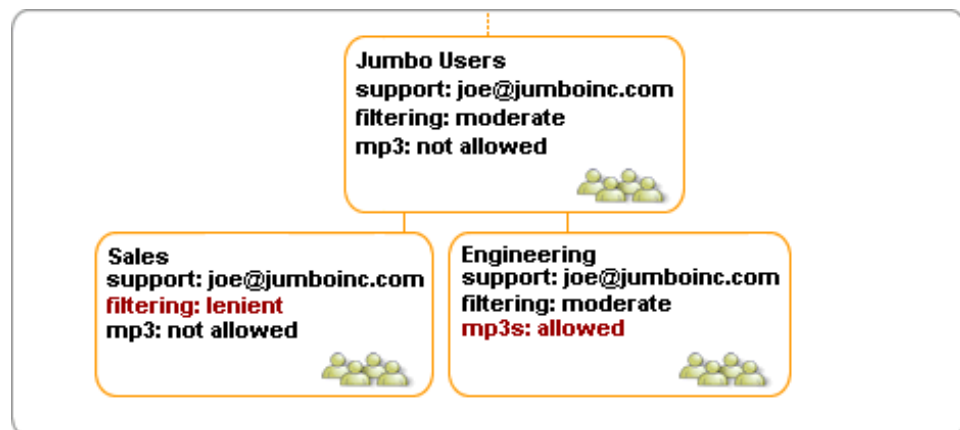
User Organization

Below an email config are one or more *user organizations*. User organizations are where you add users that should receive email protection, and also where you add their domains.

Each user org can be configured to provide its users with specific services, filter settings, administrators, and other policies. Placing users in an org applies its settings to those users. Changing a setting applies the change to the entire org. By grouping users in organizations, it's easy to manage users based on their geographical location, role in the company, service level, filtering needs, and so on.

Sub-Organization

A sub-organization, or *sub-org*, is simply an org created below another org in the hierarchy. When it's created, a sub-org gets a copy of settings from its parent, and you can then modify these settings to apply only to users in the sub-org. Creating sub-orgs allows finer levels of control among a larger group of users.



Sub-orgs Jumbo configures its top-level user org with settings common to all users. It then creates sub-orgs that get a copy of standard Jumbo settings from the parent, and that are then customized for the sub-org's users.

- A sub-org receives a copy of org-level settings from its parent, making it easy to retain common settings throughout a leg of the hierarchy.
- A sub-org can be managed by any administrators you assign to it, and also by the parent org's administrators. This is because an administrator has privileges to manage the org he or she is assigned to, and all of its sub-orgs.
- Once created, a sub-org remains otherwise independent of its parent. Changes made later to the parent's settings are not copied to its sub-orgs, unless you specifically choose for them to be.

Hierarchy Requirements & Configurations

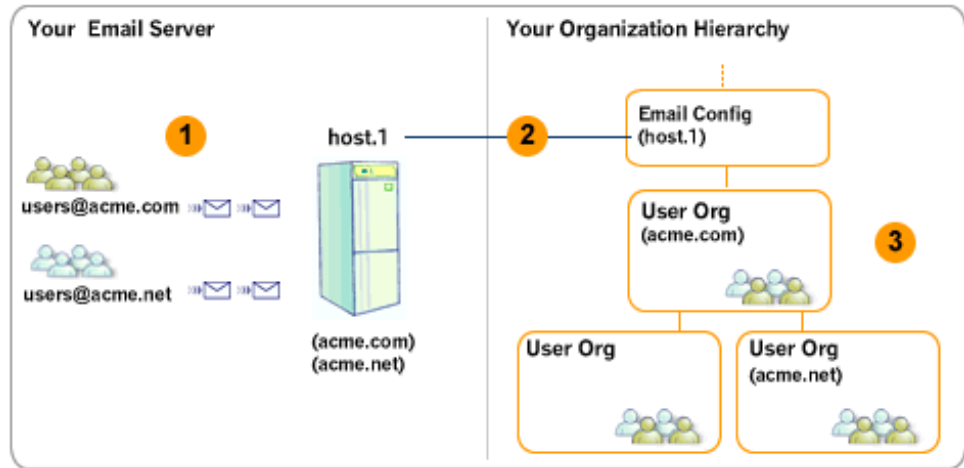
For the message security service to filter users' email, it has to know about their email server, their email address, and their domain (the part of their address that comes after the @ sign). This requires registering your servers, domains, and users with the service. You do this by associating them with organizations in your hierarchy. When doing so, you must follow a few basic requirements as described below.

Hierarchy Requirements

For users to send and receive mail via the service data center, your email server and organization hierarchy must be set up as follows:

1. In *your* email environment, users' email should be routed to the email server containing their domains. (This will be the case if your users have already been successfully sending and receiving email.)
2. Your email server must then be mapped to an *email config* in your hierarchy. An email config is a special kind of org that typically resides below your top-level Account org. You can map only one server per email config.

- Each domain on your server, and each user in the domain, must be added to a user org somewhere *below* the server's email config in the hierarchy—it doesn't matter how many levels below. You can add as many domains or as many users to an org as you want.



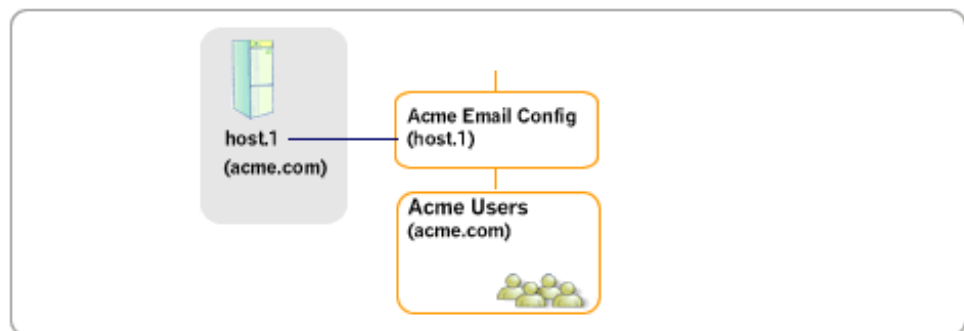
Design Requirements: (1) Route users' email to the email server that contains their domains. (2) The server must be mapped to an email config. (3) Add users and their domains anywhere below their server's email config.

Users and their domains can be distributed among organizations however you want. A user and its domain don't need to be in the same org, but both of them must reside somewhere—anywhere—below the email config mapped to their server. There are reasons for adding a domain or user to a particular organization, however, depending on the services you want to provide.

See the sections below for some common hierarchy configurations.

Basic Hierarchy: One Domain / User Org

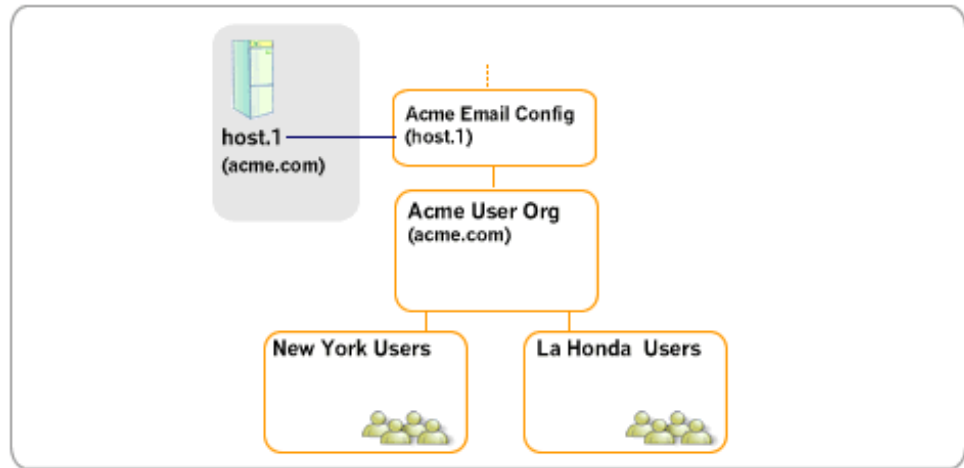
If you have only one domain, and all its users have the same filtering, services, and administrators, you can stick with the basic configuration set up when your account was created—one email config, and one user org with one associated domain. Customize the user org's settings, add your users to it, and you're done.



Basic Configuration: Acme has one domain, and all its users have the same filtering, services, and administrators. Users and their domain therefore reside in one user org.

Hierarchy with Multiple User Orgs

If some users have unique service requirements, you can create additional orgs, configure them with the unique settings, and add the users to them. Each user receives the filtering, services, and administrators defined for its organization. For example, you might separate users in your New York and La Honda offices to give each group its own administrator and support address.



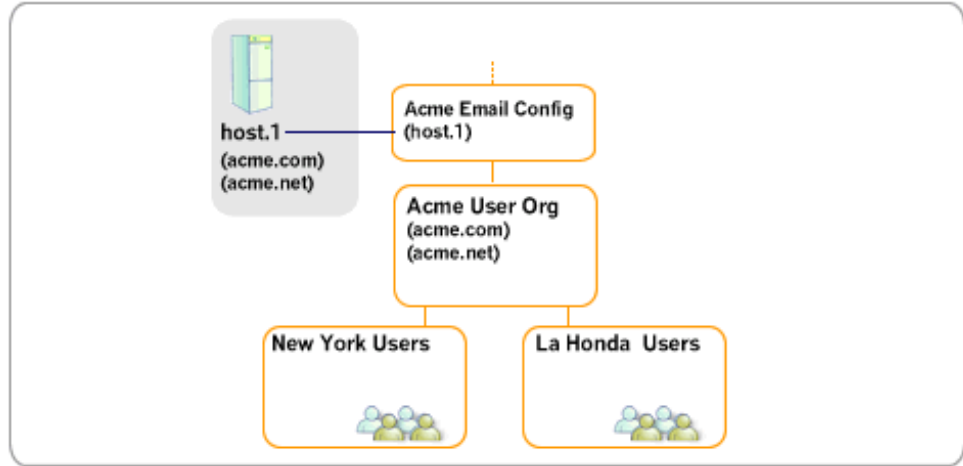
Multiple User Orgs Users in New York and La Honda need different filtering, so they're divided into sub-orgs. The users can be located anywhere below the same email config as their domain.

Create orgs directly below your email config at the same level as your initial user org, or as sub-orgs below it. Create as many orgs as you want, and as many levels deep. For guidelines on arranging users in organizations, see “Plan Your Organization Hierarchy” on page 68.

Hierarchy with Multiple Domains

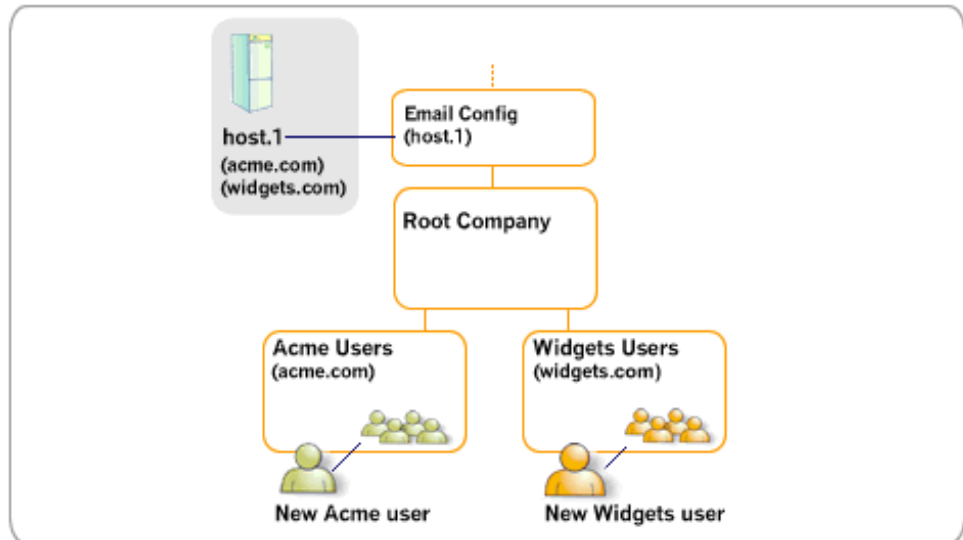
If you have other domains on your server whose users need email protection, go ahead and add those domains to your hierarchy—to any org below the server's email config. Add each domain's users somewhere below that email config, too.

If users will be distributed among several sub-orgs, you might add their domain to a parent organization.



Multiple domains, no particular org affiliation Here, *acme.com* and *acme.net* users are distributed across the New York and La Honda sub-orgs. Their domains are added to these orgs' parent.

If you want users to be added automatically to the message security service, add their domain to an organization with Automatic Account Creation enabled. Unrecognized users in the domain are then added to that org, either when they receive three legitimate messages within a two-week period (Automatic Account Creation) or when they first log in to the Message Center (Web AutoCreate).

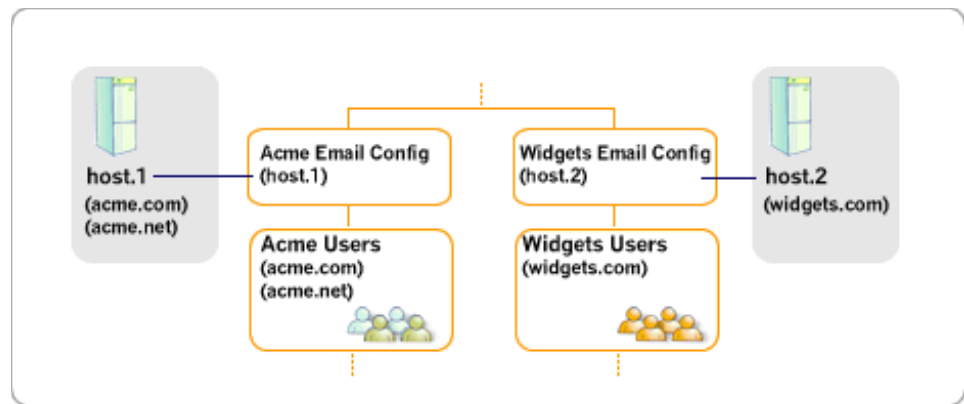


Domain placement for automatic user creation Here, *acme.com* and *widgets.com* users reside, along with their domain, in separate orgs tailored for their respective business divisions. Each org is configured so its domains' users are added to the service automatically. The placement of each domain determines which org users get added to.

If mail to unregistered addresses in a domain should instead be bounced, or delivered without filtering, add the domain to an org configured with that behavior. Add as many domains to an org as you want. Just make sure they all share the org's policies for handling mail to unrecognized addresses.

Hierarchy with Multiple Email Servers

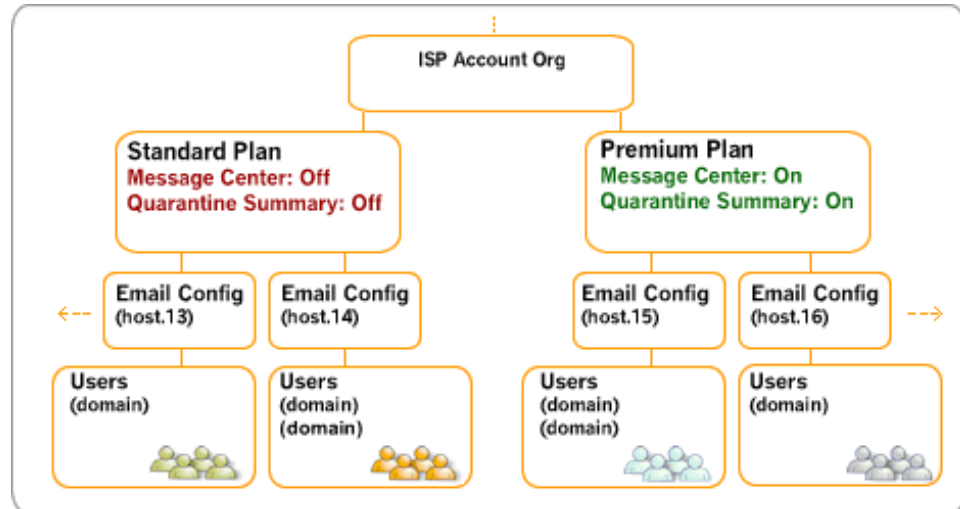
If your domains and users are spread across multiple email servers, you must create an email config for each server, and map the server to it. Then add the server's domains and users to orgs created below that email config.



Create a new leg of the hierarchy for each server Here, *widgets.com* resides on a different mail server than *acme.com* and *acme.net*. A new email config is therefore created and mapped to *host.2*. The *widgets.com* domain and users must then be added somewhere below this email config.

ISP Hierarchy

If you're an ISP that's hosting email protection for domains spread across multiple email servers, and your users sign up for a particular service plan, your hierarchy might look something like this:



Large ISP offering service plans This ISP offers two service plans. Its users are distributed across many email servers that each contain a few domains. Users are placed in a domain based on their service plan. Under each plan's org is an email config for each server whose domains are covered by the plan. A user org under each email config contains the server's domains and users.

Plan Your Organization Hierarchy

Initially, your service is set up with only one user organization. If all of your users have the same filtering, services, and administrators, configure that org accordingly and place all your users in it.

More likely, however, users will have different needs. The Sales department might want more lenient spam filtering. The New York office might have its own administrator and support address. You might want to enable the Message Center for some users, but not for others. And so on. To tailor service for groups of users, place them in separate orgs, and configure each org for those users.

You might group users by geography or domain name; by their department or role in the company; by the security services they can access or their level of filtering; according to the administrator who will manage their service; or most likely by some combination of factors. Because each new org receives a copy of settings from its parent, it's easy to maintain common settings throughout a leg of your hierarchy.

The best strategy is to decide policies for different user groups, then create orgs to support your strategy. See “What Settings Are Made Where” on page 73 to begin your implementation.

Group Users by Domain Name

If users belong to different business divisions or companies that have their own domain, and if each group requires separate services or administration, consider grouping users by domain. Then tailor each org as appropriate for the division or company.



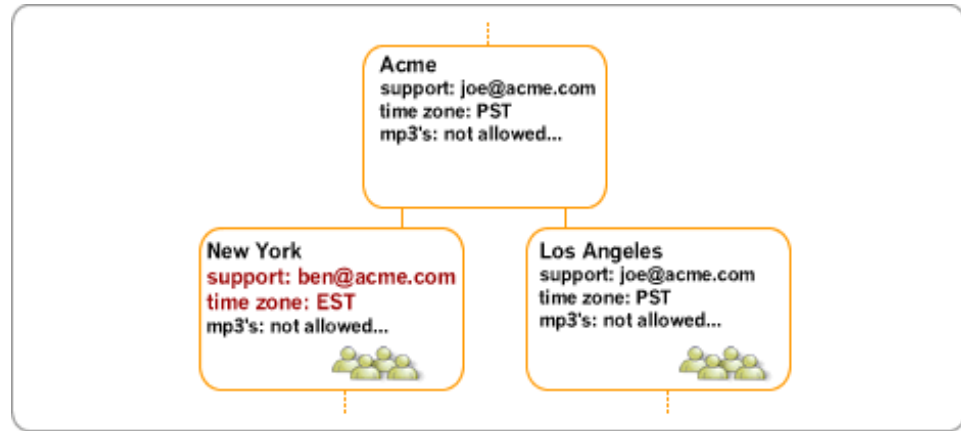
Group by domain Acme and Wilsons Widgets are separate companies whose users require independent filtering and administration. Each company's users are best identified by their domain name (the “@domain.com” part of the address), so an org is created for each domain.

Arranging users by domain is the most common org structure. You might begin your hierarchy in this way, tailoring each domain's org with settings common to all users in the domain. Then create sub-orgs below to provide a finer level of control within a domain.

Tip: If this structure works for your users, consider enabling SMTP or Web Autocreate for your orgs. These features can add a domains' users to the org automatically, making it easy to populate the message security service with new users. See “Add Users Automatically to an Org” on page 126.

Group Users by Geographical Location

If users are in different geographical locations, you might want to give each office its own time zone and support address. Create an org for each location, and tailor its settings accordingly.

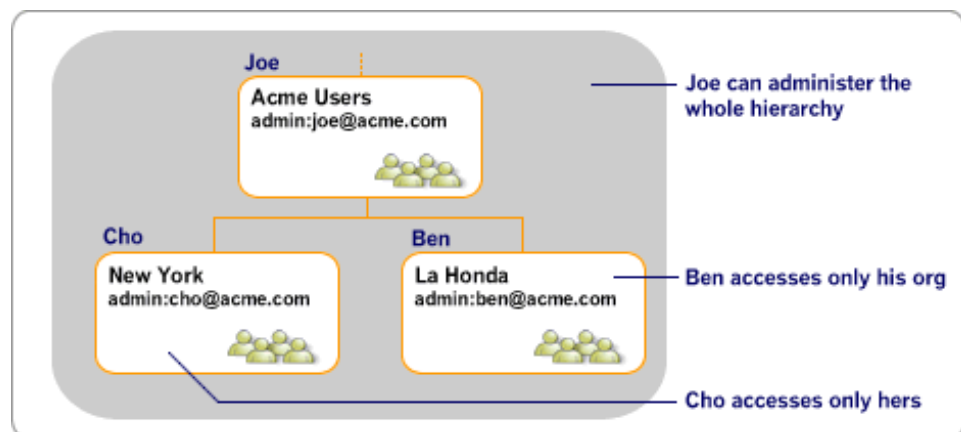


Group by geography Acme users in New York and Los Angeles initially inherit Acme's general settings from the parent org. The New York office is then assigned a local time zone and its own support address.

Create sub-orgs as necessary below each location to tailor users' service further. Each new sub-org will inherit the location-specific settings from its parent, so you don't have to make these settings again, yourself.

Distribute Administrative Control

To distribute management of user groups across several administrators, or allow individual customers to manage their own service, assign each administrator to the organization they should be able to manage. An administrator has permissions to manage his or her own org, and all sub-orgs below it.



Here, Joe is an administrator at the parent-level and can therefore administer the entire hierarchy below. Cho and Ben, however, can access only their own orgs, with no visibility into any other.

Assign Email Policies

To prevent certain groups of users from sending or receiving certain kinds of messages, or to ensure that some content gets through regardless of spam-like content, place those users in an organization configured with those specific policies. Policies you can control include:

- **Attachment Filtering** (Attachment Manager) Specifically allow or block messages containing certain types of attachments. For example, prevent most employees from sending or receiving mp3 sound files or potentially harmful executable files. But place system administrators, who need to be able to exchange all file types, in an org with no such restrictions.
- **Content Filtering** (Content Manager) Specifically allow or block messages based on their text content. For example, make sure all messages containing the word “resume” get through to the Human Resources, regardless of spam-like content.

Provide Access to Services

If some users need access to different services, enable or disable the service for those users’ organization. Such services include:

- **Message Center and Notifications:** If users should be able to manage their own quarantined spam and viruses, enable their Message Center. Also enable Notifications, which sends them an email summary of recently quarantined messages. If not, disable these features for their org.
- **Wireless Forwarding:** If users should be able to forward certain types of messages to a cell phone or other mobile device, enable Wireless Forwarding for their org. (This feature is currently available with *Message Center Classic* only. See “Control What Users Can View and Modify” on page 255.)

Customize Spam Filtering

Some users might need different spam filter levels, filtering turned off, or to manage their own filter settings.

- **Spam filtering on/off** Most users want their spam filters on. But they might want to forward spam that gets through the filters to Customer Support for further analysis. So the forwarded spam can get through, you might place Customer Support in an org with spam filters turned off.
- **Spam filter levels** Most users probably want all categories of spam filtered aggressively. Your Sales team, however, might want lenient filtering of Commercial Offers, so potential leads aren't wrongly identified as spam. You might place them in their own org with the Commercial Offers filter turned off.
- **Permission to modify filters** You might want to allow some users the ability to modify the strength of their own spam filters, or turn filtering on and off.

Set a Policy for Unrecognized Addresses

For each domain registered with the message security service, you must decide what to do with mail sent to addresses in the domain that the service doesn't recognize. Do you want to automatically add these addresses to the service as users? Bounce the messages? Or deliver them without filtering for spam or viruses?

If you have different policies for different domains, you'll need to create and configure an org for each policy. Then add each domain to the org with the appropriate behavior.

Provide a User Authentication Method

For each organization, you can choose a method for authenticating users and administrators when they log in to their Message Center (or the Administration Console, for administrators). To switch authentication methods, please contact Support.

What Settings Are Made Where

Settings that affect users and their service can be made for an email config, a user organization, a Default User, or a specific user—depending on the setting and its intended scope.

- **Email config settings** map your hierarchy to an email server and manage server-level protections.
- **Org-level settings** apply general policies or administration for all users in the org, such as a support address or policy against receiving mp3 files.
- **Default User settings** apply for new users in an org, and are how you enforce spam and virus filter settings across an org.
- **User-specific settings** apply to individual users, and include personal user aliases, and the user's password for logging in to the Message Center.
- **User-controlled settings** A few settings, such as filter levels and sender lists, can also be customized by users themselves at the Message Center, depending on the user's User Access permissions.

Some settings are available in more than one location—for example, you can define org-level sender lists, which users can augment with their own personal lists. You can also override some org-level settings for a user, such as User Access permissions to the Message Center. Once you do this, however, the user is disconnected from the org-level setting—that is, further changes to the org won't affect this user. If you have a lot of users, it's best to manage these settings at the org-level. It's a lot easier to apply a new policy once, across an entire org, rather than individually to tens or hundreds of users.

Similarly, some Default User settings shouldn't be changed for individual users, if they define policies that should remain in effect across the org.

See below for guidelines on where, or where *not*, to control each setting.

Email Config Settings

These settings are available only for orgs that are email configs (see “Creating an Email Config” on page 422):

- **Email server mapping** The host name of an email server whose domains and users should receive email protection. See “Delivery Manager” on page 465.
- **Server load-balancing, and failover** See “Delivery Manager” on page 465.
- **Attack blocking** against Directory Harvest Attacks, Spam Attacks, Virus Outbreaks, and Email Bombs. See “Automatically Blocking Attacks” on page 453.
- **IP blocking or pass-through** See “Manual IP Block Configuration” on page 457 and “Pass Throughs: Preventing Attack Blocking” on page 459.
- **Automated spooling / unspooling** during server outages. See “Configuring the Spool Manager” on page 484.
- **Administrator alerts** Administrators who should receive alerts announcing server events, such as a server outage or initiation of spooling. See “Setting Up Alerts” on page 489.
- **Port 25 protection**, which prevents spammers from bypassing the message security service and sending spam directly to users on the server. See “Setting Up Secure Mail Delivery” on page 495.

Organization Settings

The following *org-level settings* can be made for any organization. Users added to the org receive these settings, and changing a setting applies the change to the whole org. Managing settings from this level makes it easy to apply changes across an org, so use these settings to handle as much of your users’ service as possible:

- **Administrator privileges** Who can manage a group of users and what features can they manage (see “Create Administrators and Manage Authorization Records” on page 162).

For pointers to details on applying these remaining settings, see “Manage Organization Settings” on page 86.

- **Spam / Virus management** How messages are disposed of, whether Blatant Spam Blocking is enabled, and Virus Blocking settings.
- **Allowed / Blocked Senders** that apply for all users in the org.
- **Attachment / Content Manager email polices** What file types or content is specifically allowed or blocked.
- **Unrecognized address policy (Automatic Account Creation / Web-Autocreate / Non-Account Bouncing)** How to handle messages to unrecognized addresses in the org’s domains. You can choose to bounce the message, deliver the message without filtering, or to add the address to the message security service.
- **Notifications** (Quarantine Summary, Welcome New User, Virus Notification, Early Detection Quarantine, etc.) Which of these notifications are sent, and when.
- **Time zone and language settings** for configuring the Quarantine Summary and Message Center.
- **Default User assignment** The Default User that new users get filter settings from.
- **User Access (to Message Center)** Whether users can access quarantined spam and viruses in the Message Center, turn filters on/off, modify spam filters or sender lists, manage their own password and user aliases, or choose their language settings or other features.
- **Message Center Subject links** Whether users can view the content of a quarantined message without forwarding it to their Inbox.
- **Outbound virus blocking** Whether messages sent from users in the org are scanned for viruses.
- **Compliance footer** A standard signature inserted in all users' outbound messages.
- **Daily message limit / per user**
- **User authentication method** The method used to authenticate users and administrators when they log in to their Message Center (or the Administration Console, for administrators).
- **Industry Heuristics** Custom filtering for legal or financial users.
- **Support address**

Default User Settings

When a new user is added to the message security service, it gets certain *user-level settings* from a *Default User*—the one assigned to the organization the new user is added to. These settings include:

- **Spam filters on/off**
- **Virus filters on/off**
- **Spam filter levels** for individual categories of spam

As a template for creating new users, a Default User is how you enforce common filter settings across an org. Unlike with org-level settings, however, if you want to change your policies later by modifying a Default User, the change affects only new users added to the org afterwards, not to existing users. Existing users' filters have to be updated one-by-one. It's therefore important to set up your Default Users carefully before deploying them, and avoid making changes to them afterwards. (For details, see "Manage Default User Templates" on page 114.)

When editing an existing Default User, only edit the spam filter settings. There are settings other than spam filters. But these are best managed either at the org-level. See the other topics in this section, for details.

WARNING: Don't disable Message Center Access for a Default User. Manage User Access at the org-level, instead. See "Enable / Disable Message Center Access" on page 252.

User-Specific Settings

For an individual user, you manage personal settings that apply only for that user. These include:

- **User aliases** Additional addresses the user uses to receive email.
- **Password** The user's password for logging in to the Message Center.
- **Sender lists** The user's personal allowed or blocked senders

You can adjust other settings for a user, too, such as User Access and filter status. But to maintain common policies across an org, these are best done for the organization, and left unchanged for individual users.

For details on each user setting, see "Manage a User's Settings" on page 131.

WARNING: Don't change User Access permissions for an individual user. Manage User Access at the org-level, instead. See "Enable / Disable Message Center Access" on page 252.

User-Controlled Settings at the Message Center

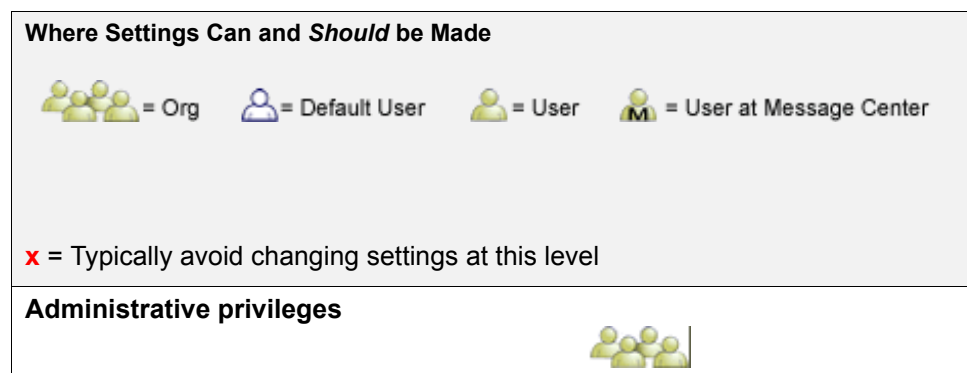
You can optionally allow individual users to manage some settings themselves, by providing them User Access permissions to the Message Center. With the appropriate permissions, users can manage their own:




























- **Spam filters on/off**
- **Virus filters on/off** (although allowing users to turn off virus filtering or virus email blocking is not recommended).
- **Spam filter levels** for individual categories of spam.
- **Approved and Blocked Sender lists** so they can manage their own allowed and blocked senders.
- **User aliases**, which are alternate addresses where the user receives mail.
- **Password** for logging in to the Message Center.
- **Language and Timezone settings**, not available in Message Center Classic.
- **Wireless Forwarding** which allows the user to forward certain kinds of messages to a text-enabled phone, PDA., or other mobile device. (This feature is currently available with *Message Center Classic* only. See "Control What Users Can View and Modify" on page 255.)

For details, see "About the Message Center" on page 247.

Recommended Settings Management

The following chart shows where all settings that affect users' service and administration can be viewed or changed. It also recommends locations where certain settings should *not* be changed.























Where Settings Can and <i>Should</i> be Made	
 = Org  = Default User  = User  = User at Message Center	
x = Typically avoid changing settings at this level	
Email policies Attachment Manager and Content Manager	
Spam / virus management Includes spam and virus dispositions	
Web Autocreate / Non-Account Bouncing Applies only for orgs with associated domains	
Notifications Includes Quarantine Summary	
Support address / time zone	
Default User assignment The Default User applied to new users	
Industry Heuristics	
Message Center subject links	
Outbound virus blocking	
Compliance footer	
User Access (to Message Center) It's strongly recommended that you change specific permissions only at the org-level	  
Daily message limit	  
Virus notification interval	  
Allowed and blocked sender lists	   

Where Settings Can and *Should* be Made

 = Org  = Default User  = User  = User at Message Center

x = Typically avoid changing settings at this level

<p>Wireless Forwarding This should be enabled only by users themselves, at the Message Center. (This feature is currently available for <i>Message Center Classic</i> only. See “Control What Users Can View and Modify” on page 255.)</p>	<p>  </p>
<p>Virus blocking On/Off (should always be On)</p>	<p>  </p>
<p>Spam filtering On/Off</p>	<p>  </p>
<p>Spam filter levels</p>	<p>  </p>
<p>Notification address (if other than the user's primary address)</p>	<p> </p>
<p>Approved recipients/ mailing lists For allowing messages sent to mailing lists</p>	<p>  </p>
<p>User aliases and password</p>	<p>  </p>

Chapter 5

Organization Management

About Organization Management

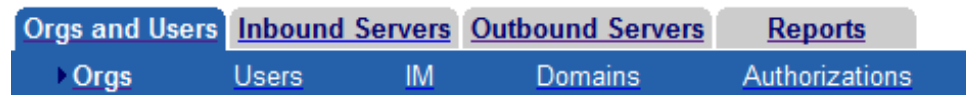
You manage your users' email protection by arranging them into groups called *organizations* (or *orgs*, for short). An org can be configured to give its users specific services or management control, such as a support address, email policy, or administrator. You can also create sub-organizations (or *sub-orgs*) below an org, to create a finer level of control within a larger group.

A few special orgs don't contain users but are for billing (your Account org) or server management (an email config).

For details on org behavior, strategies for arranging them in your hierarchy, and recommendations for managing them, see "About the Organization Hierarchy" on page 61.

See the next sections for details on viewing and navigating organizations in your Administration Console, creating, moving, and deleting orgs, and configuring their settings.

View Your Organizations



To view and manage your organizations, go to the Organizations page (under Orgs on the Orgs and Users tab). From here, view summaries of each org's service, access any org's settings, add and delete orgs, and more.

You can list organizations:

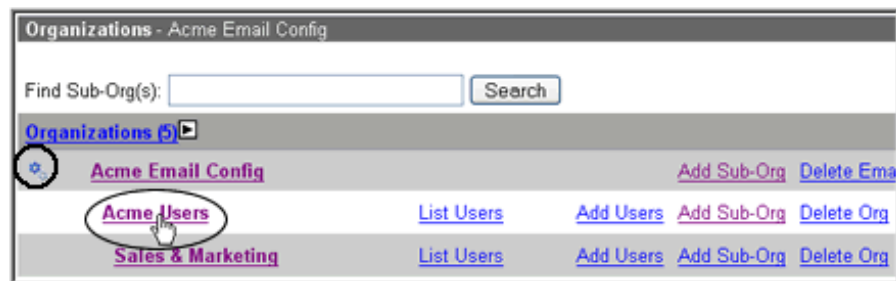
- Along with links to related commands.
- Along with a summary of service settings.
- In a list showing each org's domains
- In a convenient pop-up that you can keep around.
- In a Choose Orgs list at the top of most pages.

Note: The exact orgs you see and tasks you can perform depend on your administrative privileges. See “Create Administrators and Manage Authorization Records” on page 162.

List Organizations with Commands

Initially when you go to the Orgs and Users tab, each organization is listed along with convenient links for managing its service. The page displays the current org and all its sub-orgs.

You can adjust the number of organizations displayed per page.



Organizations page: Click an org to access its settings. An email config is marked by a gear cog icon.

Organizations page overview	
Choose Org list (top of page)	Choose an org from this list to list only that org and its sub-orgs on this page.
Organization link (in list)	Click an org to access its service settings. See “Manage Organization Settings” on page 86.
Find Sub-Org form	Find an org quickly by typing its name. See “Find an Organization” on page 92 for important details.
List / Summary Settings links (under gray bar)	Click these links to switch between viewing orgs along with commands or summaries.

Organizations page overview	
View Hierarchy with Domains link (top of page)	Click this link to list each org along with its domains.
Download Orgs/ Settings link (top of page)	Click this link to retrieve settings for currently listed orgs as comma-delimited text, which you can then import into a spreadsheet. See “Download Organization Settings” on page 101.
List Users, Add Users, etc., links (shown for each org)	Click one of these links for an org to: <ul style="list-style-type: none"> • List its users • Add users to it • Add a new sub-org below it • Delete the org. • List or add to its domains • Test its server performance

List Organization Summaries

To instead list orgs along with details about their service, click the Summary Settings link (under the gray bar). This displays the Organization Summaries page.

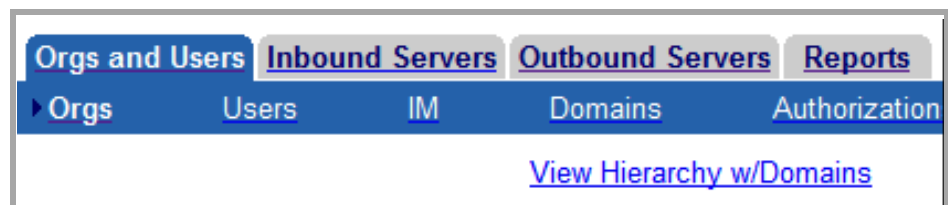
Default User	Last Modified	Date Created	Creator
-	05-31-05	03-30-05	bschmell@postintrainin ...
pdefault@a.acme.com	06-01-05	03-30-05	bschmell@postintrainin ...

Organization Summaries: Click links to switch between listing orgs with Commands or Settings Summaries.

Organization Summaries page overview	
Domains	The number of domains currently associated with the org. Click the link to list these domains.
Users	The number of users currently in the org. Click the link to list these users.

Organization Summaries page overview	
Default User	The user template whose settings are applied to new users in the org. Click the link to manage these settings.
Last Modified	The date the org was last modified (a setting changed, user added, and so on).
Date Created	The date the org was created
Creator	The administrator who created it. For the first initial organization, this is blank.

List Organizations with Domains



Each user organization can have one or more domains associated with it. This association is relevant for determining how messages to unrecognized addresses in a domain are handled (see “Handle Mail to Unrecognized Addresses” on page 98). To view all organization/domain associations:

1. Go to Orgs on the Orgs and Users tab and click the View Hierarchy w/ Domains link, at the top of the page.

The Organization Hierarchy page lists all organizations, along with their associated domains.

2. Click any org to access its service settings. Or click a domain to access settings for that domain.



View Hierarchy page: Lists orgs along with their domains. Here, [a_acme.com](#) and [a_acme3.com](#) are associated with the A_Acme Users org.

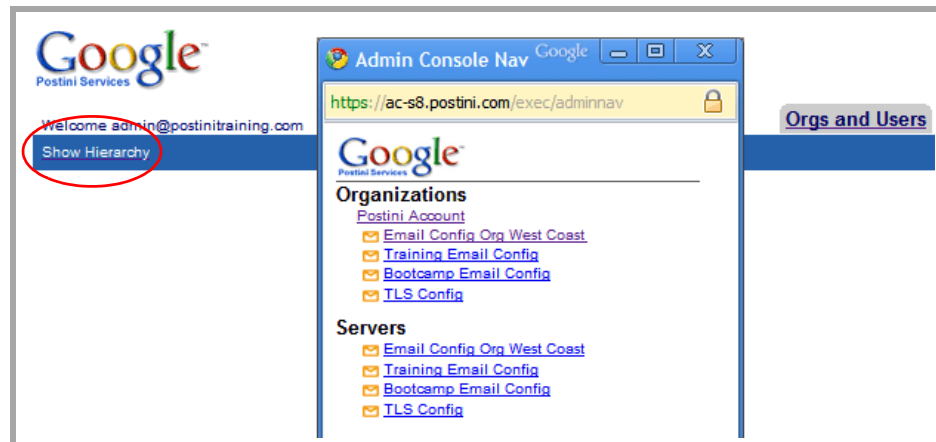
Show Orgs in a Popup Window

Keep access handy to all organizations from a popup window that can always stick around.

Note: A maximum of 25 organizations can be displayed in the popup window. To view large numbers of organizations, go to Orgs & Users > Orgs. You can adjust the number of organizations displayed per page.

1. Click the Show Hierarchy link at the top of any page.
2. In the popup window, click an org to access its settings.

Click an org under Organizations to access its service settings. Or click an email server config under Servers to manage or monitor its email server configuration.



Show Hierarchy popup window: Clicking an org goes to its service settings or Servers tab.

Change Orgs On the Current Page

To navigate between organizations while viewing a specific feature or component, use the Choose Org list at the top of most pages. For example, while viewing spam settings for the Customer Service org, choose New York from this list to instead see the New York org's spam settings.

Choosing an org while on the Organizations page (which lists all your orgs), narrows the list to only that org and its sub-orgs.

Note: Only 45 orgs can be displayed in the Choose Orgs list.

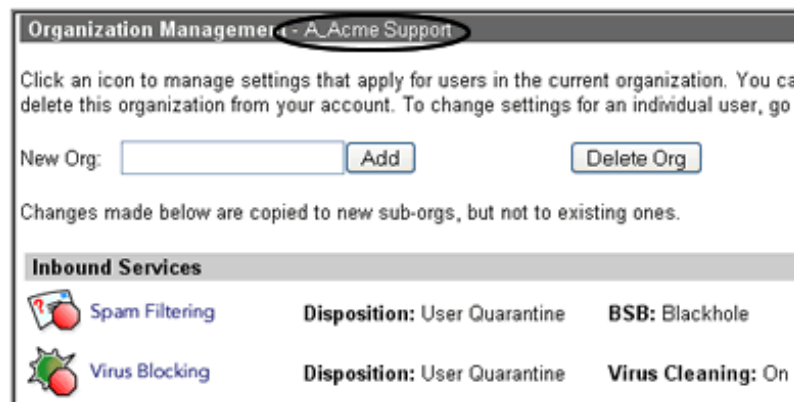


Choose Orgs list: Navigate conveniently between organizations while viewing a specific feature or component

Manage Organization Settings








To set email policies and configure services that apply for all users in an organization, go to the org's Management page. Then click a feature to view or change its settings. The change applies to all users in the org. To get to this page:

- Click the org under Orgs and Users > Orgs.
- Click it in the Show Hierarchy pop-up window.
- Or from another org's Management page, choose it from the Choose Org list at the top of the page.







Organization Management page: Shows settings for the org named at the top of the page. Click a feature to manage those settings.

Inbound Services





Inbound Services	Description
 Spam Filtering	Enable/disable Blatant Spam Blocking for the organization, and set a spam disposition (method of processing spam). See “Configure Spam Settings for an Organization” on page 297 and “Configure Spam Disposition for an Organization” on page 300.
 Virus Blocking	Set a virus disposition and manage other org-level virus settings. See “Configure Virus Settings for an Organization” on page 318.
 Attachment Manager	Filter messages based on the size and file type of attachments. See “Attachment Manager” on page 403. Optional feature, not available with all service packages.
 Content Manager	Filter messages based on their text content. See “About Content Manager” on page 329. Optional feature, not available with all service packages.
 Message Limits	Set a daily limit on the number of messages each user in the org can receive. See “Set an Organization’s Message Limits” on page 93.
 Sender Lists	Specify sender addresses that should be either approved or blocked for all users in the organization. In addition to senders listed here, individual users can define their own allowed and blocked senders. See “Editing Sender Lists in Message Center” on page 393.
 Industry Heuristics	Filter messages with legal or financial content less rigorously, or specifically allow them regardless of spam-like content. Also allow messages from a network of trusted senders within each industry. Applies when users in the organization are in a legal or financial industry. See “Industry Heuristics” on page 417. Optional feature, not available with all service packages.







Outbound Services






All outbound services are optional features that aren't available with all service packages.

Outbound Services	Description
 Virus Blocking	Apply virus blocking, or attachment or content filters to outbound messages, that is, messages sent <i>from</i> users in this organization. See "About Outbound Services" on page 507.
 Attachment Manager	
 Content Manager	
 Compliance Footer	Place a standardized text message at the bottom of messages sent from users in this organization. See "Compliance Footer" on page 518.

Organization Settings

Organization Settings	Description
 System Tests	Test mail flow to and from your mail server via the data center. Also verify MX record configurations for any domain associated with this org. See "Troubleshoot Incoming Email Delivery" on page 544.
 General Settings	Change the org's name or location in the hierarchy. Specify a support address, a Default User, policies for creating users, Message Center policies, and more. See "Organization General Settings" on page 94.
 Single Sign On	Configure Single Sign On for your account and for individual user orgs. See "Configuring Single Sign On (SSO)" on page 623.
 DNS Instructions	See instructions for configuring MX records for this org's domains. These records direct email flow to the message security service's primary and backup data centers. See "Edit a Domain" on page 243.

Organization Settings	Description
 User Access	<p data-bbox="833 201 1386 359">Control what settings users in this org have permission to view or modify at their Message Center. See “Enable / Disable Message Center Access” on page 252 and “Control What Users Can View and Modify” on page 255.</p>
 Default User	<p data-bbox="833 384 1414 510">Manage default user-level settings applied to new users added to this org, such as spam filter levels and virus blocking. See “Manage Default User Templates” on page 114.</p> <p data-bbox="833 537 1414 663">WARNING: These settings belong to a <i>Default User</i> that can be shared by several organizations. Changing its settings affects all orgs using this Default User, not just this org.</p>
 Notifications	<p data-bbox="833 684 1414 747">Specify whether users in this organization receive any of these email notifications:</p> <ul data-bbox="833 774 1414 1293" style="list-style-type: none"> <li data-bbox="833 774 1338 837">• Welcome sent when a user first gets a Message Center account. <li data-bbox="833 865 1365 928">• Virus sent when one of more viruses has recently been received <li data-bbox="833 955 1414 1018">• First Spam sent when the user’s first spam is quarantined in their Message Center. <li data-bbox="833 1045 1414 1108">• New Spam (Quarantine Summary) a periodic list of newly quarantined spam. <li data-bbox="833 1136 1354 1199">• Suspension sent when the user is temporarily suspended from the service. <li data-bbox="833 1226 1414 1289">• Attachment Manager sent when a message is quarantined by an Attachment Manager filter. <p data-bbox="833 1320 1260 1383">See “Configuring Notifications for an Organization” on page 273.</p>
 Password Policies	<p data-bbox="833 1409 1406 1587">Manage and configure password policies for users for an organization, including Length, Complexity, Maximum Age, History, and Lockout Threshold. See “Set User Password Policies” on page 144. This feature is not available for all products.</p>
 Directory Sync	<p data-bbox="833 1619 1406 1713">Directory Sync utility to import user information from a directory server. See “Directory Sync” on page 205.</p>
 Branding	<p data-bbox="833 1776 1360 1860">Control branding and logo information for the Message Center. See “Brand Your Message Center” on page 267.</p>

Organization Settings	Description
 Archiving	<p>Optional feature. Configure Message Archiving. For more information about Message Archiving, see:</p> <p><i>Message Archiving Administration Guide</i></p>
 IM Settings	<p>Configure IM Settings for Postini IM Security, an optional product. See the <i>Postini IM Security Administration Guide</i> for more information.</p>
 Encryption Settings	<p>Optional feature. Configure Message Encryption settings. For information about Message Encryption, see:</p> <p><i>Message Encryption Administration Guide.</i></p>
 Usage Details	<p>Available only for authorized administrators, and only for the Account organization</p> <p>View a monthly summary of service usage by users in all your organizations. See “About Usage Details” on page 671.</p>
 User Limits	<p>Set a limit on the number of users that can be added to an account, enable alerts for when that limit has been met, and enter addresses for alert recipients.</p> <p>Available only for authorized administrators, and only for the Account organization.</p> <p>See “Set and View User Limits, Enable Alerts” on page 103.</p>

Organization Summary

Organization Summary	Description
Organization ID	A unique ID for this organization, useful when escalating an issue to Customer Care. An org’s name can be changed, but its ID always remains the same.
Organization	The org’s name. Can be changed under General Settings.
View Email Activity Link	Goes to the Home page where you can see a graph summarizing this org’s email activity over the past 60 minutes.
Creation Date	The date the org was created.

Organization Summary	Description
# of Users	The number of users in this org. Click the link to list the users.
Domains	One or more domains associated with this org. Clicking the link goes to the Domains page. See “Domains” on page 233.

Create an Organization

To apply separate email policies or services for an individual group of users, create a new organization, configure it with those policies or services, and add the users to it. You can add an org anywhere in your hierarchy. The new org becomes a sub-organization (or *sub-org*) of the parent you add it to.

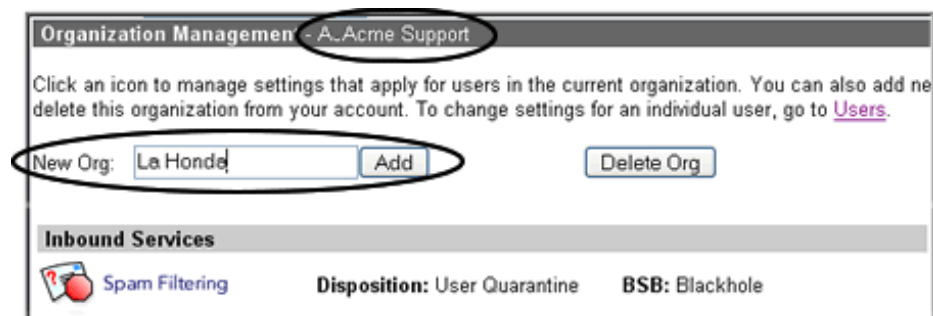
For tips on when and why to create orgs, see “Plan Your Organization Hierarchy” on page 68.

1. Go to the Management page of the org that will be the parent of your new org. (Click the org under Orgs and Users, or click the Add Sub-Org link next to it).
2. On the parent’s Management page, enter a name for the new org in the New Org field (100 characters or less). Click Add.

The name in the gray bar changes, indicating that you’re now looking at your new org’s settings, which were copied from the parent. You can change them now, to apply for this org’s users, only (see “Manage Organization Settings” on page 86).

Optionally, you can assign privileges for one or more administrators to manage the new org. Administrators of the parent org have privileges to manage it, too. See “Administrators” on page 157.

Changes made later to the parent org will not be copied to this one, unless you specifically choose for them to (see a particular feature’s topic for details on propagating changes to existing sub-orgs).



Creating a sub-org of the A_Acme Support org, named La Honda.

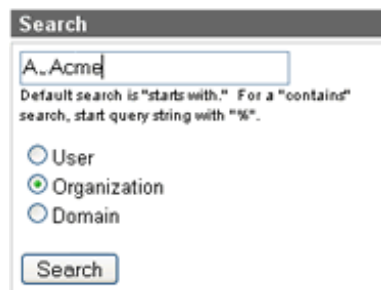
A_Acme Support	List Users	Add Users	Add Sub-Org
La Honda	List Users	Add Users	Add Sub-Org

On the Organizations page, La Honda is displayed as a sub-org of A_Acme Support.

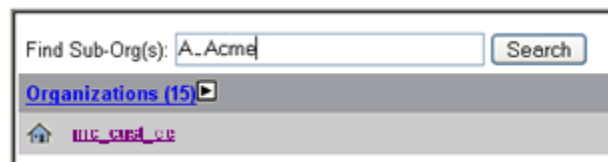
Find an Organization

You can quickly find any organization by typing its name in a search form, on either the Home page or the Organizations page:

1. Locate the appropriate search form on the Home or Organizations page.
 - Searching from the Home Page



- Searching from the Organizations page.



2. You can search only for orgs that are beneath the current org in your hierarchy. So use the Choose Orgs list change the current org, if necessary.

3. Type the org name you're looking for, in the form.
 - Enter the entire name to find one org. Preceding your search text with an = also finds an exact match.
 - Type the beginning of the name to find all orgs that *begin* with your text.
 - Precede your text with a % to find all orgs that *contain* your search text.
 - End your text with a \$ to find all orgs that *end* in your text.
4. Click the Search button. One or more orgs matching your text appear in a results list. Click an org to access its settings.

Set an Organization's Message Limits

Orgs > Organization Management >  Message Limits

To limit daily number of messages that users in an organization can receive, go to Message Limits on the org's Management page. This page also displays a maximum message size for users in this org, defined in Attachment Manager.

Field	Value
Maximum Message Size	The maximum size of attachments-per-message that users in the organization can receive. Messages that exceed this limit are bounced, returning a SMTP error <code>552 Message too large - psmtp</code> message to the sender. This value is defined in Attachment Manager (See "Configure Attachment Manager" on page 406).
Daily Message Limit	<p>The maximum number of messages each user in the org can receive, per day. Leave blank to impose no limit.</p> <p>When exceeded, incoming messages are bounced, returning a <code>554 Mailbox limit exceeded.</code> message to the sender. Setting a message limit is useful for protecting mail servers against malicious attacks, such as email bombs. All messages are counted against this limit, including legitimate and quarantined messages. The count is approximate, so it's suggested only for values over 100.</p> <p>This limit can also be set for individual users. Whichever limit is lower—the org limit or a user's limit—applies for the user. If a user's limit is blank and a value is set here for the org, the org value applies to the user. See "Manage a User's Settings" on page 131.</p>

Organization General Settings

Orgs > Organization Management >  General Settings

Under General Settings on the Organization Management page, you can change the org's name or location in the hierarchy, assign a support address and Default User, set policies for creating users in the org, and more.

Makes settings as described below, and click Save when you're done.

Organization General Settings	
Customer Name	Your account name. It's used in the name of your Account org if set for the Account org, and appears by default in user notifications (see "Quarantine Summary & Notifications" on page 273).
Organization ID	A unique ID for this org, useful when escalating an issue to Customer Care. An org's name can be changed, but its ID always remains the same.
Organization Name	The name of the current org.
Parent Organization	<p>The org one level up in the hierarchy.</p> <ul style="list-style-type: none">• When the current org was created, it received a copy of its original parent's settings.• The current org can be administered by its parent's administrators. <p>Entering a new parent here reassigns the current org to the new parent, moving it to a new location in the hierarchy. See "Move an Organization" on page 100.</p>
Auth(entication) Method	<p>Displays the method used to authenticate users and administrators in this org, when they log in to their Message Center (or the Administration Console, for administrators). The method types are:</p> <ul style="list-style-type: none">• POP Authentication (POP)• Privately Managed Password Authentication (PMP)• SHA1 Cross-Authentication (XAuth) <p>The authentication method can't be changed using the Administration Console. You must instead submit a work request with support. See "About User Authentication" on page 615.</p>

Organization General Settings	
Authentication Data	<p>(Shown only if the authentication method is XAuth or POP).</p> <p>A text string used for authenticating users and administrators when they log in to the Message Center or Administration Console. See “About User Authentication” on page 615.</p>
Email Config Org Type	<p>“Yes” means that this org is an <i>email server config</i>.</p> <ul style="list-style-type: none"> • It should be mapped to an email server (see “Setting up Delivery Manager” on page 475). • Users and domains on this server should be associated with orgs underneath this email config in your hierarchy. • The email config shouldn’t have users or domains assigned to it directly (only to its sub-orgs). • One email config can’t be the sub-org of another. <p>See “Creating an Email Config” on page 422.</p> <p>“No” means the organization is either your Account org, or a user org.</p>
Support Contact	<p>An email address where users can contact you for support. This can be any address, and does not have to be in the message security service. When a user clicks a support email link in the Message Center, a Web page opens containing a form that submits the user’s inquiry to this address.</p> <p>This address is also the sender address for notifications.</p> <p>Note: Keep the Support Contact address current, as it’s your users’ primary way of getting in touch with you for help.</p>
EZCommand Shared Secret	<p>A text string used for authentication of EZCommands submitted by administrators in this org.</p> <p>EZ Command is an interface for performing basic administrative tasks without having to log in to the Administration Console. See “About EZCommand” on page 612.</p>

Organization General Settings	
Non-Account Bouncing	<p>When Non-Account Bouncing is on, messages are bounced if they are not addressed to a registered user or alias. The SMTP error message: 550 No such user - psmtp is returned to the sender.</p> <p>This setting is used for organizations that contain domains. In other organizations, this setting has no effect. Non-Account Bouncing applies to all domains in an organization.</p> <p>No reports or statistics of bounced messages are logged.</p> <p>See “Handle Mail to Unrecognized Addresses” on page 98 for details on why this feature may be helpful.</p>
Default User	<p>Required for any org that contains users.</p> <p>The address of a user whose settings are copied to new users added to this org. The Default User must already be added to the service. Its address can be any user address if entered into this field. In addition, any user with pdefault@<your domain name> or postinidefault@<your domain name> is considered a Default User. New users added to this org receive user-level settings from this Default User.</p> <p>See “Manage Default User Templates” on page 114 and “Reset a User” on page 149.</p>
Automatic Account Creation	<p>When Automatic Account Creation is enabled, users in domains associated with this organization are added automatically to the message security service, as soon as they begin to receive valid messages. Users are added to this organization.</p> <p>Rather than relying on a SMTP “250” response from the server to validate recipients, however, Automatic Account Creation does so by identifying that the messages themselves are legitimate (that is, not spam). Automatic Account Creation can therefore be used with any type of email server, including Microsoft Exchange.</p> <p>See “Add Users Automatically (Automatic Account Creation)” on page 129 for details.</p>

Organization General Settings	
Web Autocreate	<p>Applies only if the org has associated domains.</p> <p>When Web Autocreate is enabled, unrecognized users in these domains are added automatically to the message security service when they first log in to their Message Center.</p> <p>Web Autocreate does not work if the org is an email server config.</p> <p>See “Add Users Automatically to an Org” on page 126.</p>
Message Center Subject Links	<p>When On, users can click subject links of quarantined messages in their Message Center to view the full body of the message.</p> <p>When Off, links are disabled and users can view only the subjects of messages. Users must deliver a message to their Inbox to view its contents.</p> <p>Tip: Disabling subject links is useful for meeting SEC requirements to archive all messages viewed by employees. See “Prevent Users from Opening Quarantined Messages” on page 261.</p> <p>This is an optional feature which may not be available in your service package.</p>
Time Zone	<p>If users in this organization receive a regularly scheduled Quarantine Summary notification, the notification is sent based on this time zone. See “Configuring Notifications for an Organization” on page 273.</p>
Region and Language	<p>Choose your region and language for text in the quarantine summary and the Message Center.</p> <p>Note: The Message Center supports a subset of the languages listed in the Region and Language menu.</p> <p>For more information, see “Quarantine Summary & Message Center Localization” on page 288.</p>
Character Encoding	<p>Choose the character encoding for the message Subject lines in the quarantine summary and Message Center.</p> <p>For more information, see “Quarantine Summary & Message Center Localization” on page 288.</p>

Organization General Settings	
Apply settings and filters to existing sub-orgs	<p>When this option is selected and you click Save, settings that aren't marked with a red * are applied to the organization's sub-orgs, as well.</p> <p>WARNING: Choosing this option applies all these settings to all sub-orgs, not just the settings you change.</p>

Handle Mail to Unrecognized Addresses

Once you add a domain to the message security service, all email to that domain is routed through the data center. Only addresses *recognized* by the data center—that have been added as users, for example—receive filtering. But email to other addresses in the domain—to users that aren't yet added to the service, that aren't receiving protection, or that don't exist—must be dealt with, too.

For each domain, you can choose one of two ways to handle mail to unrecognized addresses. Do this by associating the domain with an organization. Then configure the org's General Settings—Automatic Account Creation and Non-Account Bouncing—as described below. All domains associated with an org must share the same policy for handling mail to unrecognized users.

Note: An address is *recognized* if it's been added to the service as a user or user alias; if it's supported by a *domain alias* or *subdomain-stripping*; or if its domain has a catchall account. See “Manage User Aliases” on page 140, “Add a Domain for Filtering” on page 236, “Subdomain Stripping” on page 240, and “Add a Catchall Account (Legacy Feature)” on page 241.

Unrecognized Mail Option	Org General Settings
Add the user and deliver the message	<ul style="list-style-type: none"> • Automatic Account Creation = On • Non-Account Bouncing = Off <p>Unrecognized users are added automatically to the message security service, when your mail server accepts three legitimate messages (that is, not spam) for an address.</p> <p>Use Case: Use this option only if all users in a domain are to receive email protection, not just some users.</p> <p>WARNING: You must configure these settings for an org that contains your domains.</p>

Unrecognized Mail Option	Org General Settings
<p>Bounce the message</p>	<ul style="list-style-type: none"> • Automatic Account Creation = On • Non-Account Bouncing = On <p>Messages to unrecognized users are bounced, never reaching the intended recipient. The SMTP error: 550 No such user - psmtp is returned to the sender.</p> <p>If your Google Apps account has catchall enabled, Non-Account Bouncing must be Off.</p> <p>For users to receive email protection, they must be added to the service via the Administration Console (see “Manage Default User Templates” on page 114).</p> <p>Use Case: Use this option to allow only users added via the Console to receive email, filtered or not.</p> <p>WARNING: You must configure these settings for an org that contains your domains.</p>
<p>Deliver the message, without filtering or adding it to the service</p>	<ul style="list-style-type: none"> • Automatic Account Creation = Off • Non-Account Bouncing = Off <p>Messages to unrecognized users are delivered without filtering. No users are added to the message security service.</p> <p>Use Case: Use this option to allow everyone in a domain to receive email, even if they aren’t all added to the message security service.</p> <p>WARNING: You must configure these settings for an org that contains your domains.</p>

When users are passed through without filtering

If you turn off Automatic Account Creation and Non-Account Bouncing for an org, thus passing messages through to unrecognized users, without filtering them, those users still receive certain protections:

Services available to users <i>not</i> added to the message security service	
Outbound Virus Blocking	Applies, if enabled for the email config above the org containing the user's domain.
Outbound Attachment Manager or Content Manager filters	See "About Outbound Services" on page 507.
Compliance Footer	
Connection Manager: protection against Spam Attacks, Directory Harvest Attacks, Email Bombs, and Virus Outbreaks	Applies, if enabled for the email config above the org containing the user's domain. See "Automatically Blocking Attacks" on page 453.

Move an Organization

You can move an organization to a new location in your organization hierarchy by assigning it to another parent. Do this under General Settings on the org's Management page.

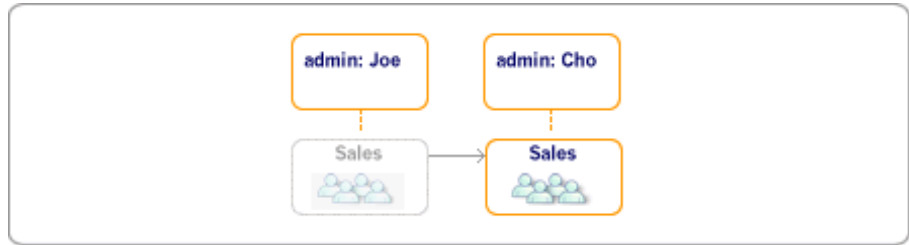
1. Locate the org you want to move, under Orgs and Users, and go to the org's Management page.
2. Scroll down and click General Settings.
3. Enter the name of the new parent org in the Parent field, and click Save.

Why Move an Organization?

An organization's location in the hierarchy can determine which administrators manage it. It also determines the server where filtered email gets delivered. You might move an org:

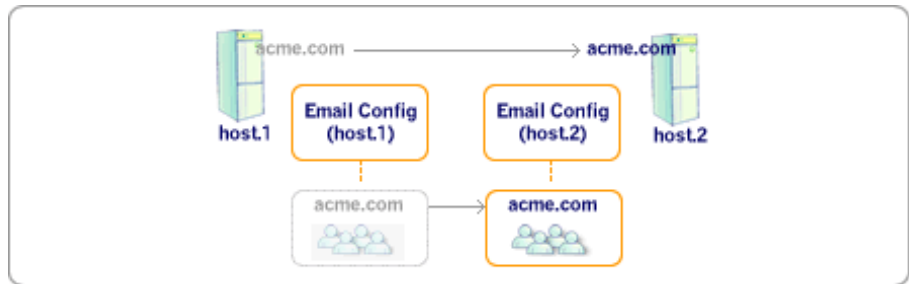
- **To assign it to a different administrator's chain of management.** An organization can be managed not just by its own administrators (if any), but by its parent org's administrators. If you arrange orgs based on who administers them, you might move an org from one administrator's leg of the hierarchy to another's.

Below shows how moving the Sales organization reassigns it to Cho's administrative care.



- **If you move an associated domain to another email server.** Users and domains processed by a particular email server, must be associated with orgs below that server's email config. If you move a domain to another server, you must move all orgs associated with that domain and its users, to somewhere below the new server's email config.

This example shows how moving a domain to a new server requires moving orgs associated with the domain and its users, to somewhere below the new server's email config.



Download Organization Settings

Orgs and Users	Inbound Servers	Outbound Servers	Reports
Orgs	Users	IM	Domains
Download Orgs/Settings			

You can download settings for one or more organizations as text. Then import the text into a spreadsheet, for easy reference. Listed for each org is its support contact, filter settings, and other details of its service.

1. Go to Organizations page under Orgs and Users, and list of the orgs whose settings you want to download as text.
 - Use the Choose Orgs list to show a particular organization and its sub-orgs (choose the top-level org to show the entire hierarchy).
 - Perform a search to list organizations with common name elements, for example those that contain the text “sales.”
2. Click the Download Orgs/Settings link at the top of the page.
3. Save the resulting text as a text file, then import it into a spreadsheet in a comma-separated format.

Delete an Organization

If you no longer have need for an organization—either its users have left the message security service, or you’ve moved them to another org—you can delete the org.

1. Delete all users from the organization, as well as any sub-orgs.
2. Locate the org on the Organizations page (under Orgs and Users), and click the Delete Org link next to it in the list.

Or on the org’s Management page, click the Delete Org button.

3. When prompted, click Confirm to delete the org.

Troubleshoot Organizations

I’m using Quarantine Redirect for an org to quarantine all its users’ spam and viruses to a single administrator’s quarantine. Only there are more quarantined messages than can be displayed at once in the Quarantine or Message Center.

Too many users are in the org to conveniently manage all their diverted messages from a single Quarantine. Divide the users into sub-orgs underneath the original org. Then assign each org a separate Quarantine Redirect address. See “Manage Quarantined Messages” on page 135.

Chapter 6

Users and Quarantines

About Users and Quarantines

A *user* is an email account on your mail server that has been added to the service. When a user is added to the service, the email for that account is then filtered by the service.

Each user resides in an organization (*org*) and inherits the associated *org-level* settings, such as a support address, administrator, or email policy. A user inherits its initial *user-level* settings, such as filter and virus settings, from a Default User. Some of these initial settings can be changed for an individual user, either by an administrator in the Administration Console, or by the user in the Message Center. For recommendations on what settings you can safely change for individual users, see “What Settings Are Made Where” on page 73.

An *administrator* is a user who has been assigned privileges to manage one or more organizations (see “Create Administrators and Manage Authorization Records” on page 162).

A user’s filtered spam and viruses can be placed in a Quarantine where administrators can review and manage them. You can quarantine each user’s suspicious messages in a separate User Quarantine, or set up a central Quarantine for all users’ messages. If you implement separate User Quarantines, you can give users access to the Message Center so they can log in to view their own filtered spam and viruses, and retrieve any legitimate messages that were wrongfully quarantined.

Access to the Message Center also lets users manage other settings, such as their own filter levels, sender lists, and wireless forwarding.

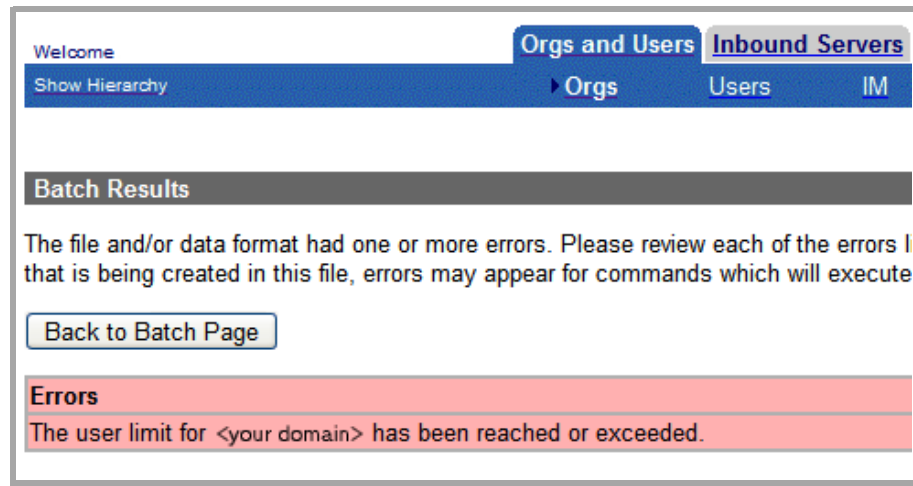
Set and View User Limits, Enable Alerts

The User Limits page lets Reseller Administrators and Postini internal administrators set a limit for the number of users that can be added to an account.

Account Administrators can use the page to track the maximum number of users allowed for an account, and the current number of users in that account. Account Administrators can also enable alerts that are sent when the limit is reached, specify the recipients of those alerts, and see when the last alert was sent.

If there is a limit on your account and you reach that limit, you cannot add users via the Administration Console or batch command. If you have enabled Automatic Account Creation, any users added after the limit has been reached remain provisional users.

If you attempt to add users by any means after the limit has been met, you receive the following error:



If you have enabled Automatic Account Creation, any users added after the limit has been reached remain provisional users.

Set User Limits

Note: The privilege to set user limits is currently reserved for Reseller Administrators.

To set user limits for an account:

1. Select the Account org for which you want to set user limits.

2. Under Organization Settings, click **User Limits**.

User Limits - Archive Stable Account

User Limit Current number of users: 167

Current user limit:

User Limit Alert Enable user alert: Yes No

List recipients who should receive alerts:

Last alert sent:

3. In the *Current user limit* field, enter the maximum number of users allowed for the account.

If you enter nothing in this field, then there is no limit to the number of users that can be added to the account.

4. Click **Save**.

View User Limits, Enable Alerts, Specify Alert Recipients

Note: The privilege to view user limits and configure alerts is reserved for Account Administrators.

Depending on your contract, you might be billed based on the total number of users added to your message security service. There might also be a limit to how many additional users you can add. The User Limits page lets you track your current usage, and see whether you're within your limit. You can also enable alerts and specify recipients.

To view user limits, enable alerts, and specify alert recipients:

1. Select the Account org for which you want to view user limits.

- Under Organization Settings, click **User Limits**.

The screenshot shows a dialog box titled "User Limits - Archive Stable Account". It contains the following information:

- User Limit**: Current number of users: 167; Current user limit: (blank)
- User Limit Alert**: Enable user alert: Yes No; List recipients who should receive alerts: (text input field)
- Last alert sent: (text input field)

At the bottom, there are two buttons: "Save" and "Cancel".

- Configure the following options:

For this option...	Do this...
Current number of users	Read Only. Displays the current number of users in your account.
Current user limit	Read Only. Displays the limit for the number of users you can add to your account. If this field is blank, there is no limit. If the limit has been met, you cannot add additional users. If you need to add new users, you can delete existing ones, or call to increase the limit.
Enable user alert	Yes: An alert is sent to recipients when the user limit is reached. No: No alert is sent when the user limit is reached.
List recipients who should receive alerts	Enter a comma-separated list of email addresses for alert recipients.
Last alert sent	Read Only. The time and date of the last alert.

- Click **Save**.

Alerts

When the system sends an alert, you see a message similar to the following:

```
From: <your internet service provider> Support
```

To: <alert recipients>
Subject: <Account org> <User> Limit Reached
Date: <date>

Dear <alert recipients>,
The organization named <Account org> has reached its user limit.

Current number of users: <your current number of users>
Current user limit: <your user limit>

No additional users can be added to your organization without raising the limit or deleting users. Please contact your email administrator to update your limit.

<your internet service provider> Support

The system sends an alert anytime you are at your limit and then attempt to add a user by any means.

View All Your Users



View a list of users currently receiving email protection under **Orgs and Users > Users**.

You can list users:

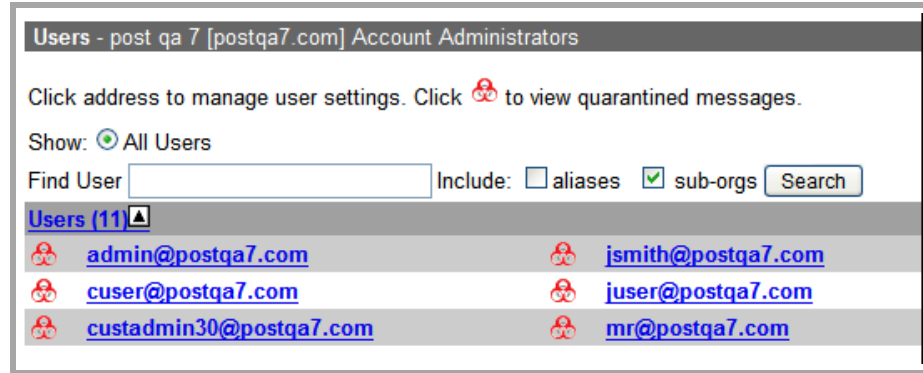
- By address only, showing many users at once
- With a summary of each user's settings
- Sorted by domain


From this page, you can also:

- Search for users (see "Search for Users" on page 111)
- Access user settings (see "Manage a User's Settings" on page 131)
- Move users ("Add / Delete / Move Users" on page 120)
- Download a list of users and settings ("Download Users and Settings" on page 150)

List Many Users

When you first open the Users page, it lists users by address only, allowing you to scan many users at once. The page displays all users in the current organization and its sub-orgs.








Users page overview	
Choose Org list (top left)	Choose an org from this list to display only users in that org and its sub-orgs.
Find User form	Find a user quickly by entering the address. See “Search for Users” on page 111 for more information.
User address link (in table)	Click a user address to access that user’s individual settings. See “Manage a User’s Settings” on page 131.
 (in table)	Click the Quarantine icon next to an address to open that user’s Quarantine. See “Manage Quarantined Messages” on page 135.
List / Settings Summary links (top right)	Click these links to switch between viewing many users in a quick list, or fewer users in a detailed list.
Add/Delete/Move Users link (top of page)	Click this link to add or delete users, or move them to another org. See “Add / Delete / Move Users” on page 120.
Download Users/ Settings link (top right)	Click this link to retrieve settings for currently listed users as comma-delimited text, which you can then import into a spreadsheet. See “Download Users and Settings” on page 150.
Provisional Users link (top right)	Click this link to manage any pending <i>provisional</i> users, recently added via Automatic Account Creation. See “Add Users Automatically (Automatic Account Creation)” on page 129.

List User Summaries

To list users along with details about their settings, click the **Settings Summary** link.

The screenshot shows a user interface with a search bar and a table of user summaries. The 'Settings Summary' link is circled in red. The table has the following data:

Spam						Virus	Wireless	Modified	Creator	Created	Method
On	2	2	2	2	2	On	Off	05-01-08	-	10-05-07	-
On	2	2	2	2	2	On	Off	04-16-08	admin@busyworkerbee.com	10-05-07	Admin Batch or API
On	2	2	2	2	2	On	Off	10-05-07	-	10-05-07	-

User Summaries page overview	
Find User form	On this page, there are additional fields for refining your search. See “Search for Users” on page 111.
Aliased To	If the address is a <i>user alias</i> , this column displays the primary user address for which this is an alias. See “Manage User Aliases” on page 140.
Spam	Shows whether or not Spam Filtering is enabled (see “Enable and Adjust Spam Filters” on page 301).
	Bulk Email filter. This master spam filter blocks most unsolicited email, across all spam categories. Additional protection for individual categories is provided by the following filters.
	Sexually Explicit filter: Level of increased protection against sexually explicit spam.
	Get Rich Quick filter: Level of increased protection against money-making offers.
	Special Offers filter: Level of increased protection against commercial offers.
	Racially Insensitive filter: Level of increased protection against hate-oriented topics.
Virus	Shows whether Virus Blocking is enabled.
Wireless	Shows whether the user has enabled Wireless Forwarding (see “User General Settings” on page 142 and “Control What Users Can View and Modify” on page 255.) Note: Wireless is available only with Message Center Classic.
Modified	The date the user was last modified.

User Summaries page overview	
Creator	The administrator who created the user.
Created	The date the user was added.
Method	How the user was added. Possible entries include: <ul style="list-style-type: none"> • Admin Console: With the Add/Delete/Move form (see “Add / Delete / Move Users” on page 120). • Admin Batch or API: Created using a Batch File or EZCommand. Users added through Directory Sync are considered to be added by Admin Batch. • Automatic Account Creation or Web Autocreate: Automatically, via one of these creation methods (see “Add Users Automatically to an Org” on page 126).

List Users by Organization

To list users in a particular organization but not in any of its sub-orgs:

1. Open the Users page and choose the org from the Choose Orgs list.
2. Clear the **Include: sub-orgs** check box in the Find User form. Enter nothing else in the form.
3. Click **Search**.

List Users by Domain

To list users in a particular domain:

1. On the Orgs and Users tab, click the **Domains** link.
2. In the list of domains, click the **List Users** link to the right of the domain name.

If you don't see this link, you might be on the Domain Summaries page. Click the **Commands** link on the top right to return to the Domains page.

Search for Users

Quickly find any user by typing its address in any of several convenient search forms. Search for users:


- Under Orgs and Users > Users, where you can also find user aliases or confine your search to particular organizations.
- From the Home page, where you can go directly to a user's Overview or Quarantine.
- By entering a partial address (as a shortcut, or to narrow your search).

Note: Search results are limited to the first 15,000 users found.


Basic Search

To search from the Users page:

1. Click the **Orgs and Users** tab.
2. Click the **Users** link.
3. Use the Choose Org list to choose an organization.
4. Enter a user address in the Find User form.



Find User Include: aliases sub-orgs

- Enter an entire address to find one user.
 - Enter the beginning of an address to find all users that *begin* with that character string.
 - Begin your entry with a % to find all users that *contain* that character string.
 - End your entry with a \$ to find all users that *end* with that character string.
 - See “Search Text Tips” on page 114 for details.
5. Click **Search**. Users that match your search appear in a resulting list. Click a user address to open its Overview page, or click the  icon to view its Quarantine.

Search from the Home Page

You can begin searching for users as soon as you log in to the Administration Console, using either the Search or User Shortcut form.

- **Search form** This is exactly like searching from User pages as described above under "Basic Search." Be sure the User option is selected.

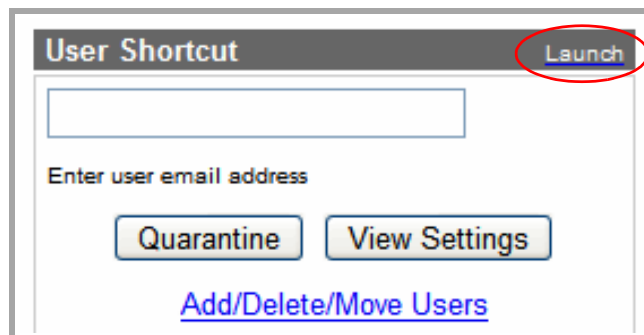
This search lists all users in the domain postqa7.com:



The screenshot shows a window titled "Search". Inside the window, there is a text input field containing "%postqa7.com". Below the input field, there is a line of text: "Default search is 'starts with.' For a 'contains' search, start query string with '%". Below this text, there are three radio buttons: "User" (which is selected), "Organization", and "Domain". At the bottom of the window, there is a "Search" button.

- **User Shortcut** This is also like searching from User pages, except entering a complete address allows you to then click **Quarantine** to view the user's Quarantine, or click **View Settings** to open the user's Overview page.

Click **Launch** to open the form in a pop-up window.



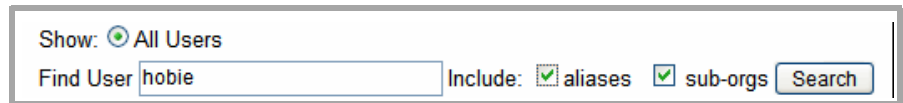
The screenshot shows a window titled "User Shortcut". In the top right corner of the window, there is a "Launch" button circled in red. Below the title bar, there is a text input field. Below the input field, there is a label "Enter user email address". Below the label, there are two buttons: "Quarantine" and "View Settings". At the bottom of the window, there is a blue hyperlink that says "Add/Delete/Move Users".

Refine Your Search

You can refine your search by specifying additional criteria on the Users and User Summaries pages. Note that all typing conventions described for a basic search apply for these searches, too.

- **Search for user aliases** Select the **aliases** check box.

This example shows how to find all users and user aliases, in the current org or its sub-orgs, beginning with “hobie”:



Search interface showing: Show: All Users. Find User: hobie. Include: aliases sub-orgs. Search button.

- **Search for a particular user’s aliases** On the User Summaries page, enter the user in the field above the Aliased To column, and select the **aliases** check box.

In this example, we find only aliases that belong to users beginning with “helen.”



Search interface showing: Find User: helen. Include: aliases sub-orgs. Search button. Below the search bar are columns: Users (0), Org, Aliased To, Spam, and several icons.

- **Confine your search to the current org** Clear the **sub-orgs** check box.

In this example, we find *users in the current organization only (no sub-orgs), that end with “postqa7.com.”*



Search interface showing: Show: All Users. Find User: postqa7.com\$. Include: aliases sub-orgs. Search button.

- **Confine your search to any org** On the User Summaries page, enter the organization in the field above the Org column. Optionally enter text in any of the other fields, too (results match *all* criteria).

In this example, we find *all addresses in orgs beginning with “postqa7” that are aliased to users whose addresses contain “sales”*



The screenshot shows a search interface with the following elements:

- Top left: "Show: All Users" with a radio button.
- Search input fields: The first is empty, the second contains "postqa7", and the third contains "%sales".
- Filters: "Include:" with checkboxes for "aliases" (checked) and "sub-orgs" (checked).
- Search button: A button labeled "Search".
- Bottom bar: A navigation bar with "Users (13)", "Org", "Aliased To", "Spam", and several icons.

Search Text Tips

When you search for users, you can enter a partial address as a shortcut or to narrow your search to users with similar addresses. You can do this in any search form on User pages or the Home page.

If you enter **jean**, for example, and only one user address begins with “jean,” you find that user. If more users begin with “jean,” you see a list of those users, and you can choose the one you want.

To find users whose address *contains* certain text but doesn't *begin* with it, enter the % character at the beginning. If you enter **%@jumboinc**, for example, you find all users whose address contains “@jumboinc.”

Similarly, enter the \$ character at the end of your text to find users whose address ends with the same address. If you enter **.org\$**, for example, you find all users belonging to a “.org” domain.

Tip: Use the techniques described here to list a subset of users, such as all users in a subdomain. If you enter **%@sales.jumboinc.com**, for example, you find all users in the subdomain “sales.jumboinc.com.”

Manage Default User Templates

A *Default User* is a template for new users in an organization. When a user is created, it receives org-level settings from its organization, and user-level settings, such as spam and virus blocking, from the org's Default User.

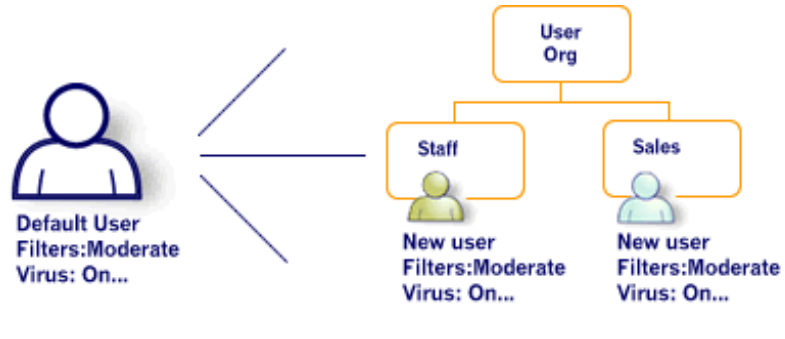
To effectively control settings for your users, we recommend the following:

- Configure the Spam Filtering setting at the Default-User level.
- Configure all other settings at the org level.
- Do not edit the Default User's User Access setting.

Note: You can customize settings for individual users. However, we highly recommend that you control settings at the org and Default-User levels rather than at the individual level. See below for details.

How Default Users Work

Initially, there is one Default User, **pdefault@yourdomain.com**, in your hierarchy. It resides in your top-level Account org. New users added to this org inherit the Default User's settings. In this default configuration, when you create sub-orgs, users in those orgs also inherit the Default User's settings.



Every org that contains users must be assigned a Default User. If you create sub-orgs, you can assign them the original Default User, or you can create additional Default Users to assign to those orgs. You can configure the settings for each Default User.

Default Users are listed under Users, and are searchable as are all your other users.



Note: Default Users (any user assigned as the default user for an org) are not counted towards billing.

Manage Default User Settings

WARNING: Before configuring a Default User, please see “Recommended Default User Settings,” below.


To configure Default User settings:







1. Locate the Default User under **Orgs and Users > Users**. For example, search for “pdefault” (see “Search for Users” on page 111).
2. Click the user name to open its Overview page.
3. Click the feature you want to modify, make your changes, and click **Save**. See below for recommended settings.




Recommended Default User Settings

Before configuring a Default User, please note:

- **Configure a Default User *before* assigning it to a hierarchy.** The configuration of a Default User only affects users as they are added to an org. Changes to the Default User do not affect users already in the org. If you reconfigure the Default User and want those settings to apply to existing users in the org, you must update each of those users’ settings separately, either one-by-one in the Administration Console, or by using Batch or EZCommands. See the “Message Center Examples” in the “Examples of Common Tasks” chapter in the *Batch Reference Guide*.
- **Changing a Default User’s settings affects *all* orgs to which that Default User is assigned.** If you want to have unique settings for an org, create a unique Default User and assign it to that org.
- **Do not use a Default User as an account for quarantine redirect or as a catchall account for a domain.** (Catchall account is a legacy feature that’s available to some customers.) The Default User is designed only as a configuration template and not intended for mail flow.
- **Don’t disable Message Center Access for a Default User.** Disable the Message Center at the org level, instead (see “Enable / Disable Message Center Access” on page 252). See below for other recommendations.

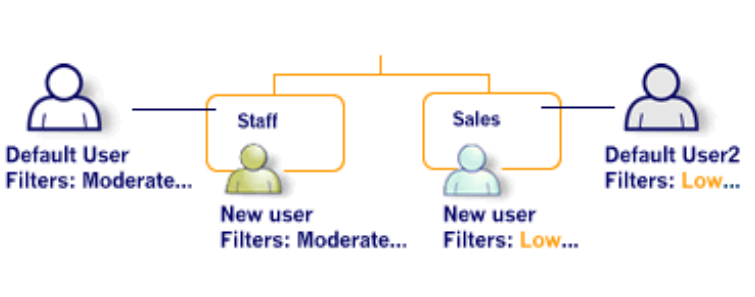
Default User Recommended Settings	
 Spam Filtering	Spam Filtering Filter Status: On Filter Sensitivity: Adjust levels as necessary. See “About Spam Filters” on page 293.

Default User Recommended Settings	
 Virus Blocking	<p>Virus Blocking: On</p> <p>Virus Notification Interval: Organization default.</p> <p>See “Configure Inbound Virus Blocking” on page 316.</p>
 Sender Lists	<p>Senders Lists</p> <p>Allowed or Blocked Senders Don’t add any senders to these lists. To apply common allowed or blocked senders across an org, use the org’s Sender Lists.</p> <p>Approved Recipients Optionally add any external mailing lists that should be approved for all users in the org.</p> <p>See “Approved and Blocked Sender Lists” on page 387.</p>
 Message Limits	<p>Message Limits: Leave the daily message limit blank. Set any desired message limit at the organization level. See “Set an Organization’s Message Limits” on page 93.</p>
 General Settings	<p>Wireless Forwarding: Off, or Not allowed.</p> <p>WARNING: <i>Do not</i> turn Wireless Forwarding On here. It should be turned on by individual users in the Message Center.</p> <p>See “User General Settings” on page 142.</p>
 Quarantine	<p>This is not a setting. Use this to manage the spam, virus-infected messages, or other filtered messages currently in the user’s Quarantine.</p>
 Aliases	<p>Not applicable for the Default User. Do not enter user aliases here.</p>

Default User Recommended Settings	
 <p>User Access</p>	<p>Message Center Access Enable this setting regardless of whether you want new users to access their Message Center. Disable Message Center access using the <i>org-level</i> User Access settings.</p> <p>Individual permissions Leave these check boxes unchanged. Set all permissions at the org-level, instead.</p> <p>See “About the Message Center” on page 247.</p>
 <p>Password</p>	<p>Not applicable for the Default User.</p>
 <p>Notifications</p>	<p>Notification Address: Enter an address here only if you intend for a single administrator to receive notifications for users in orgs using this Default User (not typical).</p> <p>Redirecting to a notification address affects all notifications. This includes spam and virus notifications, welcome notifications, and password changes.</p> <p>Otherwise, leave this field blank. See “Quarantine Summary & Notifications” on page 273.</p>

Create a Default User

To apply different user settings across an organization—say, to give the Sales org more lenient spam filtering than other orgs—create a new Default User, customize its filter levels, and assign it to the org.



Creating a Default User. The Sales org is assigned a new Default User with low filter levels. All other orgs continue using the original Default User, and get Moderate filter levels.

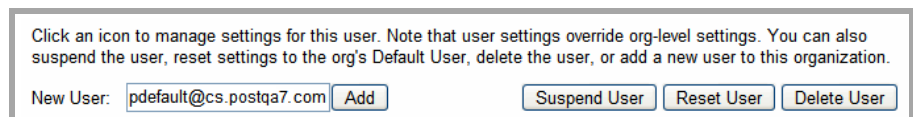
To create a new Default User:

1. Go to **Orgs and Users > Users**, and choose the organization where you want to create the new Default User.

Default Users don't send or receive mail, so they can reside in any organization. We suggest putting them in your Account org, which makes them easy to find later.

2. Click any user in that organization, such as a current Default User, to go to a User Overview page.
3. On the User Overview page, type an address for the new Default User in the New User form. For example:

pdefault@cs.postqa7.com
pdefault_sales@postqa7.com



4. Click **Add** to create the Default User and display its Overview page.
5. Configure the new Default User with your desired new-user settings. See "Recommended Default User Settings," above for important guidelines.

Note: Default Users do not count toward your billing. The initial instance of a user name that begins with **pdefault** or **postinidefault** is considered a Default User and is not counted toward your billing. Subsequent instances of those user names are counted toward your billing unless they are assigned to orgs as Default Users.

Assign a Default User to an Org

All organizations that contain users must be assigned a Default User. You do this on the org's General Settings page. You can assign the same Default User to multiple orgs. All new users created in an org receive its Default User settings. You cannot create users in an org that does not have a Default User.

Note: A user does not become a Default User for which you are not billed until you assign that user to an org. When you make that assignment, the Default User becomes a template for other users, and is removed from billing.

To assign a Default User to an org:

1. Go to the Management page for the organization to which you want to assign the Default User. For example, under Orgs and Users, locate the org in the list, and click it.
2. On the org's Management page, click **General Settings**.
3. On the General Settings page, enter the Default User's address in the Default User field, and click **Save**.

To remove a Default User from an org:

Clear the Default User field under General Settings, and click **Save**.

Do this only if the org is to contain no active users. You can clear several orgs' Default User assignments at once using a Batch File command. See the "Message Center Examples" in the "Examples of Common Tasks" chapter in the *Batch Reference Guide*.

Delete a Default User

If a Default User is no longer in use, you can delete it. Do this only if the Default User is not assigned to any organizations.

To delete a default user:

1. Remove the Default User from all orgs' General Settings.
2. Locate the Default User under Orgs and Users > Users, and click it.
3. On the Default User's Overview page, click **Delete User**.

Add / Delete / Move Users

You can use the Add/Delete/Move Users page to administer users quickly.

For information about each function, see the sections below.

Add Users

These steps explain how to add users to the service. After you add a user, the service filters that user's email.

Before You Begin

- If the new users' domain hasn't been added to the service, add it first (see "Add a Domain for Filtering" on page 236). Then come back here and add its users.
- If the users should have settings different from the org's default settings, create a new org for them and tailor its settings (see "Create an Organization" on page 91). Then come back here and add the users to the new org.
- These instructions explain how to add a small to medium-sized group of users all at once. If you have a large organization that frequently adds new users (more than two or three new users a week), consider configuring the service to add users automatically. See "Add Users Automatically to an Org" on page 126 for more information.

To add users:

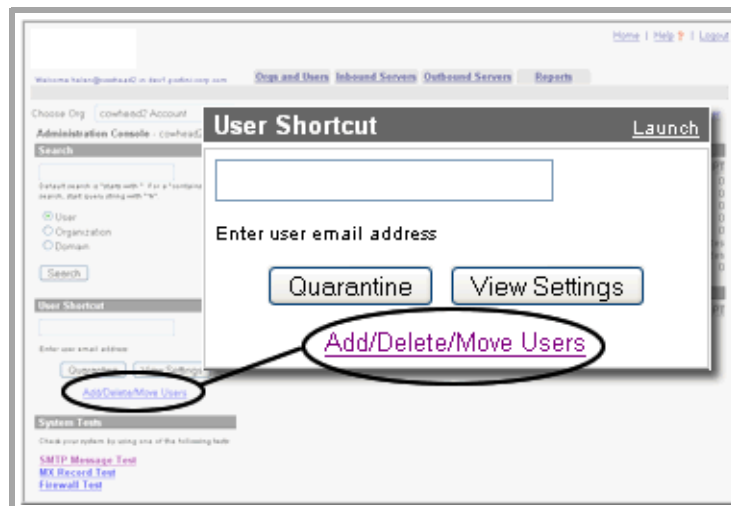
1. Log in to the Administration Console.

Log in to the Administration Console. You see the Welcome page.

If you are already logged in to the Administration Console, click the logo in the top left corner to see the Welcome page.

2. Click the Add/Delete/Move Users link.

On the Administration Console's **Home** page, click the **Add/Delete/Move Users** link, just above the System Test links.



The Add/Delete/Move Users page opens.



3. Enter your list of users.

On the **Add, Delete, and Move Users** page, enter addresses of one or more users for whom you want to filter messages. Separate addresses with a comma or put them on a separate line. Each user should already have an email account on your server.

Tip: Enter several users at once by pasting their addresses from a text file or user database.

Special characters: A user address can contain any ASCII character except following:

< > () [] \ ; : @ # = ,

Put a backslash (\) before any apostrophe (') or double quote (") characters. For example:

sara.o\'donnell@jumboinc.com

4. Choose settings (Optional).

You can modify new user behavior using the following controls:

Welcome users upon creation: If you plan to enable the users' Message Center, consider this setting.

Since a large number of welcome messages all at once might overwhelm some mail servers, the welcome messages are sent out over a span of about 24 hours by default. If you want to send them all immediately, select the "Welcome users upon creation" check box.

To this Organization: By default, new users are added to the same organization as the domain. This happens even if you clicked the Add Users link for a different organization. If you want to add the new users to a different organization, select the organization from the drop-down list. If you're not sure what organization to use, use the default.

5. Click Add Users.

Your users are now protected. Each new user receives service settings from its organization, and default filter levels from the org's Default User.

6. Add Aliases (Optional)

If your users have more than one address, such as `ben@jumboinc.com` and `benjamin_smith@jumboinc.com`, add each additional address as a *user alias*. You may also want to add mailing lists as an alias to a user that manages that list. See "Manage User Aliases" on page 140 for more information.

To add a user with a batch command:

1. On the Batch Upload page, in the Manual Input field, enter the following command for the user you want to purge:

```
adduser <email address>, org=<org name>
```

2. Click **Submit Job**.

You can add multiple users by using a batch file. For more information, see:

Batch Reference Guide

Delete Users

When users no longer need email protection, you should delete them from the service so you're no longer billed for those users.

After the user is deleted, subsequent messages sent to that address are bounced or delivered without filtering, depending on how you've configured Non-Account Bouncing (see "Organization General Settings" on page 94).

Deleting a user permanently deletes its Quarantine and all messages in it. Before deleting a user, you might want to review the Quarantine and deliver any potentially legitimate messages to the user's Inbox.

When you delete a user via the Administration Console, that user is considered *deactivated* for a period of time equal to its quarantine period (for example, 14 days). While the user is considered deactivated, you can add the user back to the service. If you have Message Discovery, then all messages for that user (before and after deactivation, and including quarantined messages) are available in the same Personal Archive.

Note: If you add back a user during the deactivation period, specify the org to which you are adding the user. Specifying the org lets you avoid errors associated with the user's original org no longer existing or with the user's original domain having been moved to another org.

To add a user and specify the org, you can use the Batch Upload page to issue the following command:

```
adduser <email address>, org=<org name>
```

For instructions, see "To add a user with a batch command:" on page 123.

After a time equal to the quarantine period has passed, the user data is fully deleted from the service. If you add that same user back to the service after it has been fully deleted, it is considered a new user. If you have Message Discovery, the user has a new Personal Archive; messages to the first instance of that user are not available in the new Personal Archive.

If you want to completely purge a user from the system without having to wait for the deactivation period to expire, you can use the Batch Upload page to issue the following command:

```
deleteuser <email address>, purge
```

For instructions, see "To purge a user with a batch command:" on page 124.

Note: If you delete a user without using the `purge` argument, you cannot subsequently purge that same user. To purge a user under these circumstances, you need to add back that user, and then delete it with the `purge` argument.

To delete users:

1. On the Add, Delete, and Move Users page, enter one or more user addresses to delete. Separate multiple addresses with a comma or line break.

2. Click **Delete Users**.

You are not prompted for confirmation.

You can also delete a user from its User Overview page by clicking **Delete User**.

Note: You can't delete a Default User if it's currently assigned to an organization. See "Delete a Default User" on page 120 for more information.

To purge a user with a batch command:

1. On the Batch Upload page, in the Manual Input field, enter the following command for the user you want to purge:


```
deleteuser <email address>, purge
```

2. Click **Submit Job**.

You can purge multiple users by using a batch file. For more information, see:

Batch Reference Guide

When a User Leaves Your Organization

If a user has left your organization, you have some options other than immediately deleting that user from the service. Depending upon your company's policy, you can either:

- Change the user name into an alias owned by a manager. The email can be reviewed. See "Add a User Alias" on page 141 for more information.
- Create a user called "terminations" with the daily message limit set to zero. Then add the former user as an alias to the terminations user. The mail is then bounced, and your former users are grouped in one place.
- Set a former user's daily message limit to zero if aliasing former users under a terminated user is not necessary. With the message limit set to zero, all that user's mail is then bounced, without ever reaching your server.

Also, if you're using Automatic Account Creation to add users automatically, subsequent messages to a deleted user can cause that user to be added again, as a *provisional* user. To prevent this from happening repeatedly, locate the user when re-created, under Provisional Users, and block the user from being added again.

Move Users

After adding users to a particular organization, you might subsequently want to move them to another org. For example, you might decide to split the New York org into two sub-orgs: Uptown and Downtown. After creating the sub-orgs, you need to move users from the New York org to the Uptown or Downtown orgs.

To move users:

1. On the Add, Delete, and Move Users page, enter one or more user addresses to move. Separate multiple addresses with a comma or line break.
2. Choose the organization to which you want to move the users. Select the org from the list or enter its name.
3. Click **Move**.

Users retain their existing user-level settings, but acquire new org-level settings from their new organization.

To move a single user, you can also go to General Settings on the user's Overview page, and enter a new parent organization for the user. See "User General Settings" on page 142.

Add Users Automatically to an Org

The service offers a number of different ways to automatically add users:

Automatic Account Creation	Add users when they receive valid mail. Requires mail servers that bounce mail asynchronously, such as Microsoft Exchange or Qmail.
Directory Sync	Synchronize with the user list in your LDAP Directory.
Batch processing	Add users programmatically.

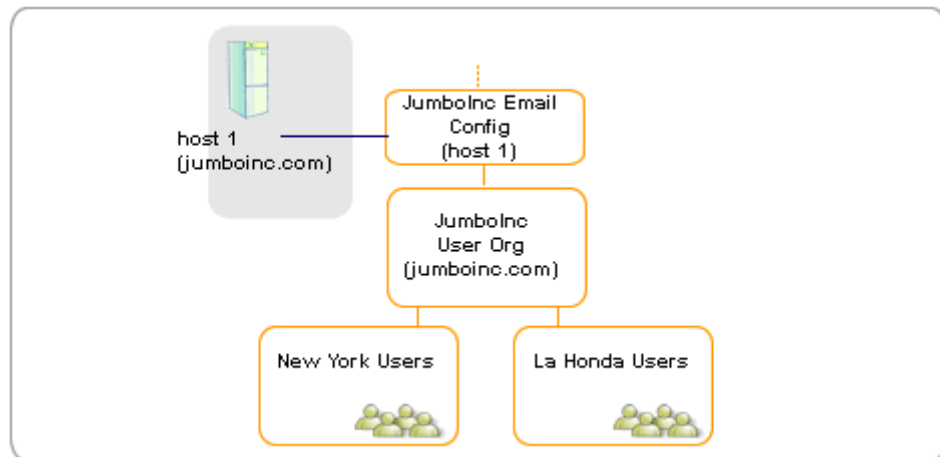
Each method is described in detail below.

Automatic Account Creation

Automatic Account Creation automatically adds a user to the service when within a span of two weeks, three valid messages are received for that user's address.

Considerations:

- Automatic Account Creation automatically creates users for mail sent to valid addresses, including both primary addresses and aliases. You may consider turning on domain aliasing or domain substripping (if applicable) to avoid the creation of multiple user accounts.
- Automatic Account Creation adds users to the organization that contains the domain of the email address. So if your domain is one org and your users are another, Automatic Account Creation may not be the best method. In the example below, if Automatic Account Creation is turned on for the domain jumboinc.com, users are added to the JumboInc User Org.



Advantages

- You can use Automatic Account Creation with any mail server, including servers which bounce mail asynchronously such as Microsoft Exchange.
- Best suited for small organizations with simpler hierarchy structures.

See “Add Users Automatically (Automatic Account Creation)” on page 129 for more information.

Directory Sync

Note: This section describes Directory Sync Hosted Edition, which is set in the Administration Console and pulls data from your server using DSML. If you are interested in the Directory Sync Server Edition utility, which runs on your server and pushes data to the service, see the following URL:

http://www.postini.com/dir_sync

Directory Sync makes user management easier by connecting to your LDAP directory server and collecting user information. Directory Sync imports this information into the service. It adds, deletes or moves users so that your organization matches an *organizational unit* (OU) on your directory server.

Directory Sync acts as a one-way synchronization. Your user and alias information in the service may be added, moved or deleted, but your directory server is not changed in any way. Directory Sync can be launched manually from the Administration Console or scheduled to run automatically.

Considerations

- To use Directory Sync, you'll need to set up DSML with SSL on an internet-facing machine and possibly perform some configuration on your LDAP directory server and the service.
- Directory Sync is offered for certain LDAP directories. See the “About Directory Sync” on page 205 for Directory Sync requirements.

Advantages

- Directory Sync adds, deletes, and moves users and aliases based on your LDAP directory, automating user management.
- Directory Sync can be scheduled to synchronize automatically on a regular schedule.
- Directory Sync is useful for large organizations with complex organization hierarchies and a dynamic user base.

See “About Directory Sync” on page 205 for more information.

Batch Commands

Batch processing is a quick and efficient method to perform a large number of configuration changes by creating, validating and running command scripts in real-time.

You can run batch commands in the Administration Console to create, delete, and modify users and organizations.

You can also use EZCommand, a Perl-based scripting interface that allows administrators to perform basic tasks without having to log in to the Administration Console.

Considerations

- Some familiarity with scripting or programming is helpful.
- EZCommand requires expertise with Perl and the ability to debug and troubleshoot your own scripts.

Advantages

- Useful for mass-user or organization operations.
- Can be integrated with your management tools.

For more information, see the *Batch Reference Guide*

Enable Web Autocreate

You enable Web Autocreate for a domain by configuring the domain's organization. This means that other domains associated with the org must use this feature, too.

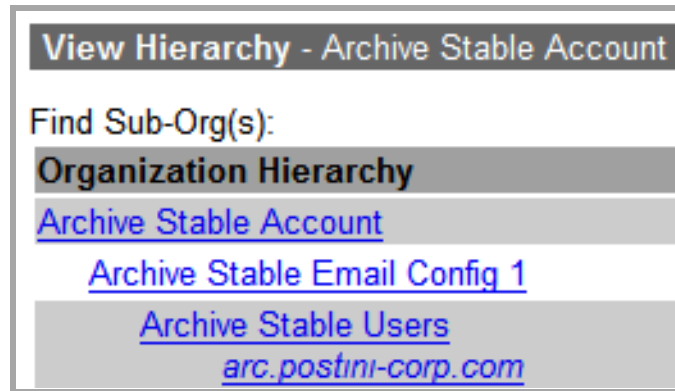
1. If the domain isn't already added to the service, add it now (see "Add a Domain for Filtering" on page 236). Associate it with the org whose users you want to add. This org must be somewhere below the email config mapped to the domain's server (see "Hierarchy Requirements & Configurations" on page 63).

Associate the domain with a user-org, not an email config. SMTP or Web Autocreate won't add users to an email config.

2. Go to General Settings for the associated org.

Tip: To find a domain's org, click the View Hierarchy w/Domains link under Orgs and Users > Orgs, and locate the domain in the list.

In this example, the domain arc.postini-corp.com is associated with the Archive Stable Users org.



You can also locate the domain under Orgs and Users > Domains. Then click the domain, and the domain's Organization Name is displayed.

3. On the org's General Settings page,
 - Turn Web Autocreate On.
 - Turn Non-Account Bouncing Off.
4. Click **Save** when you're done.

Tip: After enabling Web Autocreate, send a message to users requesting that they log in to the Message Center to activate their own spam filtering accounts.

Add Users Automatically (Automatic Account Creation)

If your account has the Automatic Account Creation feature enabled, users in your domains are added automatically to the service after they receive valid messages.

To add users automatically using Automatic Account Creation:

1. Under Domains on the Orgs & Users tab, add the domains whose users should be added automatically (see "Add a Domain for Filtering" on page 236).
2. Under General Settings on the Orgs & Users tab:
 - Turn Automatic Account Creation On.
 - Turn Non-Account Bouncing Off. Automatic Account Creation is not compatible with Non-Account Bouncing.

WARNING: If a user receives email at more than one address (via a *user alias*), add the additional addresses to the user's Aliases page. Otherwise, Automatic Account Creation adds new users for these aliases, and you will be billed for those new users. See "Manage User Aliases" on page 140.

How Automatic Account Creation Works

When, in the span of two weeks, three valid messages arrive for an address not registered in the service, Automatic Account Creation creates the user. Automatic Account Creation sends a welcome message and begins filtering email for that address. The domain must be registered in the service.

Automatic Account Creation considers a message valid only if it meets all of these conditions:

- Has no more than a single unregistered recipient.
- Accepted by the receiving server.
- Definitely not spam (score is over 50).
- Not infected with a virus.
- Not a message refusal from another server.

At first, a newly added user is an unconfirmed *provisional user*. The user is promoted to a regular user when they receive at least three valid messages within two weeks. This prevents bad user addresses from being added to the service and appearing on your bill. Once a provisional user meets this criteria, the user is added to the service and appears on the Users tab.

Mail to provisional users is delivered and not filtered until the user has received three valid messages. If the provisional user does not receive three legitimate messages within two weeks of creation, the provisional user is deleted.

You can use Automatic Account Creation with any mail server, including servers that bounce mail asynchronously, such as Microsoft Exchange. To enable Automatic Account Creation, set Automatic Account Creation to On in General Settings for your domain organization.

When a domain alias (or domain substripping) is enabled, Automatic Account Creation adds users in the primary domain, not in the alias domain. For more information about domain aliases, see "Add a Domain Alias" on page 239.

Promote / Delete / Block Provisional Users

A provisional user (created via Automatic Account Creation) automatically either becomes a regular user or is deleted within two weeks, depending on whether the user is validated as someone in your organization. To override this process or speed it up, manage provisional users yourself by clicking the **Provisional Users** link on the Users page.

To promote, delete, or block a provisional user:

1. On the Provisional Users page, optionally view only unblocked or blocked provisional users, by clicking the **Unblocked Only** or **Blocked Only** link at the top of the page (click **All** to go back to listing all provisional users).

Note: Active indicates that a user is still eligible to become a regular user, while Blocked indicates a permanently blocked user.

2. For one or more users, select one of the following actions:
 - **Promote:** Promote a provisional user that you know is legitimate.
 - **Delete:** Delete a provisional user that is known to be illegitimate. It won't appear on your bill.
 - **Block:** Permanently block a provisional user from being added via Automatic Account Creation in the future. Do this for users for whom you don't want to provide email protection, such as a user who has left your company but continues to receive email.
3. Click **Save**.

Mail to provisional users is delivered unfiltered.

Manage a User's Settings

You can manage a user's individual settings and Quarantine from the user's Overview page.

WARNING: Many user-level settings are best made at the org-level where they apply to all users in the org, or to only the default user. See "Manage Default User Templates" on page 114 and "What Settings Are Made Where" on page 73.

To view an individual user's settings:








- Click a user address on the Users or User Summaries page, or
- Perform a search from the Home page, using the View Settings button (see "Search for Users" on page 111).

User Overview - adamico@arc.postini-corp.com

Click an icon to manage settings for this user. Note that user settings override org-level settings. Y

New User:

Inbound Services

 Spam Filtering	Filter: Off	Filter Levels:  1,  1,  1,  1,  1
 Virus Blocking	Filter: On	Notification Interval: Organization default

The User Overview page shows settings for the user named at the top of the page. Click a feature to manage it for that user.



You can modify several users at once using a Batch File or EZCommand. See the “Building a Batch File” section of the “Introduction to Batch Processing” chapter of the *Batch Reference Guide*.



Suspend, Reset, or Delete a User

On the User Overview page, you can:



- **Suspend a User:** Stops all filtering and protection for the user, but retains the user’s settings and account information in the service. See “Suspend a User” on page 148 for details.
- **Reset a User:** Sets the user’s settings to the Default User’s settings. See “Reset a User” on page 149 for details.
- **Delete a User:** Stops all filtering and protection for the user, and deletes all of that user’s information from the service. See “Delete Users” on page 123 and “When a User Leaves Your Organization” on page 125 for more information.

Inbound Services

Inbound Services Overview	
 Spam Filtering	<p>Spam Filtering: Enable/disable spam filtering for this user.</p> <p>Adjust sensitivity for filtering spam (Bulk Email)</p> <p>Optionally, set levels for filtering specific categories of spam even more aggressively.</p> <p>See “Enable and Adjust Spam Filters” on page 301.</p>
 Virus Blocking	<p>Virus Blocking: Enable/disable virus blocking for this user.</p> <p>Set how frequently to send this user a Virus notification. Organization Default uses the setting defined for the user’s organization (recommended).</p> <p>See “Virus Notification Interval” on page 317.</p>

Inbound Services Overview	
 <p>Sender Lists</p>	<p>Senders Lists: Manage approved and blocked senders for this user. These apply in addition to those defined for the user’s organization.</p> <p>Enter addresses, such as mailing lists, from which this user should always receive mail (Approved Recipients). The user receives messages regardless of spam-like content.</p> <p>See “ Approved and Blocked Sender Lists” on page 387.</p>
 <p>Message Limits</p>	<p>Message Limits: Track how many messages this user receives for the current day.</p> <p>In general, we recommend leaving blank the daily message limit for a user. Set any desired message limit at the organization level.</p> <p>You can enter 0 to block all messages for this user (useful when a user has left the company.) For details, see “Set an Organization’s Message Limits” on page 93.</p>

User Settings

User Settings Overview	
 <p>Quarantine</p>	<p>Quarantine: Manage the spam, virus-infected messages, or other filtered messages currently in the user’s Quarantine.</p>
 <p>General Settings</p>	<p>General Settings: View the user’s primary email address, user ID, organization, creation date, and wireless settings. You can also change the user’s primary address here, or assign the user to a different org.</p> <p>See “User General Settings” on page 142.</p>

User Settings Overview



User Access

User Access: View which settings this user has permission to view or modify in the Message Center. These settings are defined at the org-level, but you can change them here for an individual user.

WARNING: If you change a user's settings here, you cannot then manage them at the org-level. To maintain the same user access settings across an org, we highly recommend you make no changes here, but manage all user access at the org-level.

See "About the Message Center" on page 247.



Aliases

Aliases: If a user receives email at more than one address (such as jonathan@jumboinc.com and john@jumboinc.com), add the additional addresses here as *user aliases*. See "Manage User Aliases" on page 140.



Password


Initial Password Shows the password assigned to this user when it was first added to the service, or indicates that the password has been changed. Users are prompted to set a new password when they first log in to the Message Center, so you can find out here whether the user has done so.

Reset Password Allows assigning this user a new, temporary password. The user needs this password to access the Message Center (or the Administration Console if the user is an administrator). From this page, an administrator can choose to send a notification to the user when the password is reset.

Requirements The password requirements are determined by the administrator through settings on the organization password policies page. These requirements are displayed on the User Password page for reference. For information about setting password requirements for users, see "Set User Password Policies" on page 144.

For information about resetting a user's password, see "Reset a User's Password" on page 145.

See also "PMP Authentication" on page 615.

User Settings Overview	
 Notifications	<p>See whether the user has ever logged in to the Message Center, or received a Welcome notification (sent when the user is first added to the service).</p> <p>You can also specify the address to which the user's notifications are sent. Normally this is the user's primary address. However, if an administrator is managing the user's service, you can add the administrator's address here. See "Quarantine Summary & Notifications" on page 273.</p>

Summary

The Summary box (to the right of Inbound Services) contains the following information:

Summary Overview	
User ID	A unique ID for this user, useful when escalating an issue to Customer Care. A user's primary email address can be changed, but its ID always remains the same.
Organization	The user's organization. Click the link to go to that org's Management page.
Creation Date	The date the user was added to the service.
Quarantine Status	Indicates whether any new messages have been quarantined since the user last logged in to the Message Center. Click the link to view the quarantine.
Active	Yes/No, indicating whether the user has ever logged in to the Message Center.

Manage Quarantined Messages

Users > User Overview >  Quarantine

Incoming messages filtered as spam or otherwise diverted from delivery to a user, can be placed in a Quarantine where administrators can go to review and manage them. You can quarantine each user's suspicious messages in a separate User Quarantine. Or you can set up a central Quarantine for collecting all users' quarantined messages.

From a Quarantine, you can:

- Review and safely open quarantined messages for analysis.
- Find messages based on sender, subject, or content.
- Deliver legitimate messages to the user.
- Deliver messages you want to review further to your own administrator account.
- Delete messages.

Note: Users with the appropriate User Access permissions can view and manage their own quarantined messages at the Message Center. See "About the Message Center" on page 247 for details.

Enable User Quarantines

You can quarantine messages caught by Content Manager filters, spam filters, and virus blocking in individual User Quarantines by setting the filter's *disposition* to User Quarantine.

You can also use different dispositions for different filters. For example, you might quarantine each user's spam (by setting the spam disposition to User Quarantine), but have viruses deleted (by settings the virus disposition to Delete).

To set dispositions, see:

- "Enable and Adjust Spam Filters" on page 301
- "Configure Inbound Virus Blocking" on page 316
- "Create or Edit a Content Manager Filter" on page 340
- "Create / Edit Attachment Manager Filters" on page 409

Quarantine Messages Centrally

Instead of quarantining each user's suspicious messages separately, you can collect all users' prohibited content, spam or viruses in a central Quarantine. To do so, set the spam or virus disposition to Quarantine Redirect, or configure Content Manager filters to copy messages to a specific quarantine. In each case, you supply a user address whose Quarantine you want to use. You can then access the central Quarantine, sort messages, and delete and deliver messages, as described below for any Quarantine.


You can also quarantine messages caught by Attachment Manager filters in a central quarantine. Do this by setting the Attachment Manager filter's disposition to Quarantine or BCC Quarantine.

To set dispositions, see:

- "Enable and Adjust Spam Filters" on page 301
- "Configure Inbound Virus Blocking" on page 316
- "Create or Edit a Content Manager Filter" on page 340
- "Create / Edit Attachment Manager Filters" on page 409

Access a Quarantine

You can get to a user's Quarantine in the following ways:

- From the Home page: Perform a search under User Shortcut, then click **Quarantine**.
- From a user list on the Users tab: Locate the user in the list and click .
- From the user's Overview page: Under Settings, click **Quarantine**.
- From the user's Overview page: In the User Summary area, click **View Quarantine**.

Display Quarantined Messages

To manage large numbers of quarantined messages, you can filter and sort the display by recipient or sender address, subject text, or the filter that quarantined the messages. You can also view messages that have been recently deleted or delivered.

Note: A User Quarantine displays the 5,000 most-recent messages. If more than 5,000 messages are quarantined, you need to deliver or delete some of the newer ones to see the older ones.

To manage the display of quarantined messages:

1. In the form above the list of quarantined messages, choose the number of messages to display per page.

2. Select the type of quarantined traffic you want to view:
 - **All:** Messages that are currently quarantined, messages that were quarantined and delivered, and messages that were quarantined and deleted.
 - **Quarantined:** Messages that are currently quarantined.
 - **Delivered:** Messages recently delivered from the Quarantine to the user or an administrator (if they were delivered with the “Marked as delivered” option). Copies of these are kept for three days, and then deleted.
 - **Trashed:** Messages recently deleted from the Quarantine (copies of these are kept for three days, and then deleted).
3. To view messages based on recipient/sender address or subject, enter text in the fields above the column headings.

For example, if you enter **mortgage** in the Subject field, all messages whose subject includes “mortgage” are displayed.

To find messages based on the filter that quarantined them, choose an option from the list above the Filter column (see below for a description of these options).

If you apply multiple criteria, messages are displayed that meet all criteria.
4. After supplying your criteria, click **Apply** to display the matching messages.

Options for sorting messages by filter

All	Show all messages.
Attachment Mgr	Attachment Manager filter (optional feature not available with some service packages)
Attachment Mgr BCC	Attachment Manager BCC filter (optional feature not available with some service packages)
Bulk spam	The base-level spam category filter (may include characteristics of the other spam filters).
Content Mgr	Content Manager filter (optional feature)
Content Mgr BCC	Content Manager BCC filter (optional feature)
Early Detection (Pending)	Early Detection filter
Get Rich Quick	Get Rich Quick spam filter
OB Attachment Mgr	Outbound Attachment Manager filter (optional feature)
OB Attachment Mgr BCC	Outbound Attachment Manager BCC filter (optional feature)
OB Connection Block	Outbound Connection Block filter (optional feature)
OB Content Mgr	Outbound Content Manager filter (optional feature)
OB Content Mgr BCC	Outbound Content Manager BCC filter (optional feature)

OB Virus	Outbound virus blocking (optional feature)
Org Blocked Sender	Sender is on the org's Blocked Senders list
Racial	Racially insensitive spam filter
Sexually Explicit	Adult content spam filter
Special Offer	Special Offers spam filter
Undeliverable Bounce	Outbound undeliverable bounce messages (optional feature)
User Blocked Sender	Sender is on the user's Blocked Senders list
Virus	Virus blocking (message contained a virus)

Tip: Click a column heading to sort the messages by that heading.

Open Quarantined Messages

You can safely view the content of any message in the User Quarantine, regardless of its content, by clicking the subject link. All scripting is blocked, so you can't unleash a virus. However, images encoded in the message's HTML are loaded from the sender's remote server. Depending on the sender, this might send an indication to the spammer that the message has been read and therefore has a valid recipient, resulting in more spam from the same sender.

Deliver or Delete Quarantined Messages

A User Quarantine can collect thousands of messages. To stay ahead of accumulating spam, you should process messages regularly by deleting them, delivering them to the user, or delivering them to an administrator account.

Note:

- Quarantined messages are held for 14 days from the date received, or for 3 days after they are deleted or delivered, whichever comes first. After that, messages are deleted automatically.
- If a user's quarantine contains over 10,000 messages, the Delete All button is automatically removed from the Junk, Virus, Trash, and Delivered tabs in Message Center. In this case, you delete only selected messages (up to 250 at a time) on a tab, instead of all messages at once.

To delete or deliver quarantined messages:

1. On the User Quarantine page, select the check box for each message you want to delete or deliver.
2. To delete the selected messages, click **Delete**.

3. To deliver the selected messages, select an option:
 - **Deliver to original recipient:** Delivers selected messages to the user to whom they were originally sent.
 - **Deliver to administrator:** Delivers selected messages to your administrator account (the account currently logged in to the Administration Console).

Also select any of these options:

- **Mark as delivered:** The message is tagged as “delivered” and kept in the quarantine for a few days before being automatically deleted (helpful for tracking message delivery).
 - **Virus clean before delivering:** Messages with a detected virus embedded in valid content (such as a document attachment) are cleansed and delivered virus-free.
4. Click **Process** to deliver all selected messages as specified above.

Manage User Aliases

Users > User Overview >  Aliases

Sometimes users have more than one address they use to receive email. For example, john@jumboinc.com might like to receive email from friends using his alias address spoonman@jumboinc.com, and from external clients using the more formal jonathan_smith@jumboinc.com. Since messages to all three addresses go to the same person, they should be filtered the same way, and share the same User Quarantine.

To associate an additional address with a user so it receives the same filtering and uses the same Quarantine, add a *user alias*. Do this on the user’s Aliases page.

Note: Users with appropriate Message Center access can manage their own user aliases. See “Control What Users Can View and Modify” on page 255.

WARNING: If Automatic Account Creation is enabled, users' alias addresses can potentially be added automatically to the service as independent users. To prevent this from happening, add the user aliases before enabling Automatic Account Creation.

When User Aliases Aren't Necessary

User aliases are typically necessary only for users with personal aliases that apply only for themselves. If a group of users has addresses in other domains or subdomains, one of the following methods of aliasing is probably more appropriate:

- **Domain Alias** If users in a domain also have addresses in another domain, for example, if *users@jumboinc.com* have addresses in *users@jumboinc.net*, you might want to add *jumboinc.net* as a *domain alias*, instead of adding individual user aliases. See "Add a Domain Alias" on page 239.
- **Subdomain Stripping** Similarly, if some users in a domain also have addresses in a subdomain, for example, if *users@jumboinc.com* have addresses in *users@sales.jumboinc.com*, set up *domain stripping* for that domain, instead of adding individual user aliases. See "Subdomain Stripping" on page 240.
- **Catchall Account** This is a legacy feature that is available to some customers. If one user receives all traffic for an entire domain, configure a *catchall account* for that domain. See "Add a Catchall Account (Legacy Feature)" on page 241.

Add a User Alias

To add a user alias:

1. Locate the user to which you want to add the alias, for example, by clicking a user address under Orgs and Users > Users, or by performing a user search.
2. On the user's Aliases page, enter the alias address in the Aliases field, then click **Add**.

To enter multiple aliases, enter a comma-separated list of addresses in the Alias field, then click **Add**.

When you add an alias through the Administration Console, the email address is not checked against your mail server's user list, so it's possible to add any address at a domain you've configured in the message service. Be sure your alias addresses are valid and have corresponding email accounts on your mail server.

3. If the alias you add has already been added as a separate, primary user, you are asked whether you want to merge the two accounts. Click **Confirm** to merge the accounts. This automatically converts the primary address to an alias.

You can only add an alias address for a domain under the same Email Config organization as the user. If you try to add an alias address for a domain that is not listed in the same Email Config organization, you get an error:

```
We can't create an alias for domain.com: Differing mail host
```

You can locate an alias by performing a search on the Users tab (see “Search for Users” on page 111). When you click the alias or the Quarantine icon in the search results, you go to the Overview or Quarantine of the primary user.

You can add several user aliases at once using a Batch File or EZCommand. See the “Building a Batch File” section of the “Introduction to Batch Processing” chapter of the *Batch Reference Guide*.

Remove a User Alias

To remove a user alias:

Go to the user’s Aliases page, select the alias you want to remove, then click **Remove**.

Removing a user alias deletes it completely from the message service.

View User Aliases

To view user aliases:

1. Go to **Orgs & Users > Users**.
2. Select the **Include: aliases** check box, and enter any search criteria. Aliases are listed in italics.

User General Settings

[Users > User Overview >](#)  [General Settings](#)

Under General Setting on a user’s Overview page, you can manage the user’s primary address and organization, reference its ID, and view its Wireless Forwarding settings.

Configure the settings as described below, then click **Save** when you have finished.

User General Settings	
Primary Address	The user's primary email address (as opposed to any user aliases it might have). You can enter a new address here.
User ID	A unique ID for this user, useful when escalating an issue to Customer Care. A user's primary email address can be changed, but its ID always remains the same.
Organization Name	The user's organization. Enter another org to move the user to that org. See "Add / Delete / Move Users" on page 120.
Creation Date	The date the user was added to the service.
Wireless Forwarding	<p>Note: This is a legacy feature available only with Message Center Classic.</p> <p>Indicates whether Wireless Forwarding is allowed, and if so, whether this user has it enabled. Wireless Forwarding allows the user to forward messages to a text-enabled phone, PDA, or other mobile device.</p> <p>The setting is available in the Message Center if the user has the proper User Access permissions (see "Control What Users Can View and Modify" on page 255).</p> <p>On Wireless Forwarding is available for the user, who has turned the feature on at the Message Center.</p> <p>Off Wireless Forwarding is available for the user, but the user has not turned it on.</p> <p>Not allowed Wireless Forwarding is not available for this user. Wireless settings do not appear in the user's Message Center, even if the user has the proper User Access settings.</p> <p>WARNING: Do not change this setting here except to choose Not allowed. If Wireless Forwarding is allowed, users should turn the feature on or off themselves in the Message Center.</p>
Time Zone	<p>Applies only if Wireless Forwarding is enabled for the user.</p> <p>The time zone selected by the user for scheduling <i>quiet times</i> when messages should not be forwarded to the user's mobile device.</p> <p>WARNING: Do not change this setting here. It should instead be managed by users themselves in the Message Center.</p>

Set User Password Policies

Orgs > Organization Management >  Password Policies

Under Password Policies on the Organization Management page, you can manage and configure password policies for all users in an organization, including Length, Complexity, Maximum Age, History, and Lockout Threshold.

Notes:

- Default password policies for administrators are more complex. For information on minimum requirements for administrator passwords, see “Administrator Passwords” on page 50.
- When users are moved to an organization that has a different password policy than their previous organization, they are not required to change their current passwords and adhere to the new org's password policy. Also, when the password policy of an organization is changed to be more complex, existing users are not required to change their current passwords to meet the new complexity requirements.

Set the policies as described below, then click **Save** when you have finished.

Organization Password Policies	
Length	Require passwords to have a minimum number of characters (1 to 10). Note: For customers who began with the email protection service before May 2007, the default is 1 for both users and administrators. For customers who began with the service May 2007 and later, the default is 6.

Organization Password Policies	
Complexity	<p>When you require complex passwords (Yes or No), passwords cannot match English dictionary words or the user's email address, and they must contain a combination of at least three of the following four character types:</p> <ul style="list-style-type: none"> • English uppercase letters (A through Z) • English lowercase letters (a through z) • Numbers (0 through 9) • Symbols (such as !, #, \$, %) <p>Note: For customers who began with the email protection service before May 2007, the default is NO for both users and administrators. For customers who began with the service May 2007 and later, the default is YES.</p>
Maximum Age	<p>Passwords <i>Never</i> expire, or they expire after this many days (1 through 999). When this policy is set, a user is required to change the password upon next login.</p>
History	<p>Users can <i>Always</i> reuse passwords, or users can reuse passwords after a specified number of password versions have elapsed (1 through 24).</p>
Lockout Threshold	<p>Lock out users for failed login attempts "Never" or after a set number of login attempts (1 to 10).</p> <p>Set the lockout to end after a specified number of minutes (1 through 999), or when an administrator resets the password.</p>

You can also use a batch command to display the password policy for an organization. Additionally, you can create a password policy for a new organization or update the password policy for an existing organization. See the "password_policy display" and "password_policy update" commands in the "Commands" chapter of the *Batch Reference Guide*.

Reset a User's Password

To reset a user's password:

1. In the Administration Console, click the **Orgs and Users** tab.
2. Click the **Users** link.
3. Click the user to open the User Overview page.

4. In the Settings section, click the **Password** icon.

See the description of the User Password page below for information about how to set passwords.

5. Click **Save** when you are finished.

User Password Page

Initial Password: Shows the password assigned to this user when it was first added to the service, or indicates that the password has been changed. Users are prompted to set a new password when they first log in to the Message Center, so you can find out here whether the user has done so.

Reset Password: Allows assigning this user a new, temporary password. The user needs this password to access the Message Center (or the Administration Console, for an administrator). From this page, an administrator can choose to send a notification to the user when the password is reset.

Replacing the password with a *temporary value* automatically generates a 6-character password that meets complexity requirements, and sends a notification to the user that the password has been changed. Users must then change this password when they log in. If you manually choose a temporary password for this user, the password must meet the requirements listed at the bottom of the page.

Requirements: The password requirements are determined by the administrator through settings on the organization password policies page. These requirements will be displayed on the User Password page for reference. For information about setting password requirements for users, see “Set User Password Policies” on page 144.

These settings are used with an organization using the PMP password policy configuration. See “PMP Authentication” on page 615.

User Password - admin@arc.in.dev1.postini-corp.com

To reset the password for this user, generate a new temporary password and send a notification to the user.

Initial Password (This password has been changed.)

Reset Password Reset the password for this user and send a notification with the new password

Replace password with temporary value and notify user

Reset temporary password to

Notify user

Requirements

- Contain at least 6 characters
- Not be a dictionary word
- Not be your email address
- Contain 3 of the 4 character types: English uppercase letters, English lowercase letters, numbers, and symbols (such as !, #, \$, %)

You can also use a batch command to force one user or all users in an organization to change their passwords the next time they log into the system. Additionally, you can use a batch command to reset a user's password. See the "password force_update" and "password reset" commands in the "Commands" chapter of the *Batch Reference Guide*.

Protect Your Mailing and Distribution Lists

You can protect mailing and distribution lists from spam and viruses. These lists are addresses that deliver a message from outside your network to a group of people in your domain, such as `partners@your_domain.com`, or `noon_cyclers@your_domain.com`. Often, when users complain about spam passing through, they are receiving the spam through their membership in a mailing list.

To protect a mailing list from spam and viruses, alias the mailing list to an existing or new user account.

WARNING: Do not add the mailing list as a user account. Under these circumstances, the mailing list is treated as a user, and all members of the mailing list, including those outside of your organization, receive the notifications and quarantine summaries.

You have two options to protect mailing lists:

- Alias the mailing list to an existing user, such as an administrator or the designated owner of the mailing list.

Considerations: The mailing list receives the same settings as the user—spam filters, approved and blocked senders, etc.—which may or may not be appropriate for the mailing list.

- Create a new user account for the mailing list and alias the mailing list address to this account. You can choose to send the notifications to the designated owner of mailing list.

Considerations: The advantage of this method is that you can specify the filter settings for the mailing list. However, this is another user account to manage.

To alias the mailing list to an existing user:

1. Select the user in the Administration Console.
2. In the User Settings section, select **Aliases**.
3. Add the mailing address as an alias.

The mailing list receives the same protections as the user. Only the registered user receives the notifications and quarantine summary.

To alias the mailing list to a new user:

1. Designate an owner for the mailing list.

The owner is not required to be a member of the mailing list.

2. Create a user for the mailing list.

Add a user to represent the mailing list. For example, *info_mailing_list@jumboinc.com*. This user **should not have** an email account on your mail server. This user account serves only for filtering and not for mail traffic.

The user can be added to any user organization. The filter settings for the organization apply to the mailing list, so this may help you choose the appropriate organization.

3. Set the Notifications address.

Select the mailing list user. Under Settings, click **Notifications**. Add the list owner's email address to the Notification address. This allows only the list's owner to receive the quarantine summary, notifications, and password changes.

4. Configure filtering for the mailing list user.

Select the mailing list user account, and configure Spam Filtering. Add any approved or blocked senders.

5. Select the mailing list user, and add the mailing list address as an alias.

The mailing list receives virus and spam protection. The users on the mailing list do not receive notifications.

Suspend a User

Suspend a user to temporarily disable all email filtering and the user's access to the Message Center. Suspension does not disable email flow to that user.

When you suspend a user:

- That user's account settings are saved. You can remove the suspension by resetting the user. See "Reset a User" on page 149.
- That user appears in the lists of users in the Administration Console, and in reports, but filtering for Spam and Virus is turned off. Non-Account Virus Blocking does not provide virus protection for that user, as it is still a registered account.

Note: The Status field in the User Summary does not reflect whether user is suspended, only whether the user has ever logged into the Message Center.

- You are not billed for suspended users.

To suspend a user:

1. Go to the Overview page of the user you want to suspend.
2. Click **Suspend User**.

3. When asked to confirm suspension of the user, make the following optional selections:
 - **Deliver this user's undelivered messages** Delivers all quarantined messages to the user's Inbox before suspending the user.
 - **Notify this user of suspension** Sends the user a Suspension notification.
 - **Suspend this user's future Message Center access** Prevents the user from logging in to the Message Center. If the user has User Access modify privileges for Junk Email Settings or Virus Settings, you must select this option to prevent the user from logging in to the Message Center and re-enabling filtering.
4. Click **Confirm**.

You can suspend several users at once using a Batch File or EZCommand. See the `suspenduser` command in the "Commands" chapter of the *Batch Reference Guide*.

To remove the suspension, reset the user. See "Reset a User" on page 149.

Reset a User

You can undo changes to a user's settings by *resetting* that user. This applies all settings from the Default User assigned to the user's organization. See "Manage Default User Templates" on page 114.

You might want to reset a user if:

- The Default User assigned to the user's org was modified, and you want this user to assume the new settings.
- User Access permissions were changed for this user and can no longer be controlled from the org-level User Access. Resetting the user returns control of these settings to the org-level.
- Several unwanted changes were made for the user and you want to eliminate all of them at once.

WARNING: Resetting a user changes most of the user's personal settings to the Default User settings.

To reset a user:

1. Go to the user's Overview page.
2. Click **Reset User**, and confirm that you want to reset the user.

You can reset several users at once using a Batch File or EZCommand. See the Org Settings Examples section in the "Examples of Common Tasks" chapter of the *Batch Reference Guide*.

Download Users and Settings

From the Users or User Summaries page, you can download a text list of users and their settings, and then import the text into a spreadsheet. For example, you can download the results of a user search or a list of all users in a particular domain.

To download users and settings:

1. Go to **Orgs and Users > Users**, then click the **Download Users/Settings** link at the top right of either the Users or User Summaries page.
2. Save the result as a text file, then import that file into a spreadsheet in a comma-separated format.

The following fields are listed:

Address	Address of the user account
User ID	Unique ID number for the user account
Notice Address	Address to which notifications for this user are sent
OrgID	Unique ID for the organization containing the user
JunkMail Filter	0: Spam Filtering Off 1: Spam Filtering On
Filter Bulk	Master filter setting to block spam 11-15 -> 1-5 on the User Management page 11 : Lenient (1) 12 : Moderately-Lenient (2) 13 : Moderate (3) 14 : Moderately-Aggressive (4) 15 : Aggressive (5)
Filter Adult	Sexual content category filter setting for the user 11-15 -> 1-5 on the User Management page 11:Off (1) 12:Lenient (2) 13:Moderate (3) 14:Moderately-Aggressive (4) 15:Aggressive (5)

Filter GetRich	Get Rich Quick category filter setting for the user Same scale as Filter Adult
Filter Offers	Special Offers category filter setting for the user Same scale as Filter Adult
Filter Racial	Racially Insensitive category filter setting for the user Same scale as Filter Adult
Wireless State	0: On 1: Off 2: Not allowed
Virus Notify	Frequency of user virus notifications NULL: use organization setting 0: Send immediately 1: Send one per day 9: Disable virus notifications
Virus State	0: On 1: Off 2: Not allowed
Approved Senders	Comma separated list of user approved senders
Approved Recipients	Comma separated list of user approved recipients
Blocked Senders	Comma separated list of user blocked senders
WebLocked	0: Message Center Access is enabled 1: Message Center Access is disabled
TimeZone	Timezone for Wireless
Message Limited	0: The user's message limit <i>has not</i> been reached 1: The user's message limit <i>has</i> been reached
Message Count	Approximate number of messages received within one day
Message Limit	Maximum number of messages per day NULL if there is no limit
Msg Quarantined	0: No quarantined messages since last Message Center login 1: There are quarantined messages since last Message Center login

Troubleshoot Users

How do I protect internal distribution or mailing lists from spam and viruses?

Do this by adding each list to the service, either as a user, or aliased to a user. See “Protect Your Mailing and Distribution Lists” on page 147.

Mail from external mailing lists is being falsely filtered as spam. What should I do?

Users can add these addresses to a special list that approves incoming mail based on the address in its To and CC fields. You can do this on the user's Overview page (under Sender Lists), or the user can do this at the Message Center. See “Approved and Blocked Sender Lists” on page 387.

How do I modify all users in a domain?

To make changes to all users you need to adjust the individual user records, as well as the default user (the template for new user creation). This is performed most efficiently by creating a batch file using the modifyuser command:

1. Go to **Orgs and Users > Users** and select your Account org from the Choose Org pull-down list.
2. Enter the “%” character and then the domain name, then click **Search**.

This performs a search across all of your organizations for user addresses using that domain, returning the first 15,000 users.
3. Click **Download Users/Settings**.
4. Select and copy all of the lines that have email addresses.
5. Open a text editor (if using Microsoft Untapped, turn word-wrap off) and paste the text. Save the file using the file extension “.csv”.
6. Using a standard spreadsheet program, such as Microsoft Excel, open the .CSV file you saved in Step 5.
 - a. Delete all columns except the one containing the email addresses.
 - b. Add a column to the left of the addresses column.
 - c. Fill that column with the word: modifyuser.
 - d. In as many columns as necessary to the right of the addresses column, enter field=value pairs (see the Orgs and Users > Batch page for a link to User field and value information on the Summaries link or the *Batch Reference Guide*).
 - e. Save the file again as a CSV file.

7. Load the file created in Step 6 into a text editor and replace all occurrences of “modifyuser,” with “modifyuser “to remove the comma and add a space. Make sure there is a comma between the user’s address and the fields, and between each field=value pair. The result should look something like this example:

```
modifyuser msmith@sales.jumboinc.com, junkmail_filter=0,  
virus_notify=9
```

Save result as a TXT file.

8. You can now validate this file and upload it as a batch file. See the “Introduction to Batch Processing” in the *Batch Reference Guide* for details on how to submit the batch command.

How do I delete all users in a domain by batch file?

Use the steps in the item above (“How do I modify all users in a domain?”) to create a batch file which uses the deleteuser batch command instead of the modifyuser command. Default users cannot be deleted in this way. See “Manage Default User Templates” on page 114 for details.

How do I block all traffic to an address?

The service passes traffic through if there is no associated user account. To block all traffic to an address, create a user account for the address, and set the user’s Daily Message Limit to 0.

1. Go to **Orgs and Users > Users**.
2. Enter the User address and click **Search**.
3. Click the user address, and click **Message Limits** in the Inbound Services section.
4. Scroll down to the bottom of the page and set the Daily Message Limit field to 0 (zero).
5. Click **Save**.

Why does a user receive a message with the title *Mail Limit Exceeded*?

Either the user or the organization containing the user has a Daily Message Limit set. That limit has been reached.

1. Go to **Orgs and Users > Users**.
2. Enter the user address in the Find User field and click **Search**. (You may need to use the Choose Org pull-down menu to select the org containing the user.)
3. Click the user address.
4. Click **Message Limits** in the Inbound Services section of the page.
5. If the limit is not listed there, it is imposed on the organization that contains the user, so click “View Org-Level Message Limits”.

The limit is configured there.

Changing this limit does not restore mail flow to the user.

How can I view a list of all my user aliases?

You can see a list of users and aliases through the Administration Console:

1. Go to **Orgs and Users > Users**.
2. Select the **Include: aliases** check box, then click **Search**.
3. You see a list of all users and their aliases in your org structure.
4. To narrow this search, you can enter special criteria into the Find User text box.

You can also see a list of aliases in the Usage Details. You must be logged in as an administrator on the Account level org to do so.

1. Go to **Orgs and Users**, then click the Account level organization in the list of organizations.
2. In the Organization Management page, scroll down to Organization Settings and click **Usage Details**.
3. On the Monthly Usage Details page, go to Alternate Addresses.

You see a list of alias addresses, sorted by organization. This information is compiled monthly, so recent changes are not be included in this report.

Health Check: Update User Settings

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration.

Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust. Use the instructions below to make any adjustments if necessary to your user settings.

Unfiltered Mail and Unregistered Users

You are required to register all valid email addresses with the message security service. Any unregistered address will be unfiltered and your mail server will need to process large quantities of spam messages sent to invalid recipients.

Health Check will display the number of messages that were delivered unfiltered to your mail server during the past 30 days.

For instructions on adding users to the message security service, see “Add / Delete / Move Users” on page 120 and “Manage User Aliases” on page 140.

Related Topics

- **Add / Delete / Move Users**
- **Manage User Aliases**
- **Health Check: Update Virus Settings**
- **Health Check: Approved Senders List Cleanup**
- **Health Check: Update Settings for Executable Attachments**

Chapter 7

Administrators

About Administrators and Authorization

Administrators have access to the Administration Console where users and organizations are managed. Each administrator must have a user account and assigned privileges to access organizations. Administrator privileges are assigned by creating an *authorization record*. The authorization record doesn't need to be in the same organization as the administrator -- the authorization record can be anywhere in the organization hierarchy. In addition, an administrator can have multiple authorization records with different privileges assigned to various organizations through out the hierarchy.

The privileges are automatically propagated down the hierarchy. When an authorization record is created for an administrator in an organization, the administrator has privileges for that organization and all of its sub-organizations. For detailed reference information for the privileges, see *The Message Security Authorization Reference*.

Administrators and the Organization Hierarchy

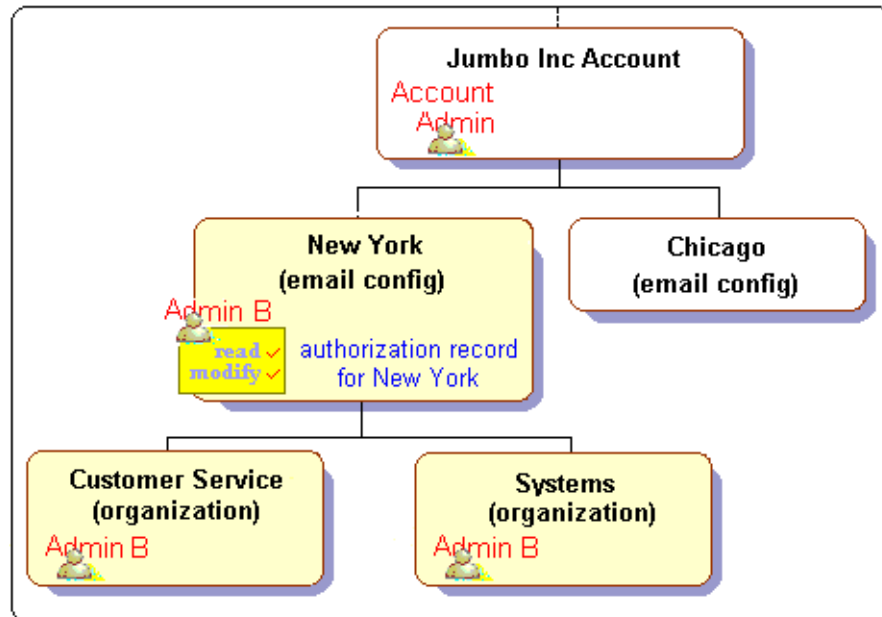
When an existing administrator creates a new authorization record for a user account, that user becomes an administrator and is granted administrative privileges and access to the Administration Console.

An authorization record is assigned to an organization. Depending on the authority settings, the administrator is able to view and modify certain aspects of the organization, such as configuring spam filter settings. The new administrator's record can be in the same organization as the existing administrator's record or in a sub-organization.

To provide a scalable administrative framework that can serve a large user base, while maintaining the security of each organization, the administrative hierarchy is linked to the organizational hierarchy.

Authority Privilege Propagation

In an organization hierarchy, administrator privileges are propagated down the organizational tree. The following example illustrates how administrative authority affects management privileges in the organization.



The Jumbo Inc account administrator maintains authority over both the New York and Chicago email configs, and all sub-organizations.

Admin B is assigned an authorization record and privileges for the New York email config. Admin B therefore has privileges to configure and manage the Customer Service and Systems organizations. Admin B also has the same privileges over any sub-organizations of Customer Service and Systems.

Since Admin B has no authorization record in the Chicago email config organization, Admin B cannot view or modify any Chicago organizations.

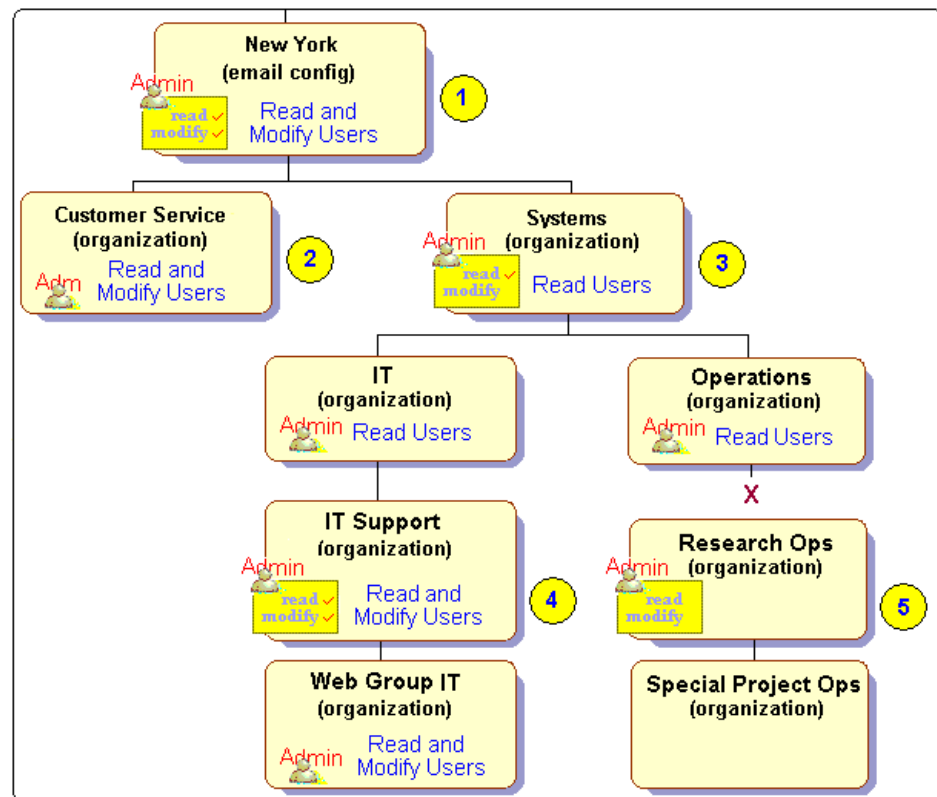
Limiting Authority

An administrator is limited to managing the organization where he or she has authority, and can manage any sub-organizations as well. The specific privileges assigned to that administrator are inherited down the hierarchy unless another authorization record changing that authority is added to a sub-organization.

An administrator's access to an organization is determined by the closest authorization record in the organization hierarchy, or in a direct parent of the organization. An authorization record created at a peer or lower level takes precedence over an authorization record at a higher level.

A peer administrator can modify and delete another administrator's privileges, if it is assigned to the same organization, by clicking **Delete** on the Authorization List page. This does not remove the impacted administrator as a user. It removes the administrator's authorization record for this organization. If this is the impacted administrator's only authorization record, this user is no longer an administrator and is not allowed to log into the Administration Console. The purpose of this functionality is to provide a quick way to remove access to the Administration Console in special circumstances.

This example illustrates how insertion of authorization records in sub-organizations impacts the administrative control that is available from that point down in the hierarchy. The example shows one administrator with four different authorization records that narrow, expand, and block administrator access.

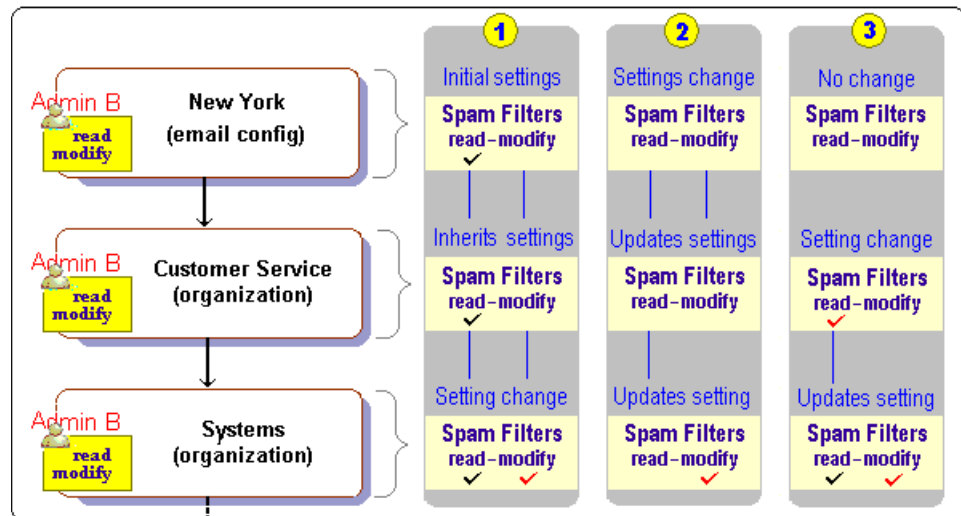


1. The administrator has an authorization record assigned in the New York organization. This record includes privileges to read (or view) and modify user settings.
2. This authority is inherited to the Customer Service organization. The administrator can view and modify user settings in this organization.
3. At the Systems organization, our administrator has a new authorization record with privileges limited to just reading user settings. The administrator can only read and not modify user settings for the sub organizations IT and Operations.

4. For the IT Support organization, our administrator's full read and modify privileges are restored. A new authorization record with full read and modify privileges is assigned to this organization. And, in turn, these privileges are inherited in the Web Group IT organization.
5. For business reasons, this company limits administrative access to the Research Ops organization hierarchy to a select set of administrators. Since our administrator is not one of those, she is blocked by a new authorization record with no privileges (all read and modify rights are blank). This record is assigned to the Research Ops organization.

Multiple Authorization Record Updates

When an administrator has multiple authorization records within an organization hierarchy, changes to these records are updated down the organizational tree unless an administrator changes an authorization record setting in a sub-organization. The following example illustrates how changes in one authority record affect the automatic updates across multiple authorization records.



1. Examples of initial inheritance and a sub-organization record change:
 - a. The top-level authorization record assigned to the New York organization has the read-only privilege for managing spam filters.
 - b. When created, the Customer Service and Systems authorization records inherit the New York authorization setting. Both have read-only privileges for managing spam filters.
 - c. In the Systems record, the account administrator enables the Spam Filters modify privilege. At this point, the Spam Filters modify privilege is no longer updated if either parent organization's record changes.

2. Example of the modify privilege in the Systems record not updating:
 - a. In the top-level New York authorization record, the account administrator turns off the Spam Filters privileges.
 - b. In the Customer Service authorization record, the Spam Filters settings are automatically updated to the New York record changes.
 - c. In the Systems authorization record, the Spam Filters read-only privilege automatically updates. Since the modify privilege was changed after the initial settings, it does not change.
3. Example of changing a record that updates sub-organizations:
 - a. The top-level New York organization does not change in this example.
 - b. In the Customer Service record, the administrator changes the Spam Filters privilege to read-only. At this point, this read privilege is no longer updated when the parent New York record changes.
 - c. In the Systems record, a sub-organization, the Spam Filters privilege updates to read-only since the parent's setting has changed. The modify privilege, changed in step 1, does not change.

Create Administrators and Manage Authorization Records

When you create an administrator:

- **Check your authorization record** -- Your authorization record needs the Add Users, Assign Authority, and Assign Peer Authority (optional) privileges:
 - Add Users -- If the new administrator is not yet a user in the system, you must have full Add Users privileges for the organization where you are adding the new administrator. For more information, see *The Message Security Authorization Reference*, “All Standard Privileges” chapter’s AddUsers privilege.
 - Assign Authority -- To create new authorization records for users in your organization and sub-organizations, and to view or edit existing authorization records for users in your organization and sub-organizations, you must have full Assign Authority privileges. For more information, see *The Message Security Authorization Reference*, “All Standard Privileges” chapter’s Assign Authority privilege.
 - Assign Peer Authority -- To create a peer administrator record in the same organization as one of your administrator records, you must have the +Modify Assign Peer Authority privilege. For more information, see *The Message Security Authorization Reference*, “All Standard Privileges” chapter’s Assign Peer Authority privilege.

For further information on viewing your authorization record, see “Viewing and Editing Authorization Records” on page 164. If you, as the managing administrator, do not have these privileges, contact your account administrator.

- **Create a user** -- The new administrator must be an existing user in the system. If the user does not already exist, you must create a new user. For more information about how to add a new user, see “Add / Delete / Move Users” on page 120.
- **Define the new administrator** -- Deciding what type of administrator to create is a critical preliminary step before configuring the new administrator. It is common for one administrator to have several administrative jobs. This administrator’s configuration is a combination of the administrator types described in this chapter. For a chart comparing different administrator types, see “Comparing Types of Administrators” on page 167.
- **Decide where to place the authorization records** -- Once the administrator type is determined, decide what part of your organization hierarchy the new administrator will manage. This is where you assign the administrator’s authorization records. In some instances, an administrator has several records assigned to different organizations. See “Types of Administrators” on page 166.
- **Create an administrator** -- Create the new administrator and configure the authorization record. Follow the instructions in “Creating an Administrator” on page 163. When you are ready to populate the administrator’s authorization record, see “Types of Administrators” on page 166 for the recommended privilege settings for each type of administrator.
- **If needed, customize the authorization record** -- Use the detailed reference information for each privilege to customize your administrator’s settings. See *The Message Security Authorization Reference*, “Message Archiving

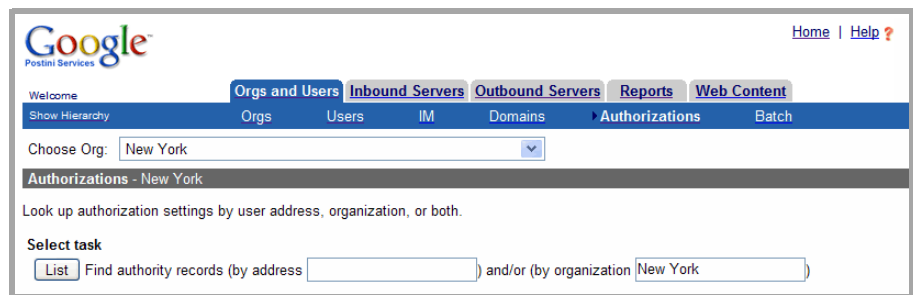
Privileges”, “All Standard Privileges”, and “Inbound Mail Processing” chapters.

Note: An account administrator, with the Assign Peer Authority privilege enabled, can create and change settings for a peer account-level administrator.

Creating an Administrator

To create a new administrator:

1. If the user does not already exist, create a user account for the administrator. See “Add / Delete / Move Users” on page 120 for more information.
2. In the Administration Console, go to Orgs and Users > **Authorizations**.



3. Choose the organization where the administrator should have privileges.
4. Click **List**.



5. Enter the administrator’s email address in the User field, and click **Add record**.
6. Edit and set the privileges you want to give the administrator. For more information on recommended settings for common administrator types, see “Types of Administrators” on page 166.

WARNING: Modifications to the authorization record take effect immediately. Unlike modifying a user or organization, you do not have to click a submit button to save to the authorization record.

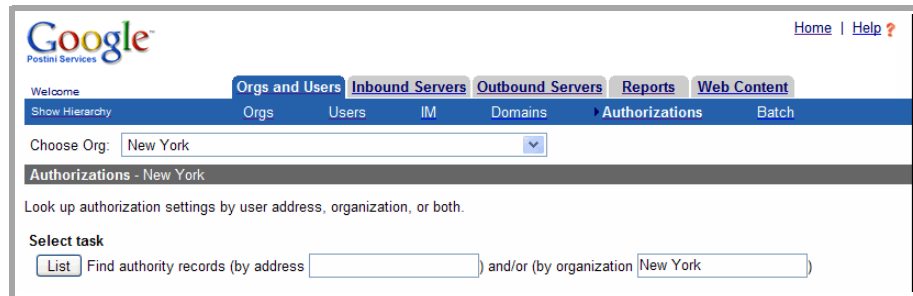
If the administrator needs access to support, please contact the appropriate support channel.

7. The new administrator receives a temporary password for the Administration Console. You can view this password in the **User page** for the new administrator. When the administrator logs in for the first time, the administrator is prompted to change the password.

This new password also becomes the password for the administrator's Message Center.

Viewing and Editing Authorization Records

1. Go to Orgs & Users > Authorizations.
2. In the Authorizations page, choose an organization from the **Choose Org** pull-down list, or enter an administrator's address, and delete the text in the **by organization** field (if any).



3. Click **List**.
4. You see a list of users who have authorization records.

Example of results by organization:

Authorizations - New York			
Authorization records for New York			
User	Organization		
bchad@corp.jumboinc.com	New York	Delete	Edit profile
abradley@corp.jumboinc.com	New York	Delete	Edit profile
mprinz@corp.jumboinc.com	New York	Delete	Edit profile
<input type="text"/>	New York	<input type="button" value="Add record"/>	

Note: By selecting a User, you see all of the other organizations this user can administer.

Example of results by address:

Authorizations - New York			
Authorization records for mprinz@corp.jumboinc.com			
User	Organization		
mprinz@corp.jumboinc.com	New York	Delete	Edit profile
mprinz@corp.jumboinc.com	Customer Service	Delete	Edit profile
mprinz@corp.jumboinc.com	<input type="text"/>	<input type="button" value="Add record"/>	

Note: Administrators who have authorization records in the same organization (peer administrators) can edit each other's authorization records.

5. In an emergency or under special circumstances, an administrator can delete a peer administrator. For example, bchad@corp.jumboinc.com can delete the New York authorization record assigned to abradley@corp.jumboinc.com. Click **Delete** to delete a peer administrator's authorization record.

Note: This does not delete the administrator's user record.

6. Click **Edit profile** to display the administrator's authorization record for that organization.

7. Edit the administrator's **Read or Modify** privileges.
 - a. With the Read privilege, an administrator can view settings and configurations.
 - b. With the Modify privilege, an administrator can edit settings and configurations. For recommended administrator-privilege settings, see recommendations for each type of administrator in "Types of Administrators" on page 166.
 - c. If the privilege checkboxes are greyed out, you do not have privileges to edit the administrator's authentication record. Contact your appropriate support channel.
 - d. You have the option of assigning a category of privileges (such as "User Settings") or a specific privilege within that category (such as "Add Users"). By selecting a category, all privileges in the category are selected. You can then deselect specific privileges if necessary.

WARNING: Unlike modifying a user record or organization record, you do not have to click a "Submit" button to enforce changes or additions to the authorization record. Modifications to the authorization record take place immediately. There is no opportunity to cancel changes.

Administrators and POP Authentication

Note: POP Authentication is a legacy feature of the message security service. If you would like to know more, or if you have any questions, please contact Support.

Authenticating users through POP authentication passes unencrypted passwords across the Internet. Because that would introduce a security risk, administrators *never* authenticate using POP. When you create an administrator in an organization which uses POP authentication, PMP will be used instead.

Authentication by cross-authorization and by PMP is secure, and therefore acceptable for administrator log in. For more information, see "User Authentication" on page 615.

Types of Administrators

To simplify the range of possible administrator configurations, this section describes the common types of administrators, where to place their authorization records, and recommended privilege settings. Use these descriptions as a guide that you can customize. It is common for an administrator's job to be composed of several administrative types.

The administrator types are:

- Account Administrators -- The top-level, fully authorized email administrator
- Monitor Administrators -- Observe the activity and status of the hierarchy
- Compliance Officers and Security Administrators -- Prevent illegal and unethical conduct across the account hierarchy
- Archive Administrators -- This includes the Archive Security Administrator, Archive Search, Audit, Retention, and Investigator Security administrators for the account. (Message Archiving is available optionally for an additional fee.)
- Email Config Administrators -- Maintain mail flow and server connections
- Organization Policy Administrators -- Manage common settings and services
- User Administrators -- Manage the day-to-day user help desk needs

Comparing Types of Administrators

	Account Admin	Monitor Admin	Compliance, Security Admins	Archive Admins	Email Config Admin	Org Policy Admin	User Admin
Suspend and Reset Users	read/ modify						read/ modify
Search User Quarantines	read/ modify	read/ modify	read				read/ modify
Add, Delete, Move Users	read/ modify						read/ modify
Message Center Settings	read/ modify	read	read			read/ modify	read/ modify
Create an Administrator	read/ modify					read/ modify	
Add, Delete Organizations	read/ modify					read/ modify	
Generate and View Reports	read/ modify	read	read	modify	read/ modify	read/ modify	read
Notifications	org&user: read/ modify		notifications: read/modify			notify: read/ modify	users: read/ modify
Alerts	org&user: read/ modify				alerts: read/ modify		
Manage Domains	read/ modify	read	read		read/ modify	read/ modify	read

	Account Admin	Monitor Admin	Compliance, Security Admins	Archive Admins	Email Config Admin	Org Policy Admin	User Admin
Spam Filters, Sender Lists, Traffic Limits, Virus, Early Detection Quarantine	read/ modify	read	read			read/ modify	read
Industry Heuristics	read/ modify	read	read			read/ modify	read
Archive Security, Search/Discovery, Audit, Retention, Investigator			read/modify	read and/or modify			
Outbound Mail Processing	read/ modify	read TLS	read TLS		read/ modify	read/ modify	read
Inbound Delivery Management, Spooling, TLS	read/ modify		read		read/ modify	read	read
System Tests	run	run	run		run	run	run
Encryption Services	read/ modify	read	read			read/ modify	read/ modify
Directory Sync	read/ modify						
Attachment Manager	read/ modify	read	read			read/ modify	read
Content Manager	read/ modify	read	read			read/ modify	read
Postini Message Archiving	read/ modify	read	read	optional		read/ modify	read
Postini Web Security and Compliance	read/ modify	read (modify)	read (modify)			read/ modify	read (modify)

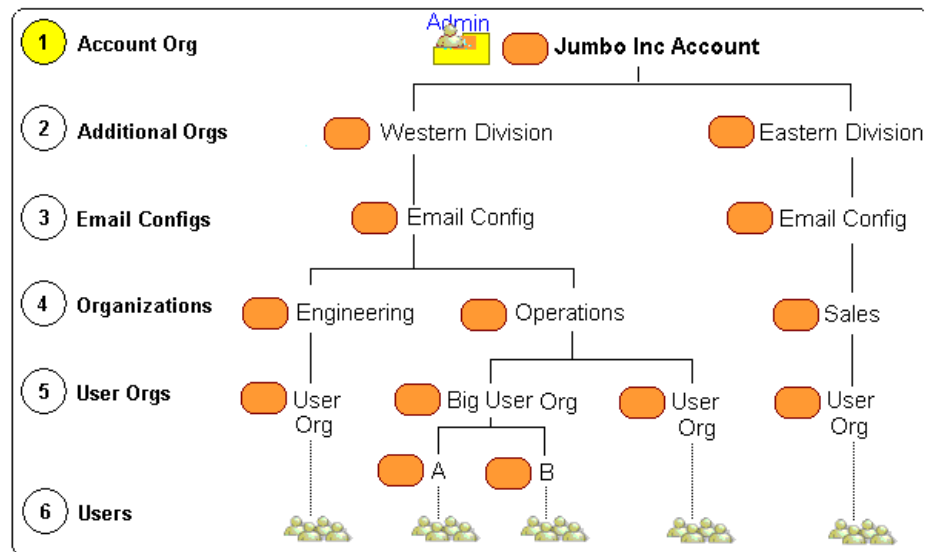
Account Administrators

An *account administrator* manages the top-level account organization and is fully authorized to perform almost all administrative tasks including using Directory Sync. The exceptions are searching and auditing the account's archive, which is managed by a compliance and security administrator. Often, the account administrator roles and the compliance and security administrator roles are given to the same person.

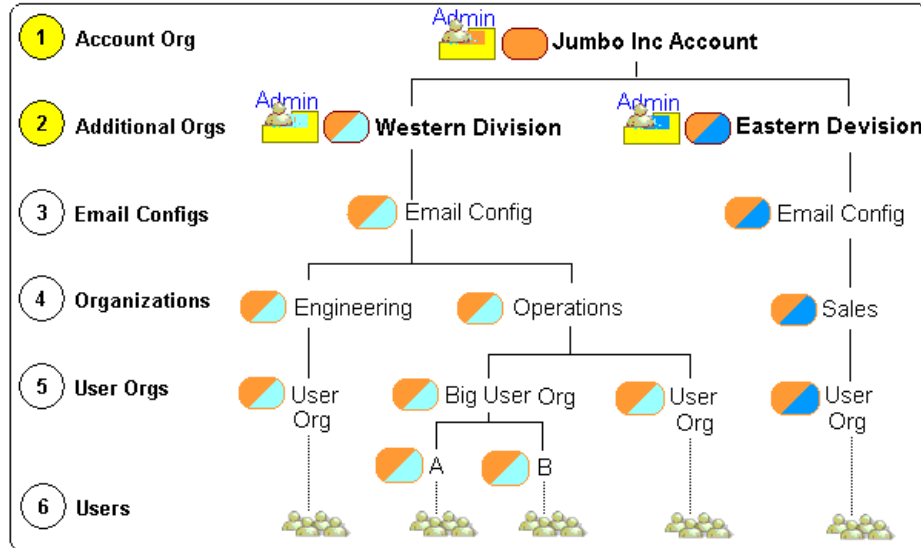
After activation, all accounts have one account administrator positioned at the top of your hierarchy. Depending upon the complexity of your organization hierarchy, additional *fully authorized email administrators* can manage sub organizations below the account level. For example, a large account encompassing several diverse corporate divisions needs *division or regional administrators* who manage the unique complexities of all of the organizations within that division.

Positioning Account Authorization Records

The account administrator's authorization record is assigned to the account organization. This administrator has global management privileges across the whole account hierarchy. And, in turn, this administrator creates additional administrators to manage either peer or sub organization levels. The following example illustrates how the account administrator for Jumbo Inc has administrative privileges for every level of the hierarchy.



In the following example, fully authorized email administrators are assigned to organizations below the account level. These administrators have the same privileges as an account administrator. In the example, the Jumbo Inc account administrator has access to the Western and Eastern Divisions. The Western Division and Eastern Division regional administrators manage their respective divisions.



Recommended Account Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

Account Administrator Privilege	Read /Modify	Notes
All Standard Privileges	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Help Desk	<input checked="" type="checkbox"/>	
Suspend User	<input checked="" type="checkbox"/>	
Reset User	<input checked="" type="checkbox"/>	
View Quarantine	<input checked="" type="checkbox"/>	
User Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Change Address	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Add Users	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	

Account Administrator Privilege	Read /Modify	Notes
Delete Users	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
IM Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Message Encryption Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Sender Lists	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Spam Filters	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Sexually Explicit	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Virus Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Pending Quarantine	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Wireless Settings	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Account Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Password	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Email Aliases	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Regional Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Personal Archive	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Search	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Recover	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email Analysis	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
View Images, Attachments, and Links	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Organization Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Assign Peer Authority	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Change Admin Passwords	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Create Organizations	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Delete Organizations	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
View Reports	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Outbound Mail Processing	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config
Outbound Applications Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config

Account Administrator Privilege	Read /Modify	Notes
Outbound Server Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Outbound Transport Security	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config
Outbound Message Encryption	<input checked="" type="checkbox"/> <input type="checkbox"/>	email config
Edit Organizations	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Notification Messages	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Manage Domains	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Usage Statements	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Message Center Branding	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Virus	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Wireless Email	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Advanced Applications	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Attachment Manager	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Content Manager	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Industry Heuristics	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Message Archiving	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Web Content Manager	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Inbound Mail Processing	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Mail Connection Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Auto Connection Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Delivery Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Spooling	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Inbound Transport Security	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Security Administrator	<input type="checkbox"/> <input type="checkbox"/>	archive security/ compliance
Archive Search	<input type="checkbox"/> <input type="checkbox"/>	archive security/ compliance
Archive Discovery	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Audit	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Retention	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Investigator Security	<input type="checkbox"/> <input type="checkbox"/>	security/archive

Account Administrator Privilege	Read /Modify	Notes
Archive Reports	<input type="checkbox"/>	security/archive

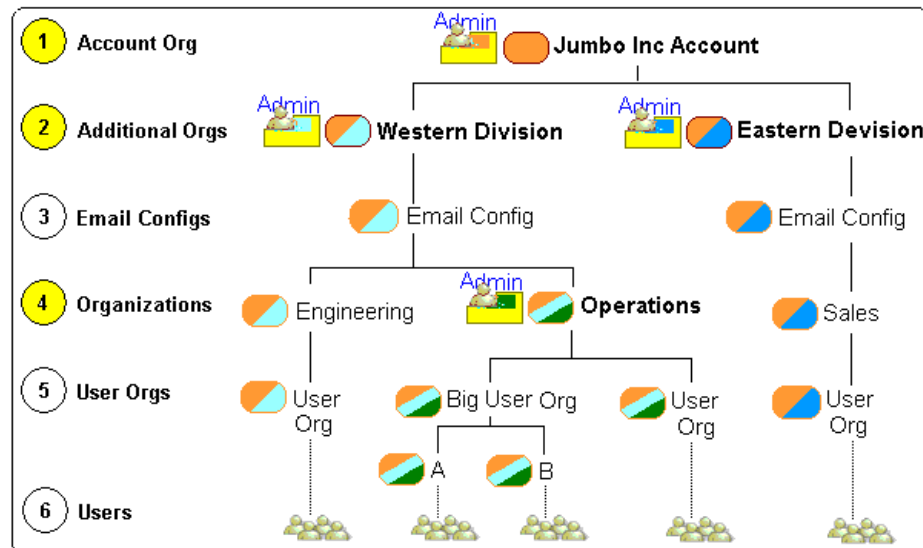
Monitor Administrators

A *monitor administrator* views the overall status and activity of an account or a sub-organization. This administrator is able to run reports but most privileges are read-only. A monitor administrator's role is to maintain a daily view of an established organization hierarchy and status. This relieves the need for additional account administrators in large systems.

A monitor is not used for Directory Sync, password policies, or inbound and outbound mail processing configurations.

Positioning Monitor Authorization Records

In large accounts, an authorization record for monitor administrators is assigned to the account organization. In addition, large sub-organizations may need monitor administrators. In the following example, the administrator assigned to the Jumbo Inc Account monitors the status of the whole account hierarchy. The division-level administrators monitor their specific sub-organizations. On occasion, a monitor administrator is assigned to a lower level organization such as the Operations monitor in the following example. In this case, the Operations monitor could have less read-only access than the monitor administrators assigned to higher-level organizations. The Operations monitor's authorization record would grant fewer privileges based upon your business needs.



Recommended Monitor Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

Monitor Administrator Privilege	Read /Modify	Notes
All Standard Privileges	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Help Desk	<input type="checkbox"/>	
Suspend User	<input type="checkbox"/>	
Reset User	<input type="checkbox"/>	
View Quarantine	<input checked="" type="checkbox"/>	Low level monitor
User Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Change Address	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Add Users	<input type="checkbox"/> <input type="checkbox"/>	
Delete Users	<input type="checkbox"/> <input type="checkbox"/>	
IM Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Message Encryption Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Junk Email Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Sender Lists	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Spam Filters	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Sexually Explicit	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Virus Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/>	
Pending Quarantine	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Settings	<input type="checkbox"/>	
Account Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Password	<input type="checkbox"/>	
Email Aliases	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Regional Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Personal Archive	<input type="checkbox"/>	
Archive Search	<input type="checkbox"/>	
Archive Recover	<input type="checkbox"/>	

Monitor Administrator Privilege	Read /Modify	Notes
Junk Email Analysis	<input checked="" type="checkbox"/> <input type="checkbox"/>	
View Images, Attachments, and Links	<input type="checkbox"/>	
Organization Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Peer Authority	<input type="checkbox"/>	
Change Admin Passwords	<input type="checkbox"/> <input type="checkbox"/>	
Create Organizations	<input type="checkbox"/> <input type="checkbox"/>	
Delete Organizations	<input type="checkbox"/> <input type="checkbox"/>	
View Reports	<input checked="" type="checkbox"/>	
Outbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Applications Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Server Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Message Encryption	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Edit Organizations	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Notification Messages	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Manage Domains	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Usage Statements	<input type="checkbox"/>	
Message Center Branding	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Junk Email	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Virus	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Email	<input type="checkbox"/> <input type="checkbox"/>	
Advanced Applications	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Attachment Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Content Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Industry Heuristics	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Message Archiving	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Web Content Manager	<input checked="" type="checkbox"/>	Pages viewable
Inbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org

Monitor Administrator Privilege	Read /Modify	Notes
Mail Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Auto Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Delivery Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Spooling	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Inbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Archive Security Administrator	<input type="checkbox"/>	archive security/ compliance
Archive Search	<input type="checkbox"/>	archive security/ compliance
Archive Discovery	<input type="checkbox"/>	security/archive
Archive Audit	<input type="checkbox"/>	security/archive
Archive Retention	<input type="checkbox"/>	security/archive
Archive Investigator Security	<input type="checkbox"/>	security/archive
Archive Reports	<input type="checkbox"/>	security/archive

Compliance Officers and Security Administrators

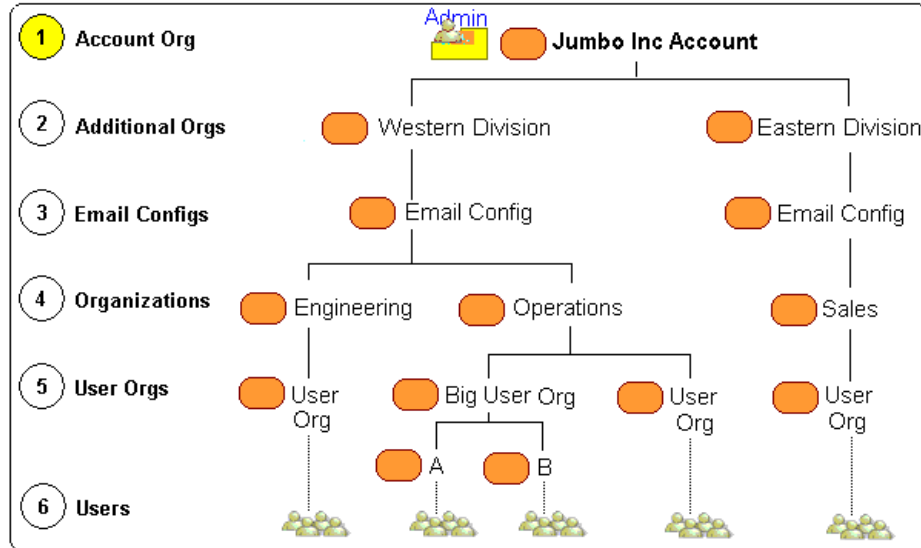
A *compliance officer* manages the operations and procedures of a company's compliance program, which prevent illegal and unethical conduct. A *security administrator* manages the protection and security of the company's assets from illegal and improper activities.

Compliance officers, security administrators, and archive search administrators are the only administrators who can search and audit an account's archive. Compliance and security administrators are not used for Directory Sync, password policies, or inbound and outbound mail processing configurations.

Even though a compliance officer and a security administrator can be different people with different jobs, their authorization record settings are very similar, and their job requirements place their administrative duties high in an organization hierarchy. Usually, this type of administrator audits a hierarchy but does not change the actual policy settings, which is why several of the recommended authorization record settings are read-only. A compliance officer or security administrator identifies system modifications and arranges for these to be done by an account administrator or by a technical administrator with modify privileges.

Positioning Compliance Officer and Security Authorization Records

Because of the sensitive nature of a compliance officer's and security administrator's jobs, these authorization records are usually assigned to the account organization. As illustrated in the following example, these administrators have access to the whole hierarchy.



Recommended Compliance Officer and Security Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

Compliance Officer and Security Administrator Privilege	Read/Modify	Notes
All Standard Privileges	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Help Desk	<input type="checkbox"/>	
Suspend User	<input type="checkbox"/>	
Reset User	<input type="checkbox"/>	
View Quarantine	<input checked="" type="checkbox"/>	
User Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Change Address	<input checked="" type="checkbox"/> <input type="checkbox"/>	

Compliance Officer and Security Administrator Privilege	Read/Modify	Notes
Add Users	<input type="checkbox"/> <input type="checkbox"/>	
Delete Users	<input type="checkbox"/> <input type="checkbox"/>	
IM Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Message Encryption Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Junk Email Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Sender Lists	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Spam Filters	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Sexually Explicit	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Virus Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/>	
Pending Quarantine	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Settings	<input type="checkbox"/>	
Account Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Password	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Email Aliases	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Regional Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Personal Archive	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Search	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Recover	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email Analysis	<input checked="" type="checkbox"/> <input type="checkbox"/>	
View Images, Attachments, and Links	<input type="checkbox"/>	
Organization Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Peer Authority	<input type="checkbox"/>	
Change Admin Passwords	<input type="checkbox"/> <input type="checkbox"/>	
Create Organizations	<input type="checkbox"/> <input type="checkbox"/>	
Delete Organizations	<input type="checkbox"/> <input type="checkbox"/>	
View Reports	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Outbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org

Compliance Officer and Security Administrator Privilege	Read/Modify	Notes
Outbound Applications Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Server Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Outbound Message Encryption	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Edit Organizations	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Notification Messages	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Manage Domains	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Usage Statements	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Message Center Branding	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Junk Email	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Virus	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Email	<input type="checkbox"/> <input type="checkbox"/>	
Advanced Applications	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Attachment Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Content Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Industry Heuristics	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Message Archiving	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Web Content Manager	<input type="checkbox"/> <input checked="" type="checkbox"/>	View pages
Inbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Mail Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Auto Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Delivery Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Spooling	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Inbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config org
Archive Security Administrator	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Search	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Discovery	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Archive Audit	<input type="checkbox"/> <input checked="" type="checkbox"/>	

Compliance Officer and Security Administrator Privilege	Read/Modify	Notes
Archive Retention	<input checked="" type="checkbox"/>	
Archive Investigator Security	<input checked="" type="checkbox"/>	
Archive Reports	<input type="checkbox"/>	security/archive

Archive Administrators

An *archive security administrator* manages the important but very focused areas of responsibility in Message Archiving (available optionally for an additional fee):

- Security Administration
- Search
- Discovery
- Audit
- Retention
- Investigator Security
- Reports

An archive administrator can be a stand-alone administrator who manages one or all of these Message Archiving areas. Usually these administrators work with a compliance officer or security administrator.

For additional insight into Message Archiving privileges and the options available with each privilege, see:

Granting Message Archiving Privileges

Note: Message Archiving features are available optionally for an additional fee.

Archive Security Administrator

Archive Security Administrators have full access to the corporate archive and full access to Message Archiving features:

- Requires the Archiving Security Administration privilege, which in turn grants all other archiving privileges.
- The Message Archiving privilege is optional -- If the Message Archiving privilege is enabled (for customers who purchase archiving), the administrator can turn on archiving and set archiving options for the org.
- The Assign Authority privilege is optional -- If assigned, the administrator can create other archive search or discovery administrators.

Archive Search or Discovery Administrators

Archive search or discovery administrators manage the account-level archive search, investigations of archived messages, search criteria, and exported messages. These administrators have one required privilege and some optional privileges:

- Requires the Archive Search privilege.
 - With Archive Search, the Message Archiving link replaces the System Administration link on the login page. The administrator has access to the Message Archiving Search and Report tabs.

From the Search tab, the administrator can search the archive. From the Reports tab, the administrator can view the Storage Overview and Storage reports.
 - With the Archive Search *and* Archive Discovery privileges, the Message Archiving link replaces the System Administration link on the login page. The administrator has access to the Message Archiving Discovery and Report tabs.

The Discovery tab includes the same features as the Search tab plus the investigation features (e.g., saving search criteria and results). From the Reports tab, the administrator can view the Storage Overview and Storage reports.

The Archive Discovery privilege requires that the Archive Search privilege is also granted.
- The Message Archiving privilege is optional -- If the Message Archiving privilege is enabled, the administrator can turn on archiving and set archiving options for the org.
- The Assign Authority privilege is optional -- If assigned, the administrator can create other archive search or discovery administrators.

Archive Audit Administrator

An archive audit administrator manages the account-level audit reports. This administrator has one required privilege and some optional privileges:

- Requires the Archive Audit privilege. If this is the only granted privilege, this administrator has access to the audit reports on the Message Archiving Reports tab. The Message Archiving link replaces the System Administration link on the login screen.

Usually this privilege is combined with the Archive Search/Discovery or Archive Retention privileges. In these cases, the Message Archiving pages have Audit Reports in the left navigation pane and in the Retention page has the Audit Reports link.
- The Message Archiving privilege is optional -- If the Message Archiving privilege is enabled, the administrator can turn on archiving and set archiving options for the org.
- The Assign Authority privilege is optional -- If assigned, the administrator can create other archive search or discovery administrators.

Archive Retention Administrator

An archive retention administrator manages account-level retention, purges, and purge history of all messages. This administrator has one required privilege and some optional privileges:

- Requires the Archive Retention privilege. If this is the only granted privilege, this administrator has access to the Message Archiving Retention tab. The Message Archiving link replaces the System Administration link on the login screen.
- The Message Archiving privilege is optional -- If the Message Archiving privilege is enabled, the administrator can turn on archiving and set archiving options for the org.
- The Assign Authority privilege is optional -- If assigned, the administrator can create other archive search or discovery administrators.

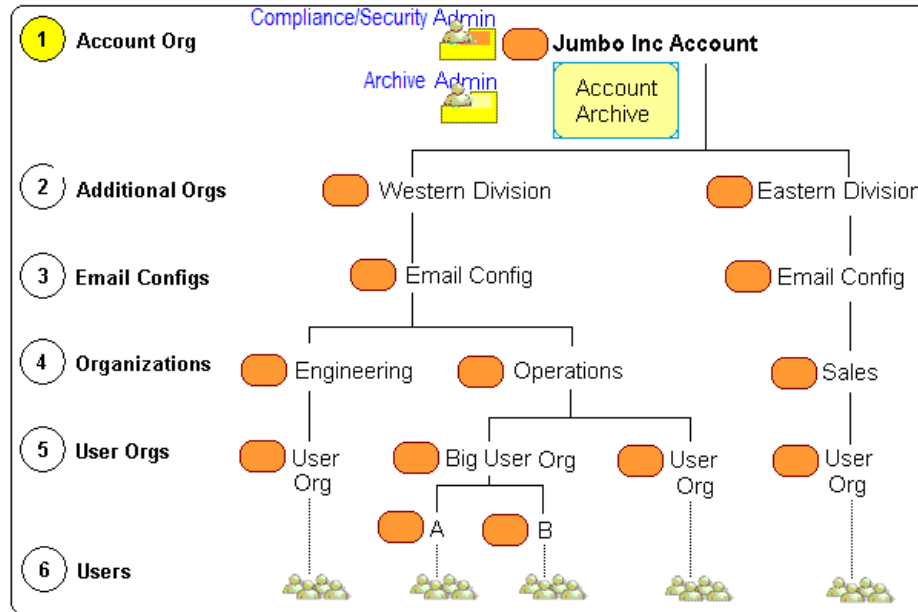
Archive Investigator Administrator

An archive investigator administrator manages which investigators can search which users' messages. This administrator has two required privileges and some optional privileges.

- If Archive Investigator Security and Archive Search are the only granted privileges, this administrator has access to the Message Archiving Search and Admin tabs. The Message Archiving link replaces the System Administration link on the login screen.
- The Message Archiving privilege is optional -- If the Message Archiving privilege is enabled, the administrator accesses the Message Archiving Admin page through the Administration Console's organization-level Archiving page.
- The Assign Authority privilege is optional -- If assigned, the administrator can create other archive investigator administrators.

Positioning Archive Authorization Records

Since the scope of archive functions are account-wide, the archive administrator's authorization record can be anywhere within the hierarchy. The record is usually assigned to the account organization. In the following example, the account organization has a compliance/security authorization record and an archive record. This record can be for an archive search/discovery, audit, retention, or investigator administrator.



Recommended Archive Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

Archive Privileges	Read/Modify	Notes
All Standard Privileges	<input type="checkbox"/> <input type="checkbox"/>	
Help Desk	<input type="checkbox"/>	
Suspend User	<input type="checkbox"/>	
Reset User	<input type="checkbox"/>	
View Quarantine	<input type="checkbox"/>	
User Settings	<input type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input type="checkbox"/> <input type="checkbox"/>	
Change Address	<input type="checkbox"/> <input type="checkbox"/>	
Add Users	<input type="checkbox"/> <input type="checkbox"/>	

Archive Privileges	Read/Modify	Notes
Delete Users	<input type="checkbox"/> <input type="checkbox"/>	
IM Management	<input type="checkbox"/> <input type="checkbox"/>	
Message Encryption Management	<input type="checkbox"/> <input type="checkbox"/>	
Application Management	<input type="checkbox"/> <input type="checkbox"/>	
Junk Email Settings	<input type="checkbox"/> <input type="checkbox"/>	
Sender Lists	<input type="checkbox"/> <input type="checkbox"/>	
Spam Filters	<input type="checkbox"/> <input type="checkbox"/>	
Sexually Explicit	<input type="checkbox"/> <input type="checkbox"/>	
Virus Settings	<input type="checkbox"/> <input type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/>	
Pending Quarantine	<input type="checkbox"/> <input type="checkbox"/>	
Wireless Settings	<input type="checkbox"/>	
Account Settings	<input type="checkbox"/> <input type="checkbox"/>	
Password	<input type="checkbox"/>	
Email Aliases	<input type="checkbox"/> <input type="checkbox"/>	
Regional Settings	<input type="checkbox"/> <input type="checkbox"/>	
Personal Archive	<input type="checkbox"/>	
Archive Search	<input type="checkbox"/>	
Archive Recover	<input type="checkbox"/>	
Junk Email Analysis	<input type="checkbox"/> <input type="checkbox"/>	
View Images, Attachments, and Links	<input type="checkbox"/>	
Organization Management	<input type="checkbox"/> <input type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Optional
Assign Peer Authority	<input checked="" type="checkbox"/>	
Change Admin Passwords	<input type="checkbox"/> <input type="checkbox"/>	
Create Organizations	<input type="checkbox"/> <input type="checkbox"/>	
Delete Organizations	<input type="checkbox"/> <input type="checkbox"/>	
View Reports	<input type="checkbox"/>	
Outbound Mail Processing	<input type="checkbox"/> <input type="checkbox"/>	
Outbound Applications Management	<input type="checkbox"/> <input type="checkbox"/>	
Outbound Server Management	<input type="checkbox"/> <input type="checkbox"/>	

Archive Privileges	Read/Modify	Notes
Outbound Transport Security	<input type="checkbox"/> <input type="checkbox"/>	
Outbound Message Encryption	<input type="checkbox"/> <input type="checkbox"/>	
Edit Organizations	<input type="checkbox"/> <input type="checkbox"/>	
Notification Messages	<input type="checkbox"/> <input type="checkbox"/>	
Manage Domains	<input type="checkbox"/> <input type="checkbox"/>	
Usage Statements	<input type="checkbox"/>	
Message Center Branding	<input type="checkbox"/> <input type="checkbox"/>	
Application Management	<input type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input type="checkbox"/> <input type="checkbox"/>	
Junk Email	<input type="checkbox"/> <input type="checkbox"/>	
Virus	<input type="checkbox"/> <input type="checkbox"/>	
Wireless Email	<input type="checkbox"/> <input type="checkbox"/>	
Advanced Applications	<input type="checkbox"/> <input type="checkbox"/>	
Attachment Manager	<input type="checkbox"/> <input type="checkbox"/>	
Content Manager	<input type="checkbox"/> <input type="checkbox"/>	
Industry Heuristics	<input type="checkbox"/> <input type="checkbox"/>	
Message Archiving	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Optional
Web Content Manager	<input type="checkbox"/>	
Inbound Mail Processing	<input type="checkbox"/> <input type="checkbox"/>	
Mail Connection Management	<input type="checkbox"/> <input type="checkbox"/>	
Auto Connection Management	<input type="checkbox"/> <input type="checkbox"/>	
Delivery Management	<input type="checkbox"/> <input type="checkbox"/>	
Spooling	<input type="checkbox"/> <input type="checkbox"/>	
Inbound Transport Security	<input type="checkbox"/> <input type="checkbox"/>	
Archive Security Administrator	<input checked="" type="checkbox"/>	Alone: Message Archiving login and, with archive settings, other archiving pages
Archive Search	<input checked="" type="checkbox"/>	Alone: Message Archiving login and Search pages
Archive Discovery	<input checked="" type="checkbox"/>	Requires Archive Search

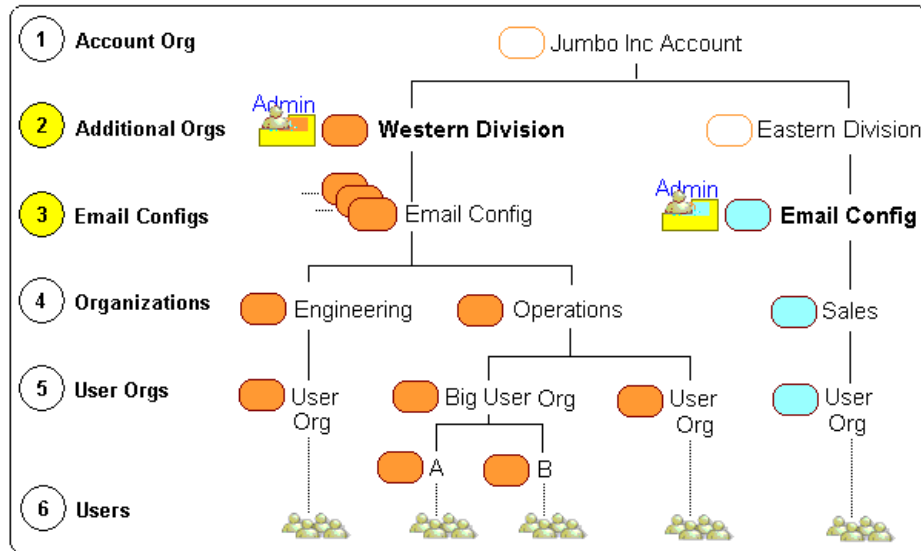
Archive Privileges	Read/Modify	Notes
Archive Audit	<input checked="" type="checkbox"/>	Alone: Message Archiving login and Audit Reports
Archive Retention	<input checked="" type="checkbox"/>	Alone: Message Archiving login and Retention pages
Archive Investigator Security	<input checked="" type="checkbox"/>	Alone: Message Archiving login and, with Search, Audit, Retention, sees Admin tab
Archive Reports	<input checked="" type="checkbox"/>	Alone: Message Archiving login, and works with Search, Audit, Retention reports

Email Config Administrators

An *email config administrator* manages the inbound and outbound servers' mail flow, security, delivery, and disaster recovery configurations.

Positioning Email Config Authorization Records

The email config authorization record is usually assigned to an email config organization. This straightforward approach is shown in the following example's Eastern Division hierarchy. If your account has multiple email config organizations and only one administrator, assign an authorization record to an organization above the email config level. The example shows this configuration using the Western Division hierarchy. If your email config administrators do not manage sub-organizations, you can block the administrator access. For more information, see "Limiting Authority" on page 158.



Recommended Email Config Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

Email Config Administrator Privilege	Read/Modify	Notes
All Standard Privileges	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Help Desk	<input type="checkbox"/>	
Suspend User	<input type="checkbox"/>	
Reset User	<input type="checkbox"/>	
View Quarantine	<input type="checkbox"/>	
User Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Change Address	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Add Users	<input type="checkbox"/> <input type="checkbox"/>	
Delete Users	<input type="checkbox"/> <input type="checkbox"/>	
IM Management	<input type="checkbox"/> <input type="checkbox"/>	
Message Encryption Management	<input type="checkbox"/> <input type="checkbox"/>	
Application Management	<input type="checkbox"/> <input type="checkbox"/>	
Junk Email Settings	<input type="checkbox"/> <input type="checkbox"/>	
Sender Lists	<input type="checkbox"/> <input type="checkbox"/>	
Spam Filters	<input type="checkbox"/> <input type="checkbox"/>	
Sexually Explicit	<input type="checkbox"/> <input type="checkbox"/>	
Virus Settings	<input type="checkbox"/> <input type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/>	
Pending Quarantine	<input type="checkbox"/> <input type="checkbox"/>	
Wireless Settings	<input type="checkbox"/>	
Account Settings	<input type="checkbox"/> <input type="checkbox"/>	
Password	<input type="checkbox"/>	
Email Aliases	<input type="checkbox"/> <input type="checkbox"/>	
Regional Settings	<input type="checkbox"/> <input type="checkbox"/>	
Personal Archive	<input type="checkbox"/>	
Archive Search	<input type="checkbox"/>	
Archive Recover	<input type="checkbox"/>	

Email Config Administrator Privilege	Read/Modify	Notes
Junk Email Analysis	<input type="checkbox"/> <input type="checkbox"/>	
View Images, Attachments, and Links	<input type="checkbox"/>	
Organization Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Peer Authority	<input type="checkbox"/>	
Change Admin Passwords	<input type="checkbox"/> <input type="checkbox"/>	
Create Organizations	<input type="checkbox"/> <input type="checkbox"/>	
Delete Organizations	<input type="checkbox"/> <input type="checkbox"/>	
View Reports	<input checked="" type="checkbox"/>	
Outbound Mail Processing	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Outbound Applications Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Outbound Server Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Outbound Transport Security	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Outbound Message Encryption	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Edit Organizations	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Notification Messages	<input type="checkbox"/> <input type="checkbox"/>	
Manage Domains	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Usage Statements	<input type="checkbox"/>	
Message Center Branding	<input type="checkbox"/> <input type="checkbox"/>	
Application Management	<input type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input type="checkbox"/> <input type="checkbox"/>	
Junk Email	<input type="checkbox"/> <input type="checkbox"/>	
Virus	<input type="checkbox"/> <input type="checkbox"/>	
Wireless Email	<input type="checkbox"/> <input type="checkbox"/>	
Advanced Applications	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Attachment Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Content Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Industry Heuristics	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Message Archiving	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Web Content Manager	<input type="checkbox"/>	
Inbound Mail Processing	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org

Email Config Administrator Privilege	Read/Modify	Notes
Mail Connection Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Auto Connection Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Delivery Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Spooling	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Inbound Transport Security	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	email config org
Archive Security Administrator	<input type="checkbox"/>	archive security/ compliance
Archive Search	<input type="checkbox"/>	archive security/ compliance
Archive Discovery	<input type="checkbox"/>	security/archive
Archive Audit	<input type="checkbox"/>	security/archive
Archive Retention	<input type="checkbox"/>	security/archive
Archive Investigator Security	<input type="checkbox"/>	security/archive
Archive Reports	<input type="checkbox"/>	security/archive

Organization Policy Administrators

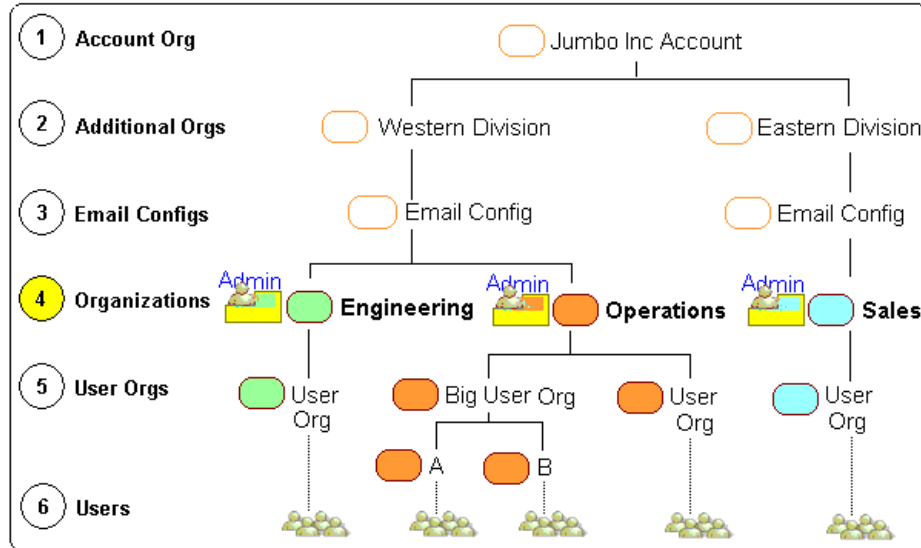
An *organization policy administrator* manages the common settings, services, and administrative controls across the organization hierarchy. This administrator also controls the Default User, common User Access options each user has in the Message Center, and Early Detection Quarantine.

An organization policy administrator can create new sub-administrators, and manage outbound mail processing configurations. This administrator does not manage Directory Sync or inbound mail processing tasks.

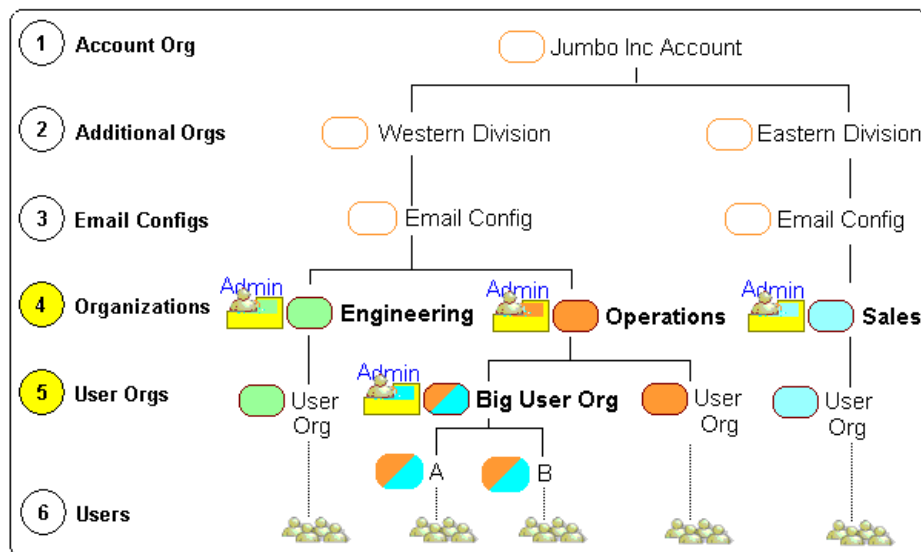
Account and organization policy administrators manage the Message Center settings. Giving these rights to other administrators has consequences. These Message Center settings should be made at the organization level. Changing the Message Center user access settings for individual users or for the Default User disconnects these users from the org-level control, and makes your organizations difficult to manage.

Positioning Organization Policy Authorization Records

An organization policy authorization record is usually assigned to a strategic organization. As illustrated in the following example, the Engineering organization has different common settings and configurations from those set up in the Operations and Sales organizations.



In an additional example of large, complex hierarchies, an organization policy administrator can have sub-administrators managing different parts of the hierarchy tree. In the following example, the Operations organization's administrator manages all of the sub-organizations. And the administrator assigned to the Big User Org shares administrative access.



Recommended Organization Policy Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

Organization Policy Administrator Privilege	Read/Modify	Notes
All Standard Privileges	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Help Desk	<input type="checkbox"/>	
Suspend User	<input type="checkbox"/>	
Reset User	<input type="checkbox"/>	
View Quarantine	<input type="checkbox"/>	
User Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Default User
Traffic Limits	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Change Address	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Add Users	<input type="checkbox"/> <input type="checkbox"/>	
Delete Users	<input type="checkbox"/> <input type="checkbox"/>	
IM Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Message Encryption Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Sender Lists	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Spam Filters	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Sexually Explicit	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Virus Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/>	
Pending Quarantine	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Settings	<input type="checkbox"/>	
Account Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Password	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Email Aliases	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Regional Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Personal Archive	<input type="checkbox"/> <input checked="" type="checkbox"/>	

Organization Policy Administrator Privilege	Read/Modify	Notes
Archive Search	<input checked="" type="checkbox"/>	
Archive Recover	<input checked="" type="checkbox"/>	
Junk Email Analysis	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
View Images, Attachments, and Links	<input checked="" type="checkbox"/>	
Organization Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	Create admins
Assign Peer Authority	<input checked="" type="checkbox"/>	
Change Admin Passwords	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Create Organizations	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Delete Organizations	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
View Reports	<input checked="" type="checkbox"/>	
Outbound Mail Processing	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config
Outbound Applications Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config
Outbound Server Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config
Outbound Transport Security	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config
Outbound Message Encryption	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	if email config
Edit Organizations	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Notification Messages	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Manage Domains	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Usage Statements	<input type="checkbox"/>	Account admin
Message Center Branding	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Virus	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Wireless Email	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Advanced Applications	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Attachment Manager	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Content Manager	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Industry Heuristics	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	

Organization Policy Administrator Privilege	Read/Modify	Notes
Message Archiving	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Web Content Manager	<input type="checkbox"/> <input checked="" type="checkbox"/>	
Inbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Mail Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Auto Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Delivery Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Spooling	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Inbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Archive Security Administrator	<input type="checkbox"/>	archive security/ compliance
Archive Search	<input type="checkbox"/>	archive security/ compliance
Archive Discovery	<input type="checkbox"/>	security/archive
Archive Audit	<input type="checkbox"/>	security/archive
Archive Retention	<input type="checkbox"/>	security/archive
Archive Investigator Security	<input type="checkbox"/>	security/archive
Archive Reports	<input type="checkbox"/>	security/archive

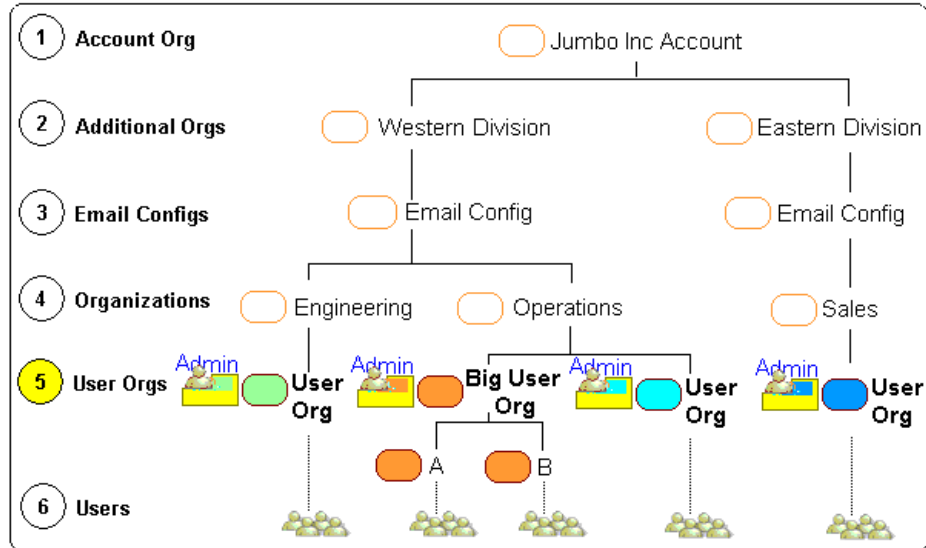
User Administrators

A *user administrator* manages the general user administration tasks such as adding, deleting, moving and suspending users, along with resetting user passwords.

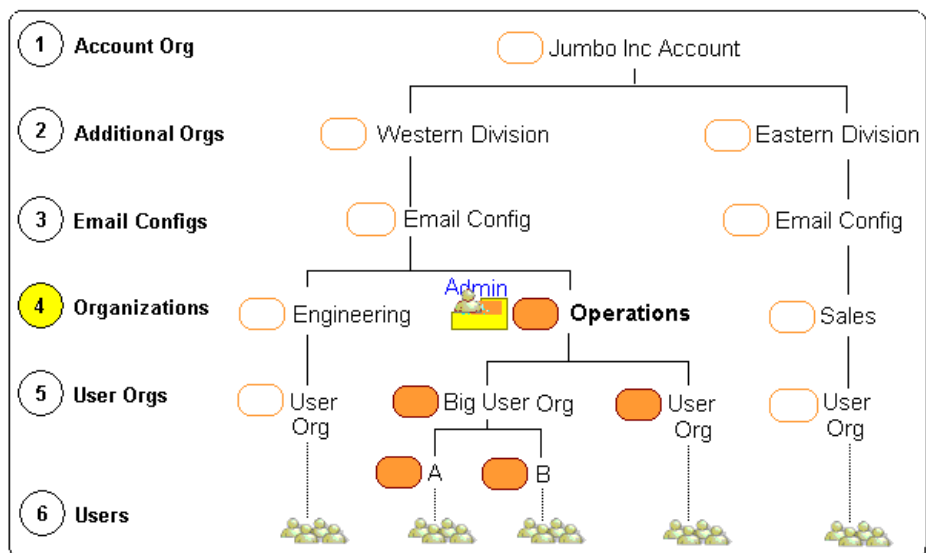
Note: This administrator does not manage the Default User or the Message Center's user-access settings. These are managed by the organization policy administrator.

Positioning User Administrator Authority Records

User administrators are generally assigned to strategic organizations that contain users. In the following example, the Big User Org user administrator has different suspend, reset, and user-management policies from the other User Orgs managed by other user administrators.



In large, complex hierarchies, a user administrator can also be assigned at a strategic managing-organization level in order to manage across several user organizations. In the following example, the user administrator assigned to the Operations organization can manage all users in the sub-organizations.



Recommended User Administrator Privilege Settings

For detailed information for each privilege, see *The Message Security Authorization Reference*.

User Administrator Privilege	Read/Modify	Notes
All Standard Privileges	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Help Desk	<input checked="" type="checkbox"/>	
Suspend User	<input checked="" type="checkbox"/>	
Reset User	<input checked="" type="checkbox"/>	
View Quarantine	<input checked="" type="checkbox"/>	
User Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Change Address	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Add Users	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Delete Users	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
IM Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Message Encryption Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Junk Email Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Sender Lists	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Spam Filters	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Sexually Explicit	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Virus Settings	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Show Delivered-As-Is	<input type="checkbox"/>	
Pending Quarantine	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Settings	<input type="checkbox"/>	
Account Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Password	<input checked="" type="checkbox"/>	
Email Aliases	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Regional Settings	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Personal Archive	<input checked="" type="checkbox"/>	

User Administrator Privilege	Read/Modify	Notes
Archive Search	<input checked="" type="checkbox"/>	
Archive Recover	<input checked="" type="checkbox"/>	
Junk Email Analysis	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
View Images, Attachments, and Links	<input type="checkbox"/>	
Organization Management	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	
Assign Authority	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Assign Peer Authority	<input type="checkbox"/>	
Change Admin Passwords	<input type="checkbox"/> <input type="checkbox"/>	
Create Organizations	<input type="checkbox"/> <input type="checkbox"/>	
Delete Organizations	<input type="checkbox"/> <input type="checkbox"/>	
View Reports	<input checked="" type="checkbox"/>	
Outbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config
Outbound Applications Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config
Outbound Server Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config
Outbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config
Outbound Message Encryption	<input checked="" type="checkbox"/> <input type="checkbox"/>	if email config
Edit Organizations	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Notification Messages	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Manage Domains	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Usage Statements	<input type="checkbox"/>	Account admin
Message Center Branding	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Application Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Traffic Limits	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Junk Email	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Virus	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Wireless Email	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Advanced Applications	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Attachment Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Content Manager	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Industry Heuristics	<input checked="" type="checkbox"/> <input type="checkbox"/>	

User Administrator Privilege	Read/Modify	Notes
Message Archiving	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Web Content Manager	<input type="checkbox"/> <input checked="" type="checkbox"/>	View pages
Inbound Mail Processing	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Mail Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Auto Connection Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Delivery Management	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Spooling	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Inbound Transport Security	<input checked="" type="checkbox"/> <input type="checkbox"/>	
Archive Security Administrator	<input type="checkbox"/> <input type="checkbox"/>	archive security/ compliance
Archive Search	<input type="checkbox"/> <input type="checkbox"/>	archive security/ compliance
Archive Discovery	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Audit	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Retention	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Investigator Security	<input type="checkbox"/> <input type="checkbox"/>	security/archive
Archive Reports	<input type="checkbox"/> <input type="checkbox"/>	security/archive

Descriptions of Privileges

You have the option of assigning a category of privileges (such as “User Settings”) or a specific privilege within that category (such as “Add Users”). By selecting a category, all privileges in the category are selected. You can then deselect specific privileges if necessary.

You may also be able to choose between “Read” and “Modify” since you might want to provide visibility into an organization (“User Settings”) but you may not want that administrator to modify those settings.

All Standard Privileges

Choosing this option provides visibility or modification privileges for all data at an organization and below. This is the most appropriate role for assigning a new “super” administrator at a newly created sub-organization. For detailed information on each privilege in this category, see *The Message Security Authorization Reference*, “All Standard Privileges”.

Help Desk

The Help Desk section describes privileges to basic user support functions in the User tab. To provide full access to Help Desk functions, administrators need authority over User Settings, and some privileges in Organization Management. These can be selected individually from the authorization record. For detailed information for each Help Desk privilege, see *The Message Security Authorization Reference*, “All Standard Privileges” chapter’s Help Desk section.

Help Desk	Enables the basic user suspend, reset, and quarantine support functions.
Suspend User	Turn off services for a user.
Reset User	Activate services for a suspended user and revert an active user to the Default User settings.
View Quarantine	Search, view, and deliver the messages currently held in a user’s Message Center.

User Settings

All privileges related to user settings. For detailed information for each User Settings privilege, see *The Message Security Authorization Reference*, “All Standard Privileges” chapter’s User Settings section.

User Settings	Enables read and modify privileges to a large set of common user policies.
Traffic Limits	Set the daily number of messages and maximum size messages a user can receive before email will bounce back to the sender.
Change Address	Change a user’s address (the Message Center account and all related services are preserved)
Add Users	If your product has this configuration, you can add new users to an organization.
Delete Users	If your product has this configuration, you can delete users from an organization.
IM Management	Enables IM administrative functions.
Message Encryption Management	Enables Encryption Settings pages for users, orgs, and Default User settings.
Application Management	Turn on/off a user’s applications and settings, if the services are available to an organization’s users. In turn, an administrator can enable these settings to be viewable and editable by the end user.
Junk Email Settings	Enables the administrator’s viewing and modification of the Spam filters in the Message Center.

Sender Lists	Enables reading and modifying a user's sender lists.
Spam Filters	Enables the reading and modifying of the user's spam filters.
Sexually Explicit	Enables users to see or modify their filter for sexually explicit content.
Virus Settings	Enables user-level virus blocking to be turned on or off, and enables limiting the interval for virus notifications.
Show Delivered-As-Is	Enables an administrator to give a user the ability to deliver virus-infected messages from the Message Center to their inbox.
Pending Quarantine	Enables an administrator to give a user the ability to either view or deliver quarantined messages in the Pending quarantine page of the Message Center.
Wireless Settings	Enables Wireless Forwarding from the Message Center to text-enabled mobile devices.
Account Settings	Enable/disable all account setting privileges at once. The account settings include Password, Email Aliases, and Regional Settings privileges.
Password	If your product has this configuration, you can enable the administrator to see a user's initial password, to reset a user's password, to generate a temporary password, and to allow users change their passwords in the Message Center.
Email Aliases	Enables administrators to let users see and, if your product has this configuration, you can modify any aliases in their Message Center account
Regional Settings	Enables administrators to manage a user's language settings in the Message Center.
Personal Archive	Enables an administrator to give a user access to the user's personal archive in the Message Center.
Archive Search	Enables the administrator to let users search for and view any archived email message that they have either sent or received in their Personal Archive.
Archive Recover	Enables an administrator to let a user export messages from the user's Personal Archive by forwarding them to the user's email address.
Junk Email Analysis	Enables administrators to let users see "Why this email was quarantined" link in the Message Center.
View Images, Attachments, and Links	Enables administrators to allow user access to view images, attached files and hyperlinks within quarantined messages in the user's Message Center.

Organization Management

All privileges related to the organization hierarchy. For detailed information for each Organization Management privilege, see *The Message Security Authorization Reference*, “All Standard Privileges” chapter’s Organization Management section.

Organization Management	Enables access to all privileges related to the organization hierarchy.
Assign Authority	<p>Create and modify administrator authority in sub-organizations.</p> <p>WARNING: By granting this privilege to another administrator, that administrator in turn can create other administrators at a lower organization-level with equivalent authority. The Assign Authority privilege should generally be given only to a single “super” administrator at the lower level or an administrator with a specific role in your organization.</p>
Assign Peer Authority	<p>Create and modify peer administrators in the same organization.</p> <p>WARNING: By granting this privilege to another administrator, that administrator in turn can create other administrators at a lower organization-level with equivalent authority. The Assign Authority privilege should generally be given only to a single “super” administrator at the lower level or an administrator with a specific role in your organization.</p>
Change Admin Passwords	If your product has this configuration, you can enable administrators to change a sub-administrator’s password.
Create Organization	Enables creating new sub-organizations.
Delete Organization	Enables the deletion of a sub-organization.
View Reports	Enables the viewing of inbound and outbound reports.
Outbound Mail Processing	Configure and modify outbound servers and services.
Outbound Applications Management	Enables managing the outbound services consisting of virus blocking, attachment manager, content manager, and the compliance footer.
Outbound Server Management	Enables the management of the Outbound Server configurations found in the Outbound tab at the top of the Administration Console.

Outbound Transport Security	Enables Transport Layer Security (TLS) configurations for outbound mail.
Outbound Message Encryption	Enables outbound messages to be sent to a secure portal.
Edit Organizations	Modify organization settings.
Notification Messages	Enables Message Center and Attachment Manager notification messages.
Manage Domains	If your product has this configuration, you can allow administrators to view and modify domains.
Usage Statements	Allows an administrator to view the account organization's monthly usage data.
Message Center Branding	Allows administrators to configure Message Center branding options.
Application Management	Allows administrators to assign read and modification privileges for the primary organization application categories.
Traffic Limits	Sets organization's message limits.
Junk Email	Enables administrators to read and modify an organization's spam filters and sender lists.
Virus	Enables administrators to read and modify virus blocking.
Wireless Email	Enables administrators to configure an organization's or a user's User Access privileges for a user's wireless email.
Advanced Applications	Settings for the inbound applications at the organization-level.
Attachment Manager	Enables the Inbound Attachment Manager functions and reports.
Content Manager	Enables administrative management of the Content Manager features and reports.
Industry Heuristics	Enables the administration of the industry specific features.
Message Archiving	Enables administration of the Message Archiving features.
Web Content Manager	Enables the Web Content tab with Web Content dashboard, Anti-Virus, Spyware, Filtering, and Web Admin pages.

Inbound Mail Processing

For detailed information for each Inbound Mail Processing privilege, see *The Message Security Authorization Reference*, “Inbound Mail Processing” chapter.

Inbound Mail Processing	If your product has this configuration, you can assign read and modification privileges for inbound mail applications managed under the Inbound Servers tab.
Manual Connection Management	If your product has this configuration, you can create manual IP blocks
Auto Connection Management	If your product has this configuration, you can configure the Connection Manager automatic attack blocking. This privilege is required to view graphs and data on the Inbound Server Overview page.
Delivery Management	If your product has this configuration, you can configure the Delivery Manager.
Spooling	If your product has this configuration, you can configure the Spool Manager.
Inbound Transport Security	If your product has this configuration, you can enable TLS settings for the Inbound Servers tab.

Archive Search, Archive Discovery, Archive Audit, Archive Retention

For detailed information for each Archive Search and Archive Audit privilege, see *The Message Archiving Administration Guide*, “Granting Message Archiving Privileges” chapter.

Archive Security Administrator	Enables the management of account-wide Message Archiving functionality including Archive Search/Discovery, Retention, Audit and Investigator Security.
Archive Search	Enables the Message Archiving pages for archive and investigation functions.
Archive Discovery	Enables the investigation of saved items, creating search criteria, and managing exported message in addition to the core Archive Search features.
Archive Audit	Enables the Message Archiving’s Audit Reports page.
Archive Retention	Enables message retention, message purges, and a purge history.

Archive Investigator Security	Restricts an archive search investigation to the messages for 50 or less users.
Archive Reports	Enables the Message Archiving Reports tab. Access to specific reports is based on having additional archive settings.

Troubleshooting Authorization

What are the authorization privileges necessary to view the Inbound Server or Outbound Server tab?

At a minimum, read privileges for “Auto Connection Management” are required to view the Inbound Server tab, and read privileges for “Outbound Server Management” are required to view the Outbound Server tab. These tabs are associated with an email config-level authorization record.

Why can't an administrator see server configuration information?

The administrator's authorization record was added to an organization below the email config in the organizational hierarchy. You must add an additional authorization record to the email config. See “Viewing and Editing Authorization Records” on page 164 for instructions.

Chapter 8

Directory Sync

About Directory Sync

Note: This chapter describes Directory Sync Hosted Edition, which is set in the Administration Console and pulls data from your server using DSML. If you are interested in the Directory Sync Server Edition utility, which runs on your server and pushes data to the service, see the following URL:

http://www.postini.com/dir_sync

Directory Sync makes user management easier by connecting to your directory server and collecting user information. Directory Sync imports this information into the message security service. It will add, delete or move users so that your organization matches an *organizational unit* (OU) on your directory server.

Directory Sync is an optional feature. For more information about the availability of this feature, contact your account manager or vendor.

Directory Sync acts as a one-way synchronization. Your user and alias information in the message security service may be added, moved or deleted, but your directory server is not changed in any way. Directory Sync can be launched manually from the Administration Console or scheduled to run automatically.

To use Directory Sync, set up your directory server to accept a DSML client over SSL. For information on how to configure your directory server, see the *Directory Sync Configuration Guide*.

Features and Capabilities

The following features are included with Directory Sync:

- **Support for Major LDAP Servers:** Support for Windows Active Directory 2000 and 2003, IBM Lotus Domino Directory Server, and Sun ONE Directory Server.
- **User Management:** Directory Sync will add, delete, and move users and aliases.
- **One-way pull:** Directory Sync pulls information from your directory server to the message security service to map your user base in one or more organizations
- **Automated Synchronization:** Directory Sync can be scheduled to synchronize automatically on a regular schedule.
- **Operation Limits:** Safeguards to limit number of deletion and addition of user accounts in the message security service with validation of data and configuration before writes to the message security service user organization.
- **LDAP Filtering:** You can specify full LDAP queries in the Advanced Filter Settings page.
- **Secure data transmission:** Directory Sync uses secure 128-bit SSL for all connections.
- **Reporting:** Directory Sync includes immediate validation reports, emailed reports, and a seven-day activity log.

Requirements

To use Directory Sync, you'll need to set up DSML with SSL on an internet facing machine and possibly perform some configuration on your LDAP directory server and the message security service.

Prerequisites

To set up Directory Sync, you'll need:

- Familiarity with DSML (Directory Services Markup Language).
- An understanding of the message security service hierarchy and configuration. Proper setup requires familiarity with your organization hierarchy and the message security service settings.
- An understanding of your LDAP hierarchy and services. To configure Directory Sync, you must provide information about your LDAP hierarchy. You'll need to be familiar with your directory server, and with LDAP technologies.

Note: Activation involves accessing and configuring your LDAP directory and associated technologies.

We highly recommend you purchase Directory Sync Activation Service if:

- You need assistance with these technologies.
- Your LDAP directory structure or your the message security service organization hierarchy is complex.

For a full description, see “Directory Sync Activation Service” on page 208.

System Requirements

Following are a summary of the requirements to configure and support Directory Sync. For complete steps on how to set up your system, see the *Directory Sync Configuration Guide*

- A directory server containing your user information. Directory Sync is compatible with IBM Lotus Domino Directory Server, Sun ONE Directory Services, IBM Lotus Notes Directory Server, and Microsoft Active Directory 2000 and 2003.
- A user with administrative READ rights to your LDAP/OU. Directory Sync will collect information with this user name.
- You'll need to install a single DSML server on an existing or new server.
- An open SSL connection. Directory Sync will connect to your DSML server through SSL. You'll need to set up your server to accept an SSL connection, and you'll need to set your firewall to allow the connection.
- An SSL certificate for transactions. To allow SSL connections, you'll need an SSL certificate. Directory Sync will accept any certificate authority, including self-signed certificates.
- A administrator account in the message security service with appropriate privileges. To set up and run Directory Sync, you will make changes to organization and user settings. Running Directory Sync requires permissions to add, move and delete users and aliases.

Directory Sync Activation Service

When you purchase Directory Sync Activation services, you receive the following assistance with setting up and configuring Directory Sync:

- Determine project schedule and job summary
- Review your system requirements and network topology
- Install and configure DSML a single DSML server on an existing or new server to use Directory Sync.
- Recommend and assure the proper SSL certificates are installed
- Set up authorized user accounts in your LDAP directory for DSML connection
- Review your LDAP Directory structure and Organization Hierarchy, and requirements for synchronization.
- Determine strategy for mapping user structures from LDAP to the message security service.
- Manage exclusions such as mailing lists and special user accounts
- Perform testing and validation; setup auto scheduling
- Document the customized setup and configuration, and process.

For more information on the Directory Sync Activation service, please contact professionalservices@postini.com or your vendor.

Directory Sync Concepts

When you use Directory Sync to synchronize your registered user list with your directory server, users are added, deleted, or moved so that the user list on the message security service matches the user list on your directory server.

- A user is *added* to the message security service if the *canonical name* (CN) is listed in your directory server, but not in the message security service.



For instance, you may have two users in the message security service, Ann and Brian, and three CNs in your directory server, Ann, Brian and Juanita. When you run Directory Sync, Juanita will be added to the message security service.

- A user is *moved* within your organization hierarchy if the *canonical name* (CN) is listed in your directory server, and registered as a user in a different organization in the message security service.



For instance, you may have two users, Ann and Brian, in your primary organization in the message security service, and one user, Emil, in a different organization, but all three users are in the same OU in your directory server. When you run Directory Sync from your primary organization, Emil will be moved to the primary organization.

- A user is *deleted* if the *canonical name* (CN) is not listed in your directory server, but is registered in the message security service.



For instance, you may have four users in the message security service, Ann, Brian, Juanita and Manish, and three CNs in your directory server, Ann, Juanita and Manish. When you run Directory Sync, Brian will be deleted from the message security service.

Directory Sync updates your users in the message security service in three steps:



1. Directory Sync connects with your server securely, using information you provide. Directory Sync will collect information on users, and optionally on aliases and organizations. No changes are made to your directory server.
2. Directory Sync creates a list of changes to your users, based on the user list from your directory server. Directory Sync changes your users in the organization in the message security service to match the OU in your directory server.
3. Directory Sync updates your users. This is very similar to running a batch command. Directory Sync executes the list of changes it has generated from the directory server.

Special Users

Normally, Directory Sync sets up your organization in the message security service to match the OU on your directory server exactly. In some cases, there are special users that don't belong on both lists.

Special users that might be unintentionally deleted

If you have users in the message security service that aren't listed on the directory server, such as accounts just for mailing lists or aliases, those users will be deleted. This might include a catchall user, an administrative user, or an alias used for mailing lists.

Move these users to another organization, or add these users to your directory server.

WARNING: Any users who are not listed in your directory server will be deleted from the message security service.

Special users that might be unintentionally added

You may have any CNs on your directory server which should not be added to the message security service. For instance, if you have internal mailing lists, they may be added to the message security service if they are listed as CNs in your directory server.

To prevent adding these users, you can set Directory Sync to exclude users from being added or moved, based on an attribute in your directory server. See “Organization Exclusions” on page 222 for more information.

Planning Directory Synchronization

To assure that your organizations map correctly, plan your synchronization before you begin to configure Directory Sync.

Map Your Organization Hierarchies

When planning for Directory Synchronization, you decide how your user organizations on the message security service will map to the organizations on your directory server.

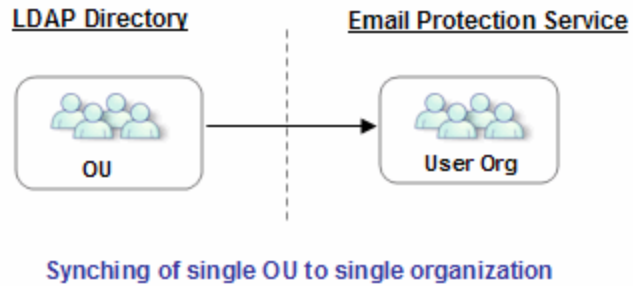
Directory Sync is set up on a specific user organization, and synchronizes that organization with an organization unit (OU) on your directory server. You have the option to synchronize with one particular organization unit, or with a whole subtree, starting with that organizational unit.

When you decide how to configure Directory Sync, compare your organization hierarchy in the message security service and your organization hierarchy on your LDAP server.

Scenario One: Simple Hierarchies

The simplest type of synchronization is when both sides have a single organization:

- One organization in the message security service.
- One organizational unit in your directory server.



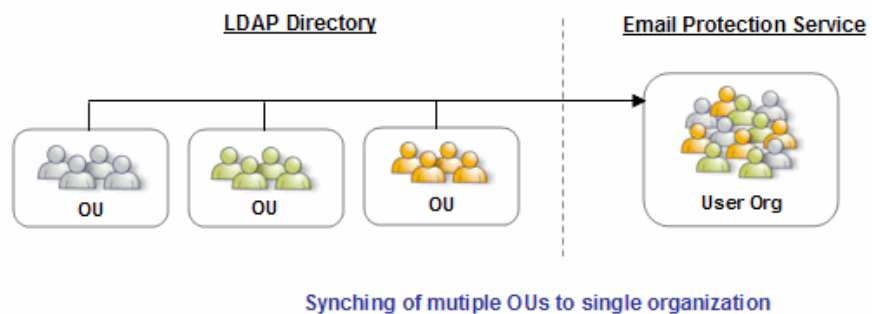
Set up Directory Sync on the one user organization, to map to the one OU on the directory server.

You may need to create another user organization in the message security service for users not listed in your OU (such as catchall users). This organization should not have any synchronization set up.

Scenario Two: Combining Hierarchies

Alternately, you may have a situation in which your directory server has a complex hierarchy, but your hierarchy on the message security service is very simple:

- One organization in the message security service.
- A full tree of OUs in your directory server.



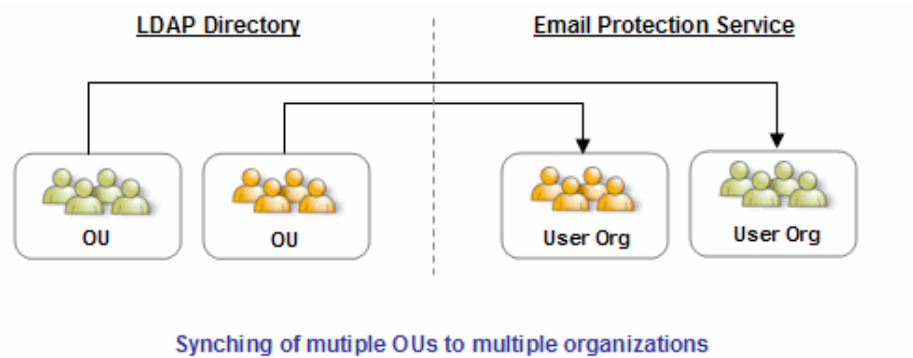
In such a situation, set up Directory Sync on a single organization, and map to the highest level OU on the directory server. Then, set Directory Sync to search the entire subtree. Your single user organization on the message security service will hold all your users for the whole directory server subtree.

You may need to create another user organization in the message security service for users not listed in your OU (such as the legacy catchall user feature). This organization should not have any synchronization set up.

Scenario Three: Matching Hierarchies

If you have several organizations on the message security service, you'll need to plan more carefully. In this scenario:

- Both your organization hierarchy on the message security service and on your directory server have multiple organizations.
- These organizations match one-for-one.



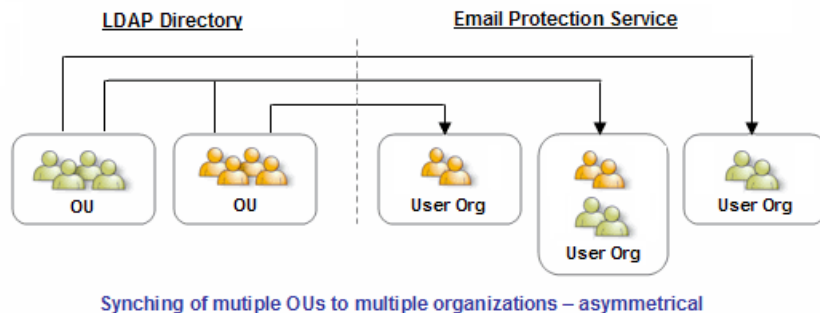
You'll need to set up Directory Sync on several organizations in the Admin Console. For each organization, set Directory Sync to use the base DN of the corresponding OU in the directory server. Be sure to match the structure one-for-one.

You may need to create another user organization in the message security service for users not listed in your OU (such as the legacy catchall user feature). This organization should not have any synchronization set up.

Scenario Four: Complex Non-Matching Hierarchies

If you have more than one user organization, and the directory server doesn't match the hierarchy on the message security service, you have several options. In this situation:

- Both your organization hierarchy on the message security service and on your directory server have multiple organizations.
- There is no simple match between organizations.



In this case, you have three options.

1. Set a mapping attribute on your LDAP server.
2. Map organizations partially.
3. Change your org hierarchy.

You can update your directory server to include information about the message security service, and set Directory Sync to add users to the organization specified on your directory server. See "Organization Hierarchy Mapping" on page 221 for more information.

It's possible that some of your organizations will match and others will not. In this case, you may be able to set up Directory Sync for the matching organizations. You can also exclude organizations on your directory server from synchronization, by using an exclusion attribute. Be careful with setting up partially-matching hierarchies. When you synchronize, users may be moved from other organizations, or deleted, to match the organizational unit on the directory server. Be sure to check the validation page carefully to be sure you are not making any unexpected or unwanted changes.

Alternately, consider reorganizing your hierarchy to better fit Directory Sync. There are two ways to reorganize your hierarchy:

- Consolidate all users into a single organization on the message security service. If you consolidate in this way, you'll have a Simple Non-Matching Hierarchy, as detailed in Scenario Two.
- Change your structure to match your directory server. This will require more work, but will allow you to maintain a complex organization hierarchy. If you reorganize in this way, you'll have a Complex Matching Hierarchy, as detailed in Scenario Three.

Configuring Your Directory Server

To connect with your directory server and synchronize data securely, Directory Sync makes a connection over SSL using the DSML protocol.

You'll need to set up the following on your directory server:

- Directory Server Markup Language (DSML) support.
- Secure Sockets Layer (SSL) security, with a certificate from any authority.
- Basic Authentication, with read permissions for an admin user.

For more information about setting up your directory server to work with Directory Sync, see the *Directory Sync Configuration Guide*.

Setting Up Directory Sync

Set up Directory Sync only in the organization in the message security service which contains your users. You can return to the Edit Configuration Settings page to change your settings at any time.

If you are not sure which organization to use, use the organization which contains your domain.

Note: Before you can set up Directory Sync, you'll need to configure your directory server to allow Directory Sync to connect and synchronize. See "Configuring Your Directory Server" on page 215 for more information.

To Set Up Directory Sync:

4. Log into the Administration Console.
5. From the Choose Org dropdown box, select the user organization you want to use for synchronization.

- On the Organization settings page, click the Directory Sync icon.



- On the Edit Configuration Settings page, fill out all required fields. See “Directory Sync Settings” on page 216 for more information.
- Click Save Configuration.

Directory Settings	Distribution Lists Settings
<p>*Authorized User: <input type="text"/></p> <p>*Password: <input type="password"/></p> <p>*Host: <input type="text"/></p> <p>*Path: <input type="text"/></p> <p>*Port: <input type="text" value="443"/></p> <p>*Server Type: <input checked="" type="radio"/> MS Active Directory <input type="radio"/> SunOne <input type="radio"/> IBM Lotus Notes</p> <p>*Base DN: <input type="text"/></p> <p>*Email Address Attribute: <input type="text"/></p> <p>Alias Attribute: <input type="text"/></p> <p>Org Mapping Attribute: <input type="text"/></p> <p>User Mapping Attribute: <input type="text"/></p> <p>Org Exclusion Attribute: <input type="text"/></p> <p>User Exclusion Attribute: <input type="text"/></p> <p>IM Screen Name Attribute: <input type="text"/></p>	<p>Email Address of The Lists Owner: <input type="text"/></p>
	<p>Options</p> <p>Search Entire Subtree: <input type="radio"/> yes <input checked="" type="radio"/> no</p> <p>Email Summary Reports To: <input type="text"/></p>
	<p>Operation Limits</p> <p>Add User: <input type="text"/></p> <p>Delete User: <input type="text"/></p> <p>Add Alias: <input type="text"/></p> <p>Delete Alias: <input type="text"/></p> <p>Total Changes: <input type="text"/></p>

Directory Sync Settings

Directory Sync uses the following settings:

Authorized User	<p>Authorized user name on your directory server. Directory Sync will log in with this user name.</p> <p>This should be a user on your directory server with read access.</p> <p>Example: dsadmin</p>
Password	<p>Password for the user provided in Authorized User. This is a case-sensitive password for your directory server.</p> <p>Example: 1YrPwHere1</p>

Host Name	<p>Domain Name of your company directory server. The host name is not a URL (i.e., it does not begin with http://).</p> <p>WARNING: If you are using Active Directory or SunONE, the host name cannot be an IP address. You can use an IP address for IBM Lotus Notes only.</p> <p>Example: <code>activedir.jumboinc.com</code></p>
Path	<p>The path to the DSML module on your directory server. This path should begin with a forward slash. The host name and path together determine the location of the directory server.</p> <p>Sun ONE Example: <code>/dsml</code></p> <p>Active Directory Example: <code>/dsml/adssoap.dsmlx</code></p> <p>IBM Lotus Notes Example: <code>/soap/servlet/messagerouter</code></p>
Port	<p>Directory Sync uses SSL to connect to the remote directory server. Port 443 is the default port used to connect to an LDAP directory server over SSL and will be the most common setting for this field. If you have configured this port differently on your server, you may need to specify a different port number. Note that this is different from the standard LDAP port number of 389. The port number should not include a leading colon.</p> <p>Example: <code>443</code></p>
Server Type	<p>The directory server you are using. If you are using Microsoft Exchange, most likely you will be using an Active Directory Server.</p> <p>Choices are Active Directory, Sun ONE DS or IBM Lotus Notes.</p>

<p>Base DN</p>	<p>A comma-separated sequence of name-value pairs. The Base DN (distinguished name) specifies the address, node, or search base in the directory server from which Directory Sync will extract the user entries. You will need to collect this information from your directory server administrator.</p> <p>Sun ONE Example: <code>uid=mailuser,ou=people,dc=jumboinc,dc=com</code></p> <p>Active Directory Example: <code>cn=administrator,cn=users,dc=jumboinc,dc=com</code></p> <p>IBM Lotus Notes Example: <code>ou=people,dc=jumboinc,dc=com</code></p> <p>Note: If you are using IBM Lotus Notes to collect distribution lists, leave this value blank. Distribution lists are found only at the root level for IBM Lotus Notes.</p>
<p>Email Attribute</p>	<p>The LDAP attribute for email addresses. The most common value for this attribute is <code>mail</code>.</p> <p>Example: <code>mail</code></p>
<p>Alias Attribute (Optional)</p>	<p>The LDAP attribute used to store user's mail aliases. If you do not enter an Alias Attribute, then aliases will not be synchronized.</p> <p>Sun ONE Example: <code>mailAlternateAddress</code></p> <p>Active Directory Example: <code>proxyAddresses</code></p> <p>IBM Lotus Notes Example: <code>cn, mail</code></p> <p>You can also add a comma-separated list of up to three attributes. Attributes after the third are ignored.</p> <p>Example: <code>mail, proxyAddress, extensionAttribute1</code></p>
<p>Org Mapping Attribute (Optional)</p>	<p>An LDAP attribute for an organization to specify where the organization should be added or moved in the message security service organization hierarchy. See "Organization Hierarchy Mapping" on page 221 for more information.</p> <p>If you do not set this attribute, users will be added or moved to the organization where Directory Sync is run.</p> <p>Example: <code>extensionAttribute1</code></p>

<p>User Mapping Attribute (Optional)</p>	<p>An LDAP attribute for a user to specify where the user should be added or moved in the message security service organization hierarchy. See “Organization Hierarchy Mapping” on page 221 for more information.</p> <p>If you do not set this attribute, users will be added to the organization where Directory Sync is run.</p> <p>Example: <code>extensionAttribute12</code></p>
<p>Org Exclusion Attribute (Optional)</p>	<p>An LDAP attribute for an organization to specify that all users in the organization should be excluded from Directory Sync. See “Organization Exclusions” on page 222 for more information.</p> <p>Example: <code>extensionAttribute9</code></p>
<p>User Exclusion Attribute (optional)</p>	<p>An LDAP attribute for a user to specify that the user should be excluded from Directory Sync. See “Organization Exclusions” on page 222 for more information.</p> <p>Example: <code>isDeleted</code></p>
<p>IM Screen Name Attribute (optional)</p>	<p>An LDAP attribute used to import IM Screen Names from Directory Sync. Only usable if you are using Postini IM Security.</p> <p>WARNING: This feature is incompatible with IM Security self-registration feature.</p> <p>Example: <code>extensionAttribute7</code></p>
<p>Email Address of the Lists Owner (optional)</p>	<p>All mailing lists on your LDAP server will be imported as aliases to this address. You can use this option to avoid Directory Sync adding mailing lists in your LDAP directory as users.</p> <p>The address should be the address of registered user under the same email config organization. Owner address.</p> <p>If this field is left blank, the mailing lists are imported as users.</p> <p>This field is supported only in Microsoft Active Directory and IBM Lotus Notes.</p> <p>Note: If you are using IBM Lotus Notes to collect distribution lists, set Base DN to empty and set Search Entire Subtree on. Distribution lists are found only at the root level for IBM Lotus Notes.</p> <p>For information about excluding mailing lists from synchronization, see “Organization Exclusions” on page 222.</p>

Search Entire Subtree (Optional)	<p>If this setting is enabled, Directory Sync will collect information not only for the Base DN specified, but for the whole subtree below. Directory Sync will add all users in the subtree to the message security service. If you do not set up Organization Hierarchy Mapping, users will be added to the organization where Directory Sync is set.</p> <p>If you're synchronizing a single organization on the message security service to a whole organization hierarchy on your directory server, choose "yes." Otherwise, choose "no."</p> <p>If you use a mapping attribute or org exclusion attribute, you must set this to "yes."</p>
Email Summary Reports to: (Optional)	<p>Enter a valid email address in the "Email Summary Reports to" field. Notifications will be sent to this address whenever synchronization occurs. This is especially useful if you have Automatic Synchronization enabled.</p> <p>The subject of the email summary report is "Directory Synchronization Notification." The sender is the Support Contact for the current organization, with the name "DirSync Manager."</p> <p>If Directory Sync tries to synchronize with your directory server and fails during a scheduled synchronization, Directory Sync sends an alert to this address. This message contains information on why the synchronization failed for further troubleshooting.</p>

Operation Limits

Operation Limits help prevent unexpected extreme changes. You can specify a maximum number of individual changes permitted for a single synchronization. If this number is exceeded, an error will be displayed during validation and no synchronization will occur. For each field, specify a value. To allow an unlimited number of changes, leave the field blank.

Add User	Maximum number of users to add
Delete User	Maximum number of users to delete
Add Alias	Maximum number of aliases to add
Delete Alias	Maximum number of aliases to delete
Total Changes	Total maximum number of user and alias changes (including all four changes listed above)

Advanced Filtering

Use the Advanced Filtering page to fine-tune synchronization. You can add exclusion and mapping attributes to your LDAP server, and use these to filter your imports. Alternately, you can specify an LDAP query for filtering.

The screenshot shows the 'Directory Synchronization: Advanced Filtering' configuration page. At the top, a warning box states: 'Configuration settings must be entered before directories can be synchronized. These settings apply to the current Org only and not the underlying hierarchy of Orgs.' Below this, the page title is 'test Docs Customer1 Users' with links for 'View Log', 'Directory Settings', 'Advanced Filtering', and 'Auto Sync Scheduling'. The main content area is titled 'Select either (1) Org and User Filters or (2) LDAP Filter.' There are two radio button options: 'Org and User Filters (specifies org and user mapping and exclusion attributes)' and 'LDAP Filter (sets up conditions for defining which objects should be synchronized)'. The 'Org and User Filters' option is selected. It includes fields for 'Org Mapping Attribute', 'User Mapping Attribute', 'Org Exclusion Attribute', and 'User Exclusion Attribute'. The 'LDAP Filter' option is also visible, with a text input field and a 'Convert to DSML >>' button. Below the input field, an example is provided: 'For example: objectclass=*'. At the bottom, there are 'Save' and 'Cancel' buttons.

Organization Hierarchy Mapping

You can customize organization mapping by setting a special attribute in your LDAP server. For example, most your LDAP server may be added to the “jumboinc-com” organization in the message security service, but a few may belong in “jumboinc Power Users”. You could specify “jumboinc Power Users” as an attribute in your LDAP server in an extension attribute, then note this attribute in Directory Sync. Directory Sync will add or move users to the organization specified.

User Mapping lets you to set a different organizations for users in the same OU, by setting a user attribute. Org Mapping lets you specify a single organization for each OU, by setting an org attribute, which can be useful if you are searching an entire subtree. If you are using both, User Mapping takes precedence over Org Mapping.

WARNING: User Mapping attributes are not restricted to sub-organizations. User Mapping can cause Directory Sync to add users to organizations with the same parent as the organization where Directory Sync is run. However, *Directory Sync will not delete these users, even if they are later removed from your server.*

Set Up User Mapping

1. In the Administration Console, collect the org name (or org ID number) of every organization which will contain users.

2. On your directory server, set a custom attribute to contain this information. For each CN that you want to synchronize to a separate organization, set the custom attribute to the org name (or org ID number) on the message security service.
3. In the Administration Console, configure the User Mapping Attribute to the name of the custom attribute you used on your server.

Whenever you synchronize, Directory Sync will check the mapping attribute. If the attribute is not empty, Directory Sync will add or move the user to the specified organization.

Set Up Org Mapping

1. In the Administration Console, collect the org name (or org ID number) of every organization which will contain users.
2. On your directory server, set a custom attribute to contain this information. For each OU (*organizational unit*) that you want to synchronize to a separate organization, set the custom attribute to the org name (or org ID number) on the message security service.
3. In the Administration Console, configure the Org Mapping Attribute to the name of the custom attribute you used on your server.

Org Mapping applies to each organization in your directory server separately. An organization's setting does not affect sub-organizations.

Organization Exclusions

You may have some users or organizations which you wish to exclude from synchronization. In these situations, set up an exclusion list to block users and orgs from being affected.

You will need to have a specific attribute in your directory server that marks whether to exclude a user or org. For instance, you may use the Active Directory attribute `isDeleted` to avoid adding invalid users. You can also use a custom attribute, such as `extensionAttribute1`, and populate your LDAP server so that users who should not be copied have non-blank values in this field.

In the message security service, enter the attribute's name in the User Exclusion Attribute field. If this attribute is not empty for a user on your LDAP server, Directory Sync will not add the user to the message security service, but will not delete the user if the user already exists.

You can also exclude a whole org from being synchronized. Use the Org Exclusion Attribute. If the attribute is not empty for an organization on your LDAP server, Directory Sync will not add any users in that organization. The Org Exclusion Attribute is normally only used when you enable the Search Entire Subtree option. To exclude a whole forest, set the exclusion attribute on each organization in the forest.

LDAP Filtering

You can use standard LDAP filtering expressions to filter your queries. LDAP filtering is a powerful language that allows complex filtering queries. Criteria of the query can reference any extension attributes for the OU or user.

LDAP Filter is not compatible with Mapping or Exclusion Attributes. If you are using LDAP Filter, Mapping and Exclusion Attributes are disabled.

To set up LDAP filtering:

1. In the Directory Sync configuration page, click on Advanced Filtering.
2. Select the LDAP Filter radio button.
3. Specify an LDAP query. For instance, you might enter

```
office=SF
```

You can enter an LDAP query up to 1000 characters long.

4. Click Convert to DSML to view the rule in DSML for troubleshooting.
5. Click Save to save your changes.

Note: Directory Sync's LDAP query structure follows RFC 2254 (International Standard on LDAP Filters). While some implementations of LDAP queries allow a shorthand use of the ! ("not") operator without parentheses, this is not supported by RFC 2254. Therefore, include parentheses when using the ! ("not") operator. For example, your filter should be formatted as "(!(extensionAttribute10=*))" instead of "(!extensionAttribute10=*)".

Synchronizing

When you have set up your directory server to accept connections, and entered connection information in the Administration Console, you'll be able to synchronize.



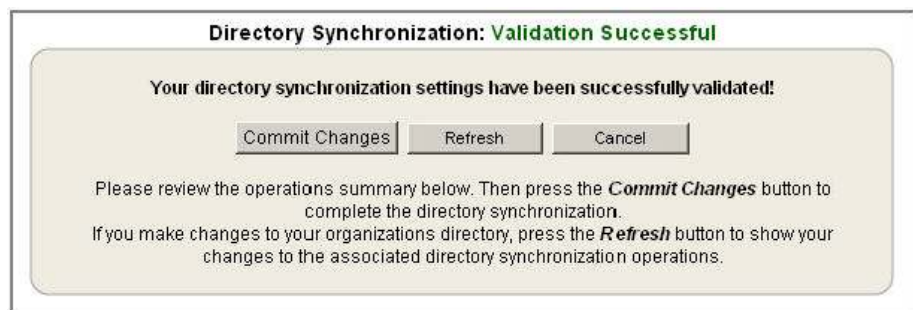
When you click Synchronize Directory, the message security service connects to your directory server and collects a list of users and aliases. Then Directory Sync compares this to your existing registered users, to determine what changes need to be made.

To synchronize your directory:

1. In the Choose Org dropdown box, select the org you want to synchronize.
2. Click Directory Sync to go to the Current Settings page.
3. In the Directory Sync page, edit your settings as needed.
4. Click Synchronize Directory to connect to your directory server and collect a list of updates. This may take several minutes. When this is complete, you'll see a summary.
5. On the Validation page, review the synchronization, and check to be sure that any changes proposed are correct. If needed, change your Directory Sync settings and synchronize again.

Validation

Before any changes are made, Directory Sync displays a validation page. No changes will be made until you confirm changes.



The Validation page also acts as a test for connectivity. If Directory Sync was unable to connect to your directory server, you will see an explanatory error message on the Directory Server page.

On the Validation page, you'll see exactly what changes will be made to your organization. If these changes are acceptable, click Commit Changes.

Validation may take several minutes to complete, especially if you have over 5,000 users.

Validation is complete when Directory Sync connects to your directory server and maps to the Base DN in your directory tree.

The resulting Validation Success page contains a preview of the changes that could be made. This Synchronization Summary lists failed operations, totals for each operation (`deleteuser`, `deletealias`, `adduser`, `addalias`, and modifications), and the total changes made. Below the totals for these operations is a list, broken down by operation, with the specific actions and associated server messages.

Synchronization Preview						
Errors: 0	Delete Users: 0	Delete Alias: 0	Add Users: 40	Add Aliases: 24	Modifications: 15	Total Changes: 79
Delete Aliases (0)						
deletealias alias1.1@p.com						
deletealias alias2.1@p.com						
deletealias alias3.1@p.com						
deletealias alias1.2@p.com						
deletealias alias2.2@p.com						

From this page, you can complete the directory synchronization by pressing the Commit Changes button.

Note: If there are no changes to commit, or the number of changes exceeds the Operation Limits you specified in configuring Directory Sync, you will not see the Commit Changes button and will not be able to make changes.

If you make changes to your server to fix potential errors, press the Refresh button to refresh the Synchronization Summary. Pressing the Cancel button returns you to the Orgs page.

Commit Changes

When you click Commit Changes, Directory Sync will update your user list in the message security service. This can take several minutes.

When changes are complete, you will see the Synchronization Results page. The Synchronization Results page contains the actual results from the synchronization operation.

If errors occur during the synchronization, commands associated with the failed operation may be skipped. For example, if an `adduser` command fails, the associated `addalias` operations will be skipped.

Viewing Current Settings

After you have configured Directory Sync, you will be directed to the Current Settings page when you click the Directory Sync icon. This page shows your synchronization settings, and acts as a starting page for all Directory Sync actions.

Directory Synchronization: Current Settings

Press the **Synchronize Directory** button to validate your configuration settings and summarize the actions associated with the directory synchronization.

[Synchronize Directory](#)

You will then have the option of committing the changes or editing the configuration settings.

Org: test dsseller11 ([view log](#)) Last Sync: Nov 8, 2005 18:26:17 GMT [Auto Sync Scheduling](#)

Directory Settings	Options
<p>*Required fields</p> <p>*Authorized User: root</p> <p>*Password: xxxxxxxxxxx</p> <p>*Host: rcdsv1tm1.p.com</p> <p>*Path: adsmil</p> <p>*Port: 443</p> <p>*Server Type: SunOne</p> <p>*Base DN: ou=dstest11,ou=dstest1,ou=qqa,d...</p> <p>*Email Address Attribute: mail</p> <p>Alias Attribute: description</p> <p>Org Mapping Attribute: sealso</p> <p>User Mapping Attribute:</p> <p>Org Exclusion Attribute:</p> <p>User Exclusion Attribute:</p>	<p>Search Entire Subtree: yes</p> <p>Email Summary Reports To: useraqst1@dom1.test.p.com</p>

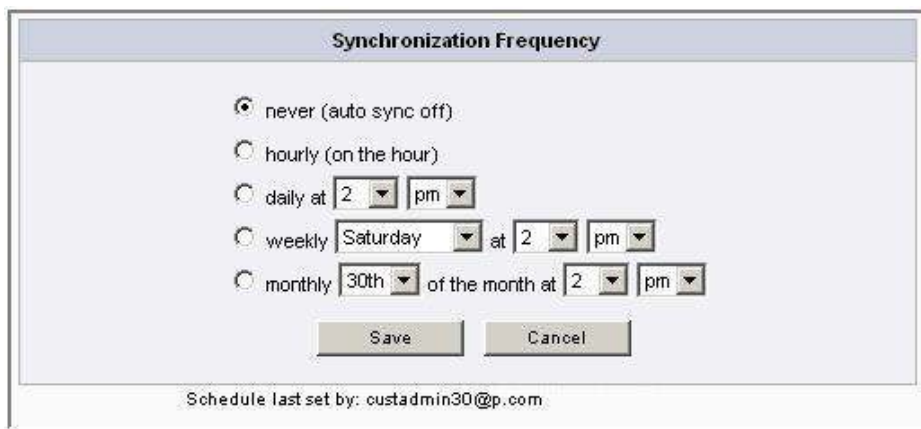
[Edit Configuration](#) [Delete Configuration](#) [Cancel](#)

From this page, you can:

- Click the Synchronize Directory button at the top of the page to synchronize manually. See “Synchronizing” on page 223.
- Click the view log link to see Directory Sync reports. See “Reporting” on page 228.
- Click the Auto Sync Scheduling link to configure Automatic Synchronization. See “Enable Automatic Synchronization” on page 227.
- Click Edit Configuration button at the bottom of the page to change your Directory Sync settings. See “Setting Up Directory Sync” on page 215.
- Click Delete Configuration at the bottom of the page to remove all Directory Sync settings for this organization.
- Click Cancel at the bottom of the page to return to the Organization Settings menu.

Enable Automatic Synchronization

You can set Directory Sync up to synchronize on a regular schedule. After configuring Directory Sync and running a manual synchronization for testing, click Auto Sync Scheduling and specify a time. You can specify how often you want to synchronize with your directory server.



The screenshot shows a dialog box titled "Synchronization Frequency". It contains five radio button options for scheduling: "never (auto sync off)", "hourly (on the hour)", "daily at", "weekly", and "monthly". The "daily at" option is selected, with "2" in the hour dropdown and "pm" in the period dropdown. The "weekly" option has "Saturday" in the day dropdown, "2" in the hour dropdown, and "pm" in the period dropdown. The "monthly" option has "30th" in the day dropdown, "2" in the hour dropdown, and "pm" in the period dropdown. Below the options are "Save" and "Cancel" buttons. At the bottom of the dialog, it says "Schedule last set by: custadmin30@p.com".

Times are in your local time zone if you have a time zone set in Organization Settings. There is no fixed ordering of orgs if multiple orgs are set to sync at the same hour. A Directory Sync configuration that has an automated setting will not prevent an administrator from doing a manual sync at any time.

If you have Automatic Synchronization enabled, it is recommended that you set up an email address to receive reports. See "Email Summary Reports to: (Optional)" on page 220. If you have summary reports set up, you will receive an alert to the same address any time a synchronization fails.

To configure Automatic Synchronization:

1. Configure Directory Sync for manual synchronization.
2. Run a manual synchronization to establish an original list of users, and to confirm that you can connect to your directory server.
3. In the Current Settings page, click Auto Sync Scheduling.
4. Set the time interval for synchronization, and the time. All times are GMT.
5. Click Save.

Reporting

To see what changes have been made with Directory Sync, click on View Log in the Current Settings page. You will see a list of all changes made by Directory Sync in the past seven days in log format.

```
Downloaded:2005/11/08 14:32:19
Report: Directory Synchronization 7-Day Log
Organization:test dsseller11
Nov 1, 2005 to Nov 7, 2005
-----
Start Time: 2005/11/07 23:00:02 GMT
End Time: 2005/11/07 23:00:03 GMT
Status: Successful
Admin: custadmin30@p.com
Org: test dsseller11

Number of users from directory server: 15
Number of user adds: 15
Number of user deletes: 0
Number of alias adds: 0
Number of alias deletes: 0
Number of total changes: 15

adduser USR1@p.com, org=test dsseller11
+Created new user usr1@p.com in organization test dsseller11.
addalias USR1@p.com, alias1@p.com
-The alias alias1@dtest11 in test nostrini-corn.com already exists for USR1@dtest11 in test no
```

The report includes the following information:

- The time and title of the report downloaded
- The organization and time span of the report
- For each synchronization, the start time, end time, and status of the synchronization, as well as the admin performing the synchronization.
- Each change made during synchronization.
- The results of each change. A log entry marked “+” indicates a successful modification. An entry marked “-” indicates a failed modification. Further details are given for each change.

Note: Directory Sync reports update daily. Results of recent Directory Sync activity will not show up in reports until the next day.

Synchronization Authorization

For manual synchronization, Directory Sync uses the authority records of the admin who clicks the Synchronize Directory button. For Automatic Synchronization, Directory Sync uses the authority records of the administrator who set up Automatic Synchronization.

When you use Directory Sync to add, delete or move users, you use the same authority records you would use if you made these changes manually, or with a batch command. Your administrators cannot make changes with Directory Sync that they could not make manually. See the “Create Administrators and Manage Authorization Records” on page 162 for more information.

Troubleshooting Directory Sync

Configuration failures

While you are configuring Directory Sync, you may see errors. Possible errors include:

Error Message	Reason
{attribute name}: The same attribute can not be used for multiple purposes	<p>This error happens when user specifies the same attribute name for two attribute fields. For example: if “mail” is used for email address attribute and alias attribute, the user would get the message: “mail: The same attribute can not be used for multiple purposes”</p> <p>Change these settings and try again.</p>
Org Mapping/Exclusion Attributes: Search subtree must be selected for org mapping/exclusion to work	<p>This error happens when either Org Mapping or Org Exclusion attribute is specified and subtree is not selected. Org Mapping and Org Exclusion is not meaningful unless Search Entire Subtree is enabled.</p> <p>Enable Search Entire Subtree, or remove Org Mapping and Exclusion attributes.</p>

Troubleshooting validation failures

The Directory Settings are validated as a first step in the synchronization process. If an error occurs, verify the settings, save them, and synchronize the directory again. Possible errors include:

Error Message	Reason
Failed to connect to host (hostname) on port {port number}. Please verify your settings and try again.	<p>Reason: The host was not available on the port specified, the open socket operation failed, or an invalid certificate was returned during the SSL handshake.</p> <p>Action: Check that your host is accessible on the specified port. Check that your server is running, and that SSL is set up properly. Make sure the path you set is correct.</p>

<p>Unexpected response {HTTP error code} from host {hostname} on port {port number} possible because of nvalid name/password combination.</p>	<p>Reason: Directory Sync was able to connect to the host and port, but was unable to log in with proper authorities. The user was invalid, did not use the correct password, or does not have the right authorization for the Base DN. Alternately, data transfer failed when sending the user name, password and Base DN.</p> <p>Action: Make sure Basic Authentication is enabled on your server. Check that the admin account on your directory server has the listed password, and has the authority to read information on the base DSN.</p>
<p>Unable to locate the directory entries specified by the Base DN, and/or Email Address Attribute.</p>	<p>Reason: Directory Sync was able to connect to the host and log in, but the Base DN and/or attributes were not valid.</p> <p>Action: Check your Base DN and attributes.</p>
<p>Directory server error: Failed to connect to host <hostname> on port 443. Please verify your settings and try again.</p>	<p>Reason: The authentication settings on the IIS server are not correct for the /dsml virtual directory.</p> <p>Action: Configure the /dsml virtual directory for Basic Authentication:</p> <ol style="list-style-type: none"> 1) Launch IIS Manager from Start -> All Programs -> Administrative Tools -> IIS Manager. 2) In (local machine), navigate to Web Sites -> Default Web Sites -> dsml (virtual directory). 3) Click on the Directory Security tab. 4) In the Authentication and access control box, click Edit... 5) Uncheck Enable anonymous access. 6) Check Basic authentication. A dialog will appear to warn you that your user name and password will be sent over the net in clear text. Since the connection will be through SSL, this warning does not apply. Click Yes to continue. 7) In Authenticated access, make sure all other boxes besides Basic Authentication are unchecked. 8) Click OK to close the dialog box.

Unable to synchronize with a whole organization tree with Active Directory, but you can synchronize with the top level as a single organization

This may be a result of an incompatibility with your directory server. You can resolve this by using the global catalog instead.

To set up Directory Sync to use a global catalog, make the following changes to your directory server setup:

1. Using Active Directory Sites and Services, set the directory server in the DSML configuration to be a Global Catalog.
2. Edit the DSMLV2.config directory in systemroot\system32. Set DSML to use the GC port (3268) for all LDAP queries, instead of the standard LDAP port (389).
3. Restart Active Directory and IIS.

Then set Directory Sync to use port 3268 in the Administration Console.

Chapter 9

Domains

About Domains

Every Internet email address includes a domain, which specifies where mail should be sent. For instance, the address `ted@jumboinc.com` directs a message to the user `ted` in the domain `jumboinc.com`.

In order for a domain to receive filtering from the message security service, that domain must be added to one of the organizations in your service. At least one domain was added as part of your setup and activation process.

Adding a domain to an organization does the following:

- Allows the message security service to accept mail traffic for the domain.
- Associates the domain with an email config organization, which holds delivery information for your mail server.
- Sets a default organization for new users.
- Associates the domain with organization settings for domain-based functionality like domain aliases, Non-Account Bouncing, Maximum Message Size, Daily Message Limit, Automatic Account Creation and Web Autocreate. See “Organization Management” on page 81 for details on these features.

After adding a domain to the organization, you must change the MX records for that domain.

Location of a domain

You associate a domain with an organization. Keep the following in mind as you decide in which organization you want to locate a domain.

1. You must add a domain to a sub-organization of one of your email configs.

Pick any organization that's below an Email Config organization. Mail to that domain uses the settings for that Email Config for delivery.

2. Adding a domain sets a default location for new users in the domain.

For easy administration, you can add your domain to the organization that will contain your users. When you add users without specifying an organization, the users are added to your domain organization. When users are added automatically, they also go into this organization.

3. Adding a domain to an organization associates the domain with that organization's settings.

The following settings are made in the organization that contains your domain:

- Non-Account Bouncing
- Maximum Message Size
- Daily Message Limit
- Automatic Account Creation
- Web Autocreate

For details on organization settings, see "Manage Organization Settings" on page 86.

4. A domain's location determines which administrators can add users to the domain, and where those users can be created.

An administrator can perform tasks only in an organization where the administrator's authority is configured or in sub-organizations of that organization.

An administrator must have authorization over the organization containing the domain to manage the users and domain.

5. A domain and its users don't have to be in the same org.

You can add users to any organization under the same Email Config as the domain.

View Your Domains

Clicking a domain-name link anywhere in the Administration Console displays the Domain View page. This page lists all domain settings:

Domain Name	The name of the domain.
Organization Name	The name of the organization that contains the domain.
Domain Aliases	A list of all domains aliased to the domain.

Catchall Account Address	The user account assigned as the catchall for the domain. Note: Catchall account is a legacy feature available to some customers. It may not be available for your service.
Subdomain Stripping	On/Off, if Subdomain Stripping is enabled/disabled. The default is Off.
Date Created	Full timestamp for when the domain configuration was created.
Date Last Changed	Full timestamp for when the domain settings were most recently changed.

Searching for Domains

If you manage a large number of domains, you can find them by using the Search form on the Start page or by using the search form in Orgs and Users > Domains. Search results also include special commands for handling domains.

1. Select the organization that contains the domain, or select any organization whose sub-org contains the domain.
2. Enter text in the fields above the Domain, Org, and/or Aliased To headings.

The search uses this text in a *Starts With* search. You can type the % character at the beginning of your text string to conduct a *Contains* search instead. Wildcards are not supported.
3. Select the **Include aliases** check box to search for domain aliases as well.
4. Click **Search**.

Viewing Search Results

When you run a search, you see all the domains that matched your search criteria. Search results show up to 15,000 domains. If necessary, the results are displayed on multiple pages.

The screenshot shows a web interface for managing domains. At the top, there is a dropdown menu for 'Choose Org:' set to 'Acme Jumbo Domains'. To the right are links for 'Add Domain' and 'Download Domains/Settings'. Below this is a header 'Domains - Acme Jumbo Domains'. A message states: 'Add all your domains, then add users associated with these domains. Users are automatically added for each domain if SmartCreate is enabled. Each domain must be associated with an organization.' To the right of this message are 'Commands' and a link to 'Settings Summary'. Below the message are three search input fields, followed by 'Include:' with checkboxes for 'aliases' (unchecked) and 'sub-orgs' (checked), and a 'Search' button. To the right of the search button is 'Page 1 of 1 | Show 25 per page'. The main content is a table with columns: 'Domain', 'Org', and 'Aliased To'. The table contains three rows of domain data, each with links for 'Add Alias', 'List Users', 'Delete Domain', and 'Move Domain'.

Domain	Org	Aliased To				
acmejumbo.com	Acme Jumbo Domains	-	Add Alias	List Users	Delete Domain	Move Domain
acmejumbo.uk.com	Acme Jumbo Domains	-	Add Alias	List Users	Delete Domain	Move Domain
stellashores.com	Acme Jumbo Domains	-	Add Alias	List Users	Delete Domain	Move Domain

You can use the following commands on the Search results page:

- Click a domain name to view that domain.
- Click **Settings Summary** to see a summary of all setting for the domains listed in the search results. This includes domain alias information, catchall accounts (legacy feature available to some customers), domain substripping, and creation and modification dates.
- Click **Download Domains** to download your search results as a comma-separated text (CSV) file. The CSV file includes the domain ID number, domain name, the ID number of the org that contains the domain, the ID number of the catchall account (if any), and whether substripping is enabled.
- Click an org name to view that organization.
- Click **Add Alias** to add a domain alias in the modify domain page.
- Click **List Users** to search for a list of users in that domain.
- Click **Delete Domain** to delete the domain. You cannot delete a domain that contains users.
- Click **Move Domain** to move a domain from one organization to another.

Add a Domain for Filtering

Your service is initially set up for users in a single domain. That domain resides in your initial user org. If you have additional domains that you want to filter, add each domain to an org.

WARNING: Follow these steps to add a domain before you change your MX records for that domain. If you change your MX records before these steps are completed, you may lose mail.

Before You Begin


- Make sure your mail server is set up to accept mail sent to the domain you want to add.
- Advanced: If the domain you're adding resides on a different mail server than your existing domains, add a new email config and map it to that server (see "Creating an Email Config" on page 422). Then come back here and add the domain.

Add A Domain

1. Go to the Orgs Page.

Log in to the Administration Console and click the Orgs & Users tab. Click the Orgs link at the top to go to the Orgs page.

2. Click Add Domain for the appropriate organization.

Choose the organization where you want to add the domain from the Choose Org list. If you are not sure which organization to use, choose the organization right below the email config. Email config organizations are marked with a gear  icon.

Note: If you have more than one email config, locate the right one for this domain (the one mapped to the domain's server). Choose an organization below that email config.

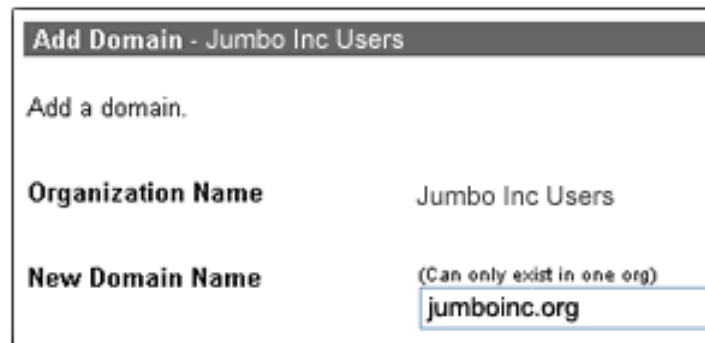
Click the Add Domain link associated with this org.



3. Fill out the Add Domain page.

On the org's Add Domain page:

- Enter your domain name in the **New Domain Name** field.



The screenshot shows the 'Add Domain - Jumbo Inc Users' form. It has a title bar 'Add Domain - Jumbo Inc Users'. Below the title bar, it says 'Add a domain.'. There are two fields: 'Organization Name' with the value 'Jumbo Inc Users' and 'New Domain Name' with the value 'jumboinc.org'. A note '(Can only exist in one org)' is visible above the domain name field.

- Do not enter anything under Domain Alias. If you are adding a domain alias, you enter this information later.
- Click **Save**.

Your domain is added.

4. Set a Domain Alias (Optional).

If this domain has the same user list as an existing organization, you can change it to a domain alias after you create the domain. For information on how to do this, see “Domains with the Same User List” on page 238.

5. Add Users.

In most cases, you add users at this point. For information on how to do this, see “Add / Delete / Move Users” on page 120.

You may wish to skip this step if:

- You set this domain as a domain alias in the step above.
- You do not want to filter mail for your users. For example, you may be starting a very small trial set.

6. Change your MX records.

Change DNS MX records for the domain. For information on how to do this, see *Activation Step-by-Step Guide*.

Changing MX Records for a Domain

WARNING: Never route DNS MX entries to the message security service before adding the domain. All such traffic will be immediately bounced with the SMTP fatal error: 554 No relaying allowed - psmtpt.

Here are step-by-step instructions to look up the correct DNS configurations to make the message security service the preferred MX record for the domain:

1. Go to Orgs & Users > Orgs and select any organization.
2. Click DNS Instructions in the Organization Settings section.
3. For each domain, configure the DNS MX records as described in the Administration Console.

WARNING: If you use the incorrect MX record configuration your mail traffic will bounce. There are two possible MX record configurations.

If you want your DNS MX records pointing directly to a local mail server, they should have a DNS MX priority number greater than 400 to insure that the message security service mail servers are used first in normal mail flow.

Domains with the Same User List

If you have domains that share a user list, domain aliases and domain substripping can reduce your administrative load.

Add a Domain Alias

If you have two or more domains with identical user lists, you can set up a domain alias to make user management easier. To avoid the effort of maintaining multiple identical lists, set up a domain alias once you have added your users to a primary domain.

To enable a domain alias:

1. Log in to the Administration Console.
2. Click the **Orgs and Users** tab, then click **Domains**.
3. In the Choose Org dropdown box, select the organization that contains your primary domain.
4. Click **Add Domain** on the top right of the page.
5. Enter the name of the domain alias as the domain name. Leave all other entries blank, including Domain Aliases. (You add this as a Domain Alias later.)
6. Click **Save** to add the domain.
7. On the Domains page, click your primary domain, then click **Edit**.
8. In Domain Alias, enter the domain alias you just added, then click **Add**.
9. Click **Save** to set the domain alias.

Once a domain alias is set up, all user addresses in the domain alias are considered as aliases of the primary domain. For instance, if you have two domains, jumboinc.com and jumboincsales.com, you could set jumboinc.com as the primary domain and jumboincsales.com as the domain alias. Once this is set, jennifer@jumboincsales.com is automatically considered as an alias for jennifer@jumboinc.com, without any further setup.

Once you have set up the domain alias, change the MX records to redirect your mail.

Notes about domain aliases:

- Both domains should be in the same organization.
- Users can log in with only the user address in the primary domain.
- Domain aliasing is one way only. If you add a user in a secondary (alias) domain, filtering is not provided for the same address in the primary domain.

Adding a Domain Alias via Batch Files

Submit a batch command using the following syntax:

```
modifydomain DOMAINNAME, alias=+ALIASDOMAIN
```

See the modifydomain command in the “Commands” chapter of the *Batch Reference Guide* for details on how to submit the batch command.

DOMAINNAME	The name of the primary domain.
ALIASDOMAIN	The name of the domain you wish to alias to the primary domain.

Subdomain Stripping

When you configure subdomain stripping, the service filters messages for addresses in subdomains, as well. This eliminates the need for some user aliases, as well as the need for domain aliases linking the domain to each subdomain.

You must also change the MX records for each subdomain so you can route mail through the message security service. See “Edit a Domain” on page 243.

Example: Jumboinc.com has subdomain stripping enabled. Messages to dave@<subdomain>.jumboinc.com (e.g. dave@corp.jumboinc.com, dave@dev.jumboinc.com, dave@sales.jumboinc.com, etc.) are filtered according to the configuration for dave@jumboinc.com.

Note: There is a similar organization configuration called Org Substripping that can only be configured by batch commands (See the setorgsubstripping command in the “Commands” chapter of the *Batch Reference Guide*). Enabling Org Substripping is a shorthand configuration to enable Subdomain Stripping for all domains in a particular organization.

You can enable subdomain stripping through the Administration Console or by batch file.

Configuring Subdomain Stripping using the Administration Console

1. Go to Orgs and Users > Domains. If necessary, search for the domain whose subdomains you wish to strip out.
2. Click the domain name to view the domain configuration.
3. Click **Edit**.
4. Set Subdomain Stripping to **On**.
5. Click **Save**.

Configuring Subdomain Stripping using Batch Files

Submit a batch command using the following syntax:

```
addomain ORGNAME, substrip=yes
```

See the `addomain` command in the “Commands” chapter of the *Batch Reference Guide* for details on how to submit the batch command.

ORGNAME

The name or IID (unique identifying number) of the organization where you wish to enable subdomain stripping.

Add a Catchall Account (Legacy Feature)

Important: The catchall account is a legacy feature that’s available to some customers to provide junk-message and virus protection for their unregistered users. Currently, the Non-Account Virus Blocking option provides virus protection for unregistered users. For details, see “Configure Virus Settings for an Organization” on page 318.

Use a catchall account to filter messages for all addresses in a domain that do not have corresponding user accounts or aliases (including user aliases, domain aliases, or subdomain stripping) registered in the message security service.

Example: `dave@jumboinc.com` is configured as the catchall account for `jumboinc.com`. Email sent to an address like `NoSuchUser@jumboinc.com`, which does not have its own user account in the message security service, is filtered according to the `dave@jumboinc.com` settings.

You can set a user as the catchall address for a domain so long as that user is in the same organization as the domain. The user address doesn’t need to be in the relevant domain as long as it is in the same organization.

A catchall account is a type of alias.

The limitations of catchalls are:

- The Administration Console and Message Center message-viewing limits. The Administration Console searches through and displays only the most recent 5,000 messages in a user’s quarantine; the Message Center display limit is 500 messages.
- Catchall accounts do not provide individual user settings. All users filtered by a catchall account are subject to the same filter settings.

Catchall accounts take precedence over domain aliases. See “How Domain Settings Interact” on page 242 for details that will help you coordinate the use of both catchalls and domain aliases.

Add the domain and user before you configure the catchall. Here are steps to configure a catchall through the Administration Console or by batch files.

Configuring a Catchall using the Administration Console

Important: The catchall account is a legacy feature that was available to some customers. For other customers, the Non-Account Virus Blocking option provides virus protection for unregistered users. For details, see “Configure Virus Settings for an Organization” on page 318.

1. Go to Orgs and Users > Domains. If necessary, search for the domain whose subdomains you wish to strip out.
2. Click the domain name to view the domain configuration.
3. Click **Edit**.
4. In the Catchall Account field, enter the email address of the user account you want to use for the catchall.
5. Click **Save**.

Configuring a Catchall using Batch Files

Note: The catchall account is a legacy feature that’s available to some customers. For other customers, the Non-Account Virus Blocking option provides virus protection for unregistered users. For details, see “Configure Virus Settings for an Organization” on page 318.

Submit a batch command using the following syntax:

```
modifydomain DOMAINNAME, catchall=CATCHALLUSER
```

See the `modifydomain` command in the “Commands” chapter of the *Batch Reference Guide* for details on how to submit the batch command.

DOMAINNAME	The name of the single recipient domain that you wish to configure with a catchall account.
CATCHALLUSER	The name of the user that is the single recipient for the domain. The user must be located in the organization that contains the domain.

How Domain Settings Interact

To minimize the need for individual user aliases, there are three domain configurations that act as aliases to provide filtering to mirror your mail server setup:

- Domain Aliases (see “Add a Domain Alias” on page 239)
- Subdomain Stripping or Substripping (see “Subdomain Stripping” on page 240)
- Catchall accounts, if available (see “Add a Catchall Account (Legacy Feature)” on page 241)

When you configure aliasing, it is important to note the order in which different types of aliases are resolved during mail processing or during login to the Message Center.

The following order of precedence is used:

1. Users
2. User alias
3. Catchall account (legacy feature available to some customers)
4. Domain Alias (including user alias and catchall account, if available, for the primary domain)
5. Subdomain Stripping (including user alias and catchall account, if available, for the primary domain)

Edit a Domain

Once you have added a domain, you can then use the Edit page to change the configuration. Follow these steps to edit a domain:

1. Go to Orgs & Users > Domains. Select the domain you want to edit.

You may need to select the Account organization from the Choose Org list, search for the domain using the form at the top, or move to a later page of domains to select the appropriate domain.
2. Click **Edit** in the gray bar.
3. Make any changes to the following fields:
 - Domain Aliases: See “Add a Domain Alias” on page 239
 - Catchall Account (legacy feature available to some customers): See “Add a Catchall Account (Legacy Feature)” on page 241
 - Substripping On or Off: See “Subdomain Stripping” on page 240
4. Click **Save**.

Move a Domain

You can move a domain from one organization to another through the Administration Console or by batch files:

Moving a Domain using the Administration Console

1. Go to Orgs & Users > Domains to display the Commands page.
2. Click **Move Domain** in the row next to the domain name.

You may need to do one of the following to select the appropriate Move Domain link:

- Select the Account organization from the Choose Org list
- Search for the domain using the form at the top
- Move to a later page of domains

3. Select the appropriate New Organization and click **Move**.

Moving a Domain using Batch Files

Submit a batch command using the following syntax:

```
modifydomain DOMAINNAME, neworg=ORGNAME
```

See the `modifydomain` command in the “Commands” chapter of the *Batch Reference Guide* for details on how to submit the batch command.

DOMAINNAME	The name of the primary domain.
ORGNAME	The name or IID (unique identification number) of the organization where you would like the domain to be located.

Delete a Domain

Follow these steps to delete a domain either through the Administration Console or by batch files:

Deleting a Domain using the Administration Console

1. In order to delete a domain, you must first delete all users within the domain. See “Users and Quarantines” on page 103 for instructions.
2. Go to the Orgs & Users > Domains to open the Commands page.
3. Click **Delete Domain** in the row next to the domain name you wish to delete.

You may need to do one of the following to select the appropriate Delete Domain link:

- Select the Account organization from the Choose Org list
- Search for the domain using the form at the top
- Move to a later page of domains

4. Click **Delete** to confirm the deletion request.

Deleting a Domain using Batch Files

Submit a batch command using the following syntax:

```
deletedomain DOMAINNAME
```


See the `deletedomain` command in the “Commands” chapter of the *Batch Reference Guide* for details on how to submit the batch command.

DOMAINNAME	The name of the domain to delete.
------------	-----------------------------------

Chapter 10

The Message Center

About the Message Center

You can allow users to manage their own spam, viruses, and other quarantined messages, by enabling access to the *Message Center*. From the Message Center, users can see what messages are being filtered and why, they can look at quarantined messages, and they can forward any legitimate messages to their own Inbox.

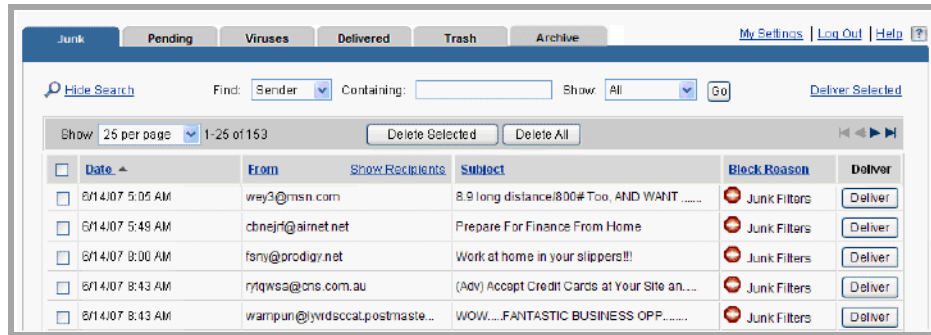
In addition, users can be given permissions to view and modify certain aspects of their own service at the Message Center. With the appropriate permissions, they can turn spam filters on or off, set spam filter levels, manage their own sender lists or user aliases, and more.

Enabling Message Center access involves the following:

- Arrange for users' filtered email to be quarantined in the first place, by setting their spam, virus, and other filter dispositions to *User Quarantine* (see "Manage Quarantined Messages" on page 135).
- Enable notifications for the users' org, so they receive necessary login information and learn about newly quarantined spam (see "The Message Center & Notifications" on page 262).
- Set *User Access* permissions to enable Message Center access and determine which settings they can view and modify.
- Set up *Branding* and configure your Message Center.

Message Center: Features Overview

When their Message Center is enabled, users can log in using any standard Web browser, and see their own personal, quarantined messages. These can include messages that triggered a Content Manager filter, spam filter or virus blocking, depending on the disposition set for the filter. They also include messages from blocked senders, on either the org level or the user's own list. An administrator's Message Center might also contain messages that triggered an Attachment Manager filter.



At the Message Center, quarantined messages are held for 14 days after being received, or for three days after users remove them (by deleting them, or by forwarding them to their Inboxes)—whichever comes first. After that, messages are deleted automatically.

Two versions of Message Center are available: Message Center and Message Center Classic. Message Center offers an enhanced user interface, the ability to search messages, and language settings.

For Message Center help, see the context-sensitive help in the Message Center itself. For details on using the Message Center, see the documents referenced under “Message Center Documentation and Help” on page 270.

Tip: You can also view a user's quarantined messages from the Administration Console, under Quarantine on the user's Overview page. Here, you can see up to 5,000 messages at once.

Message Center includes the following features or components:

- **Junk quarantine:** This lets your users can look for falsely quarantined messages and deliver them to their inboxes. This quarantine keeps messages for 14 days, and then deletes them.
- **Virus quarantine:** This lists virus-infected messages that were blocked. User's receive a Virus notification whenever there are messages in this quarantine.

By default, your service automatically deletes virus-infected messages, so users won't see any messages in the Virus quarantine. You can change this setting, but we recommend that you leave it as is.

The Virus quarantine can also let users safely review the content of messages, without risking harm to their computers. However, if message archiving is turned on (it's On by default), users can't view message content, to prevent virus-infected messages from being stored in your archive.

- **Pending Quarantine:** This lists messages that are blocked from a user's Inbox, because they may contain a recently discovered virus (often called "zero-hour" viruses) or other threat. Users receive an Early Detection notification whenever there are messages in this quarantine.

By default, the Pending quarantine does not appear in the Message Center. You can change this setting, but we recommend that you leave it as is.

The Pending Quarantine can also let users safely review the content of messages, without risking harm to their computers. However, if message archiving is turned on (it's On by default), users can't view message content, to prevent virus-infected messages from being stored in your archive.

- **Personal Archive:** This stores a copy of each message that a user sends or receives for the retention period you purchased (the standard period is 90 days). With the Personal Archive, users can search for and recover their email messages, even if they've permanently deleted them from their inboxes.
- **Personal settings:** In Message Center, users can access their personal settings to change their own filter levels and add their own approved and blocked senders.

Message Center and Message Center Classic

Message Center is a newer interface than Message Center Classic. It offers an improved user interface, language settings, and expanded search capabilities. Below is a comparison chart of the two versions Message Center, followed by information on how to switch between the two.

Comparison	Message Center Classic	Message Center
View Messages	<p>Users can view up to 500 quarantined messages.</p> <p>The virus section of the Message Center displays only 10 virus-infected messages at a time. This means that if the 500 most recent items quarantined are all virus-infected messages, the user will see only 10 virus-infected messages displayed in the Message Center, and no spam messages.</p>	<p>Users can view an unlimited set of messages.</p> <p>Note: If more than 100,000 messages are quarantined in Message Center for a user, the Delete All button on the Junk, Trash, and Delivered tabs is removed automatically. This helps prevent performance issues in the Message Center.</p>
Languages	English only	<p>Additional languages available. Administrators can set language and character set options for organizations, and individual users can specify language settings.</p> <p>Languages can be set for an organization and overridden by users (if they are given permissions to change their regional settings).</p> <p>For more information configuring languages and character sets, see “Quarantine Summary & Message Center Localization” on page 288.</p>
Help	Basic help files.	Context-sensitive help. Clicking Help on any page leads users to appropriate help files for that page.
User Access	Administrator can set User Access, giving customer full or limited access to Message Center features.	Expanded User Access options include limitations to Sexually Explicit filters, separate User Settings privileges, and individual language control

Comparison	Message Center Classic	Message Center
Quarantined Virus Messages	Quarantined Virus messages are in a different section. Depending on User Access settings, users may be able to fix and deliver virus-infected messages, or deliver them as-is with viruses.	Quarantined Virus messages are in a separate tab to reduce the possibility of users accidentally delivering viruses. Users cannot deliver virus-infected messages.
Wireless Settings	Depending on User Access settings, users may be able to configure wireless delivery.	This feature is not available.
Reporting Spam	Administrators can find out why a message was quarantined by reading the message headers, or by contacting Customer Care.	For any quarantined message, a user can view the Junk Message Analysis page, which tells the user why the message was classified as spam. If a user submits the message for further analysis, the Message Center sends it directly to us for use in fine-tuning our anti-spam technology. However, users will not receive a message from us to acknowledge receipt of any messages they submit for analysis.

Switching to Message Center

Because of the many new features, switching from Message Center Classic to Message Center is recommended. Message Center Classic will be phased out in a future release. You can turn on the Message Center for your users without making any other changes to user settings. Your users' login names, passwords, permissions, spam filter levels, and other settings remain the same.

You can enable the new Message Center for one organization at a time. Both versions of Message Center are backward and forward compatible. You can switch between the two versions without changing any settings except Wireless Email and customized Branding. If you've already placed your custom logo (a 120x60 pixel graphic image) in Message Center Classic, the logo will automatically transfer to the new Message Center.

The new Message Center does not currently support Wireless Settings. If you move Wireless Email users to the new Message Center, the wireless rules that users set up in Message Center Classic will still work; however, users won't be able to access wireless rules or settings unless you revert back to Message Center Classic. In future versions, Wireless Settings will be replaced with a message forwarding feature. Meanwhile, if your users use Wireless Settings, you may wish to consider keeping Message Center Classic.

You can choose between Message Center and Message Center Classic in the Branding page. For information about switching to the Message Center, see “Brand Your Message Center” on page 267.

Enable / Disable Message Center Access



You enable users’ access to the Message Center, under User Access, which is available both for the default user and for individual users.

- Enable or disable access for all new users you have not yet added via the org’s Default User template.
- Temporarily disable access for a particular user via user-level User Access settings.

Most User Access changes should be made for organizations. It is possible to configure User Access by individual users, but this makes administration more difficult. Except when disabling Message Center access for a specific user, use the org level User Access page, not the user level page.

User Access: Comparison of Org Level and User Level Pages

Org Level: contains org name. Use by default	User Level: Contains Message Center Access settings. Use caution with other settings.																											
User Access - p.com	User Access - ted@p.com																											
Controls whether users may access and/or modify Message Center	Controls whether users may access and/or modify Message Center																											
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 70%;">Permission</th> <th style="width: 15%;">Read</th> <th style="width: 15%;">Modify</th> </tr> </thead> <tbody> <tr><td>Application Management</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> <tr><td>Junk Email Settings</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> <tr><td>Sender Lists</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> <tr><td>Spam Filters</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> <tr><td>Sexually Explicit (+)</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> <tr><td>Virus Settings</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> </tbody> </table>	Permission	Read	Modify	Application Management	☑	☑	Junk Email Settings	☑	☑	Sender Lists	☑	☑	Spam Filters	☑	☑	Sexually Explicit (+)	☑	☑	Virus Settings	☑	☑	<p>Message Center Access Enabling will give this user access to Message Center</p> <p style="text-align: right;">Enabled ▾</p> <p>Save Cancel</p> <hr/> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 70%;">Permission</th> <th style="width: 15%;">Read</th> <th style="width: 15%;">Modify</th> </tr> </thead> <tbody> <tr><td>Application Management</td><td style="text-align: center;">☑</td><td style="text-align: center;">☑</td></tr> </tbody> </table>	Permission	Read	Modify	Application Management	☑	☑
Permission	Read	Modify																										
Application Management	☑	☑																										
Junk Email Settings	☑	☑																										
Sender Lists	☑	☑																										
Spam Filters	☑	☑																										
Sexually Explicit (+)	☑	☑																										
Virus Settings	☑	☑																										
Permission	Read	Modify																										
Application Management	☑	☑																										

You can also enable and disable the Message Center for several existing users at once using a Batch file command.

For more information, see the Message Center Examples in the “Examples of Common Tasks” in the Batch Reference Guide.

Where User Access Is Configured

You manage user access to the Message Center, by setting *User Access* permissions. These permissions are available both for an organization and for individual users, but settings should typically be made in certain locations, as follows:

- **Organization** Here is where you set permissions for whether all users in an org can modify their own spam filters, turn filters on or off, manage personal sender lists, add user aliases, and more. These permissions apply not just for existing users, but for new users added to the org, as well.
- **Default User** Here, you should make sure Message Center access is also enabled at the user-level—whether or not you want users to have it. This ensures that new users added to an org have Message Center access, unless you disable access for specific users. You should ignore other User Access permission for a Default User, as they don't apply (new users get these permissions from the org).
- **Specific User** Here, you can view a user's current Message Center permissions. Optionally, you can disable access for the user temporarily (rare), or override org-level permissions. Changing User Access for a specific user is not recommended, since it interferes with your ability to maintain the same Message Center policies across an org).

Enable Access for an Org

Orgs > Organization Management >  User Access

To enable Message Center access for an org, you make sure access is enabled at the user level. Then turn on the appropriate permissions for the org:

1. Go to the org's User Access page (from the org's Management page, click User Access).
2. Check boxes as desired to allow users to view and modify certain aspects of their service at the Message Center (see "Control What Users Can View and Modify" on page 255).
3. For each user in the org, and for the org's Default User, make sure Message Center Access is Enabled at the *user level*. Do this via User Access on the user's Overview page.
 - Don't change other User Access settings for individual users unless you intend to manage that's user's permissions separately from other users in the org.
 - Ignore other User Access permissions for a Default User, as they don't apply. New users receive these settings instead from the org's User Access, not from the Default User.

4. Enable the Welcome New User notification for the org.

This sends new users a Welcome email containing a URL and password for logging in to the Message Center. You might also want to enable other notifications, as well. See “The Message Center & Notifications” on page 262.

Disable Access for an Org

To disable Message Center access for all *existing* users in an organization, you must edit each user account to switch Message Center Access from **Enabled** to **Disabled**. To disable access for multiple accounts at once, you can use a Batch command. For details, see the Message Center Examples in the “Examples of Common Tasks” in the Batch Reference Guide.

To disable Message Center access for all new users you *have not yet added* to an organization, edit the Default User template to disable Message Center access. For details about the Default User template, see “Manage Default User Templates” on page 114.

Next, disable the Welcome New User notification for the org. Otherwise, new users will receive a Welcome email with a URL and password for logging in to the Message Center, but when they try to do so, login will fail. You might want to disable other notifications, as well. See “The Message Center & Notifications” on page 262.

For existing users, you must disable access for each account. You can use a Batch command to disable access for multiple accounts at once. For new accounts you have not yet added, make sure that access for the Default User template is disabled and the Welcome notification for the org is also disabled.

Temporarily Disable Message Center Access for a User

[Users > User Overview >](#)  [User Access](#)

If the Message Center is enabled for an organization, but you want to temporarily disable it for one user, do so at the user-level.

1. Go to the user’s Overview page and click User Access.
2. On the user’s User Access page, set Message Center Access to Disabled and click Save.

The user will no longer be able to log in to their Message Center. To re-enable access later, come back here and set Message Center Access to Enabled.

WARNING: Disabling Message Center Access for a user also disables all notifications for that user. Do this only to remove access for a user temporarily. To disable the Message Center for group of users, do so at the org-level, as described above.

Control What Users Can View and Modify

Orgs > Organization Management >  User Access

In addition to managing quarantined messages at the Message Center, users can be given permissions to view and modify aspects of their own service. With the appropriate permissions, they can turn spam or virus filters on or off, set spam filter levels, manage their own sender lists or user aliases, and more.

- Set permissions for an organization, by going to the org's User Access page.
- Override permissions for an individual user, at the user's User Access page (rarely recommended).

Note: Setting specific User Access permissions for a Default User has no effect, as new users receive these permissions from the org, instead.

Set Permissions for an Organization

User Access permissions should almost always be controlled from the org-level, and rarely changed for an individual user.

The User Access list applies to both Message Center and Message Center Classic. Some permissions apply only to Classic, and some do not apply to Message Center Classic. Settings that apply only to Message Center Classic are marked with an asterisk (*). Settings that apply only to the new Message Center are marked with a plus sign (+).

To set permissions for an org:

1. Go to the org's Management page, and click User Access.

User Access - d

Controls whether users may access and/or modify Message Center settings.

Permission	Read	Modify
Application Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Junk Email Settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sender Lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Spam Filters	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sexually Explicit (+)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virus Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Show Deliver-As-Is (*)		<input type="checkbox"/>
Pending Quarantine (+)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wireless Settings (*)		<input checked="" type="checkbox"/>
Account Settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Password		<input checked="" type="checkbox"/>
Email Aliases	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Regional Settings (+)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Personal Archive (+)		<input checked="" type="checkbox"/>
Archive Search (+)		<input checked="" type="checkbox"/>
Archive Recover (+)		<input checked="" type="checkbox"/>
Junk Email Analysis (+)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
View Images, Attachments and Links (+)		<input checked="" type="checkbox"/>

+ This setting applies only to Message Center users.
* This setting applies only to Message Center Classic users.

[Back to Overview](#)

Setting User Access permissions for an org

2. On the org's User Access page, click check boxes to assign or remove permissions for users in this org, as described in the chart below.
 - For each feature, assigning Read privileges lets users see the current setting, and Modify lets them also change it.
 - Modify permissions for a feature also requires Read permissions, so clicking one setting might change another one, accordingly.
 - Changes take effect immediately when you check or uncheck a permission.

User Access Permissions	
Application Management	<p>Checks or unchecks all permissions listed below, acting as a shortcut to enabling or disabling all permissions at once.</p> <p>WARNING: Changes are applied each time you click, so be careful when checking or unchecking these boxes.</p>
Junk Email Settings	<p>Read only Users can see whether spam filtering is on, but they can't turn filtering off.</p> <p>Read / Modify Users can also turn their filtering off or on.</p> <p>Selecting these options also sets Read or Modify permissions for Spam Filters and Sender Lists, which you can then change back, if you want.</p>
Spam Filters	<p>Read only Users can see their current filter levels, but not modify them.</p> <p>Read / Modify Users can also modify filter levels.</p> <p>Both unchecked Users can neither see nor change any spam filter levels.</p>
Sexually Explicit (Message Center Only)	<p>Read only Users can see their Sexually Explicit filter level, but not modify it.</p> <p>Read / Modify Users can modify Sexually Explicit filter level.</p> <p>Both unchecked Users can neither see nor change Sexually Explicit filter levels.</p>

User Access Permissions	
Sender Lists	<p>Read only Users can see any Approved and Blocked Senders, and Approved Mailing Lists, defined for them via their <i>user-level settings</i> in the Administration Console, but they can't add to these lists. (Users don't see any org-level senders at the Message Center.)</p> <p>Use this setting if you want individual users to have their own approved/blocked senders and mailing lists, but you don't want them to manage the lists themselves. They can send you addresses to enter for them, via the Administration Console. They can then view their personal lists at the Message Center.</p> <p>Read / Modify Users can also add their own <i>user-level</i> Approved or Blocked senders, or Approved Mailing Lists.</p> <p>Both unchecked Users can neither see nor change any of these lists.</p>
Virus Settings	<p>Read only Users can see their virus status (On/Off), and their Virus Notification interval, but not change these settings.</p> <p>Read / Modify Users can also turn virus blocking on or off (not recommended except for advanced users), and set their own Virus Notification interval.</p> <p>Both unchecked Users can neither see nor change their virus blocking settings.</p>
Show Deliver-As-Is (Message Center Classic Only)	<p>Modify When checked, users can deliver virus-infected messages from the Message Center to their Inbox.</p> <p>WARNING: Virus-infected messages can be safely opened from the Message Center, without harming the user's system. If forwarded to the user's Inbox and opened, however, such messages can harm their system. Deliver-As-Is should therefore be enabled only for advanced users, such as administrators. It should be disabled for all other users.</p> <p>You can disable the ability of particular administrators to even grant this permission to users. See "Viewing and Editing Authorization Records" on page 164.</p>

User Access Permissions	
Pending Quarantine	<p>Read (default) Users can view messages in the Pending Quarantine in the Message Center, but they can't deliver the messages to their inboxes.</p> <p>Modify Users can deliver messages in the Pending Quarantine to their inboxes. Messages in this quarantine may contain a virus or other threat. (If you are archiving messages for users, this setting has no effect, which prevents archiving of messages with viruses.)</p> <p>Both Unchecked The Pending tab in the Message Center is not visible to the users.</p>
Wireless Settings (Message Center Classic Only)	<p>Available only to customers of North American data centers. Not available in the new Message Center.</p> <p>Modify When checked, users can enable Wireless Forwarding at the Message Center. Wireless Forwarding allows the user to forward messages to a text-enabled phone, PDA, or other mobile device.</p> <p>To make Wireless Forwarding temporarily unavailable for a user without removing this permission, set Wireless Forwarding in the user's General Settings to "Not allowed." See "User General Settings" on page 142.</p> <p>Note: If a user configures Wireless Settings, then is moved from Message Center Classic to Message Center, mail will still be delivered to the wireless device.</p>
Account Settings	<p>Checks or unchecks all permissions listed below, acting as a shortcut to enabling or disabling account settings permissions at once.</p> <p>If all check boxes under Account Settings are cleared, users can't view or modify their account settings (passwords or aliases).</p>
Password	<p>Modify Users can change their passwords at any time.</p>
Aliases	<p>Read only Users can view any aliases that the administrator added to their accounts.</p> <p>Read / Modify Users can manage their own aliases.</p> <p>(Note that User aliases added here must have a corresponding email account on your server.)</p> <p>Both unchecked Users can't view or modify aliases.</p>

User Access Permissions	
Regional Settings (Message Center Only)	Read only Users can view regional settings for the Message Center.
	Read / Modify Users can change the regional settings (language, character encoding, and time zone) for Message Center. These settings will override regional settings for the organization.
	Both unchecked Users can't view or modify regional settings.
Junk Mail Analysis (Message Center Only)	Read only Users can see the "Why was this Message Quarantined?" link and click it to determine why a message was quarantined.
	Read / Modify Users can submit messages for analysis if the messages were falsely quarantined.
	Both unchecked Users can't see the "Why was this Message Quarantined?" link.
View Images, Attachments, and Links (Message Center only)	This controls users' access to images, attachments, and links in quarantined messages. It provides security from viewing offensive images, downloading suspicious attachments, and clicking links to malicious content (a common technique for virus infection).

Override Permissions for a Single User

[Users > User Overview](#) >  [User Access](#)

You can override User Access for an individual user, by going to User Access on the user's Overview page. Set permissions as described above for an organization. Overriding permissions for a single user is rarely recommended, however, as it can make your orgs difficult to manage. Do this only for very small organizations, whose users you don't intend to control from the org-level.

WARNING: Before changing any User Access permissions for an individual user, please note the following:

- Changing User Access for individual user disconnects the user from org-level control. Further changes to the org don't apply for the user, but have to be made separately, for each disconnected user. In large orgs, you can easily lose track of which user has been changed, and how.
- To return a user to org-level control, you must reset the user, which eliminates its personal user aliases and allowed/blocked senders.
- There is no Batch file command for modifying permissions of several users at once, so you can't globally control disconnected users that way.

To apply different User Access policies for a large group of users, assign them to their own org, and set permissions at the org-level, only.

Prevent Users from Opening Quarantined Messages

Orgs > Organization Management >  General Settings

When users visit their Message Center, they see a list of quarantined messages, where each message's Subject line is typically a link. Clicking the link opens the message so they can read it. This can help determine whether a message is legitimate and should possibly be forwarded to the user's Inbox.

If your company follows SEC requirements to archive all messages viewed by employees, however, allowing users to open messages in the Message Center can significantly increase the number of messages you must archive. To prevent this from happening, disable the Subject links. Then to open a quarantined messages, users must first forward the messages to their Inboxes. Delivered message can be tracked as usual by your own archiving methods.

You disable Subject links for an organization under the org's General Settings. This also disables links in the org's Quarantine Summary notification (see "About Quarantine Summary" on page 282).

1. Go to the org's Management page, and click **General Settings**.
2. On the General Settings page, set Message Center Subject Links to Off, and click **Save**.

Subject links of all quarantined messages, both at the Message Center and in the Quarantine Summary, are disabled for all users in the org.

<input type="checkbox"/>	Date	From	Subject	Junk Rating	Deliver
<input type="checkbox"/>	Mon, Nov 6, 2006 3:49 PM	newgolf75759@internet-newda...	As Seen On TV Straight Shootin Golf	<input type="text"/>	<input type="button" value="Deliver"/>
<input type="checkbox"/>	Mon, Nov 6, 2006 3:49 PM	delivery2@iname.com	The Internet Spy And You!	<input type="text"/>	<input type="button" value="Deliver"/>
<input type="checkbox"/>	Mon, Nov 6, 2006 3:49 PM	rstworld@directeservices.net	4 RT airfare to sunny Hawaii only \$99 ea.	<input type="text"/>	<input type="button" value="Deliver"/>

Disabling Message Center Subject links disables the links circled above.

The Message Center & Notifications

Users whose Message Center is enabled can receive email notifications with related information. New users, for example can receive a Welcome notification with their login information (URL and password to the Center).

Users can also receive a notification that includes a new, temporary password when an administrator resets the password. Users will be asked to log in to their Message Center with the temporary password, and then create a new password. If a user does not log in to a new account within 30 days, the temporary password will be stale, and they will receive an error message when they try logging in. An administrator can then reset the password in the Administration Console, as well as choose a setting that automatically sends a notification to the user. (For information about resetting passwords for users, see “User Settings” on page 133.)

All users can receive a periodic Quarantine Summary that lists recently quarantined messages and provides a convenient link to the Message Center. You enable notifications at the org-level, for all users in an org.

Additionally, if a message is sent to the Pending Quarantine, users can immediately receive an Early Detection notification, which alerts a user that there’s a message in his or her Pending Quarantine in the Message Center. This applies only if you have turned on the Pending Quarantine for that user’s organization. This notification is off by default.

Any user whose Message Center Access is Enabled at the *user level*, will receive notifications enabled for the org. If those users indeed have access to the Message Center, certain notifications should be enabled for the org, too. If users’ access is disabled at the org level (but still enabled for the user, as recommended under “Enable / Disable Message Center Access” on page 252), you should *disable* certain notifications.

For information on configuring notifications, see “About Notifications” on page 273. See below for recommended configurations, as regards the Message Center:

Message Center Status	Recommended Notification Status
Enabled for the org	<p>Enable Welcome New User This notification is mailed automatically to new users whose Message Center Access is enabled (via the Default User’s User Access settings). It contains the URL and password for logging in to the Center. Enabling this notification is how you provide users with their necessary login information.</p> <p>Enable New Spam (Quarantine Summary) This notification is sent periodically, listing the user’s recently quarantined spam. It also provides a convenient link to their Message Center.</p> <p>Enable First Spam This notification is sent when the user’s first filtered message is quarantined in their Message Center.</p>
Disabled for the org	<p>Disable Welcome New User Otherwise, new users will get login information to the Message Center, but not be able to log in.</p> <p>Enable or Disable New Spam Enable, if you users should be able to review Subject lines of quarantined messages by email, and forward any legitimate messages to their Inbox. So users can’t try to access the Message Center, disable Message Center Subject Links for the org (see “Prevent Users from Opening Quarantined Messages” on page 261).</p> <p>Disable this notification if you don’t want users to manage their spam at all, but you intend to manage it for them via the Administration Console.</p> <p>Enable First Spam only if New Spam is also enabled.</p>



Welcome notification Enable this notification for an org if the Message Center is also enabled for the org, as it provides each new user with a URL and password for logging in to the Center.

Log In To The Message Center

A user can log in to the Message Center in any Web browser, by going to the URL provided in their Welcome notification. They log in using their user address and a password that's also provided in the notification. The Welcome notification must therefore be enabled for the org. It's then sent to users with Message Center access, when they're first added to the message security service.

Later, users can open a Web browser and go to:

`http://login.postini.com/exec/login`

Administrators can access their Message Center from the Administration Console home page, using the Message Center link at the top right of the page.

The first time they log in, users are prompted to change their password.

Change Password

For better security, specify a password that contains a combination of letters, numbers and special characters. Do not include spaces.

Enter New Password

Old Password:

New Password:

Confirm Password:

Save Changes

Requirements

Your password must:

- Contain 3 of the 4 character types: English uppercase letters, English lowercase letters, numbers, and symbols (such as !, #, \$, %)
- Contain at least 8 characters
- Not be a dictionary word
- Not be the same password as any of your previous 5 passwords
- Not be your email address

Note: Users must log in to Message Center with the temporary password and set a new password within 30 days. If a temporary password expires, administrators can reset the password and choose to automatically notify the user that the password has been reset (see “Set Message Center Passwords” on page 265).

Set Message Center Passwords

Users > User Overview >  Password

The first time users log in to the Message Center, they're prompted to change their password. After that:

- If users forget their passwords, they can enter an incorrect password at the login page. A “Forgot Your Password link” appears that they can click to have a new temporary password emailed to them.
- Users with Account Settings “Modify” permissions in their User Access settings can change their own password at the Message Center, by clicking the Account Settings link at the top right of the page.
- If in a user doesn't have permission to change their password, but needs a new one, you can assign one via the Administration Console, on the user's Password page.
 - a. Go to the user's Overview page, and click the Passwords link.
 - b. On the User Password page (shown below), enter the new password. On this page, you can choose to send an automatic notification to the user that you have reset the password.

Initial Password: Shows the password assigned to this user when it was first added to the service. Or, indicates the password has been changed. Users are prompted to set a new password when they first log in to the Message Center, so you can find out here whether the user has done so.

Reset Password: Allows assigning this user a new, temporary password. The user will need this password to access their Message Center (or the Administration Console, for an administrator). From this page, an administrator can choose to send a notification to the user when the password is reset.

Requirements: The password requirements are determined by the administrator through settings on the organization password policies page, and these requirements will be displayed on the User Password page for reference.

User Password	
To reset the password for this user, generate a new temporary password and send a notification to the user.	
Initial Password	Q:b7kzez (This password has not been changed.)
Reset Password	Reset the password for this user and send a notification with the new password <ul style="list-style-type: none"> <input checked="" type="radio"/> Replace password with temporary value and notify user <input type="radio"/> Reset temporary password to <input type="text"/> <input type="checkbox"/> Notify user
Requirements	The new password must: <ul style="list-style-type: none"> • Contain at least 10 characters • Not be the same password as any of your previous 3 passwords • Not be a dictionary word • Not be your email address • Contain 3 of the 4 character types: English uppercase letters, English lowercase letters, numbers, and symbols (such as !, #, \$, %)

User Password page Indicates whether a user has changed their initial, temporary password. Also lets you assign the user a new password, notify the user that you have reset the password, and displays a list of requirements for the user based on organization settings.

Message Center Language Settings

The new Message Center interface and online help are available in English, French, German, Japanese, and Spanish. Please see “Quarantine Summary & Message Center Localization” on page 288 for information on configuring language settings.

Message Center Security

After login, the Message Center provides a secure Web interface during the user’s entire session:

- The user’s login address and password are encrypted using SSL.
- All web content is encrypted with HTTPS.
- Cookies are used only to identify and validate the user, *not* to track history or session information.
- The only persistent cookie is the email address last used to log in. All other cookies expire within 40 minutes or when the user logs out of the Message Center (by clicking the Logout link).

Brand Your Message Center



Use the Branding page in the Administration Console to configure branding and Message Center options that your users will see. Make all Branding changes in the organization that contains your users.

The Branding page consists of three sections: Message Center User Interface, Message Center Color Palette, and Upload Logo. Each section has a separate Save and Cancel button. To save changes in a section, click the Save button in the appropriate setting.

Message Center Branding - testtest

Message Center User Interface Select the Message Center II option to activate the new interface and functionality for Message Center II. Select the Classic option to revert to the original Message Center look-and-feel.

Interface: Classic Message Center II


Message Center Color Palette Select a palette for styling the Message Center interface. The selected palette determines the color combination for the Message Center for this organization and becomes the default palette for sub-orgs.

Upload Logo Upload a logo image to display in the Message Center. Browse your local disk to identify your file.

Logo Requirements

Image Size: 120 pixels wide by 60 pixels high
Resolution: 72 dpi
Format: GIF89, GIF, JPEG or PNG format
PNG format images are not backwards compatible with all browsers
File size: Less than 10K in size

Logo Display




fake_logo.gif

Logo Placement top-left top-right none

Message Center User Interface

In the Message Center User Interface section, set your interface to Message Center or Message Center Classic.



Message Center User Interface Select the Message Center II option to activate the new interface and functionality for Message Center II. Select the Classic option to revert to the original Message Center look-and-feel.

Interface: Classic Message Center II

You can change between Message Center and Message Center Classic freely. Changes affect all users in the organization who can access the Message Center.

To switch between Message Center and Message Center Classic:

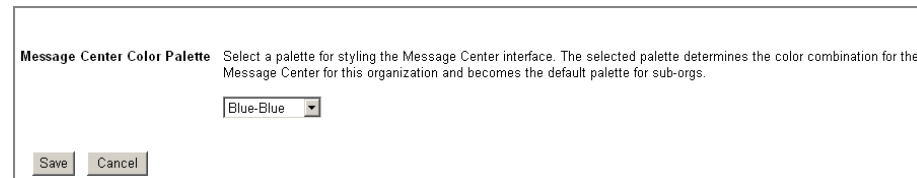
1. In the Administration Console, go to the Orgs & Users tab and select the organization which contains your users.
2. Click the Branding link.
3. Message Center Branding, select Message Center or Message Center Classic and click Save.

For more information about the difference between Message Center and Message Center Classic, see “Message Center and Message Center Classic” on page 250.

Message Center Color Palette

Use the Message Center Color Palette to set Message Center colors for your users. This setting also acts as a default for all sub-orgs.

Note: The Color Palette does not apply to Message Center Classic.



Message Center Color Palette Select a palette for styling the Message Center interface. The selected palette determines the color combination for the Message Center for this organization and becomes the default palette for sub-orgs.

To set your Message Color Palette

1. In the Administration Console, go to the Orgs & Users tab and select the organization which contains your users.
2. Click the Branding link.

3. Choose from the following options:

- Blue
- Red
- Green
- Gray
- Orange

4. Click Save to make your change.

These colors affect the shaded areas of your Message Center. Tabs and text remain in the same color for all configurations.

Upload Logo

You can add your own company logo to your user's Message Center. This affects all users, and acts as a default for sub-organizations as well.

Upload Logo

Upload a logo image to display in the Message Center.
Browse your local disk to identify your file.

Logo Requirements

Image Size: 120 pixels wide by 60 pixels high
Resolution: 72 dpi
Format: GIF89, GIF, JPEG or PNG format
PNG format images are not backwards compatible with all browsers
File size: Less than 10K in size

To change your logo:

1. Design a logo to fit these requirements:
 - 120 pixels wide by 60 pixels high
 - 72 dpi
 - GIF89, GIF, JPEG or PNG format
PNG format images are not backwards compatible with all browsers
 - Less than 10K in size
2. Select the organization in which you wish to add the logo. This affects all sub-orgs, except for those sub-orgs which have a separate branding.
3. Click Branding and scroll to the Upload Logo section.
4. Click Browse link.
5. Browse to your file.

6. Click Save to upload the logo and add your file. You will be redirected to the Organization Management page.
7. Click Branding again to confirm your image.

Additional Branding

Other branding changes, including changes to your message center layout and template, may be available. Contact Support for more information on available branding changes.

Message Center Documentation and Help

See the following documentation resources:

- *Postini Message Center Trifold*
A quick reference double-sided page for the Message Center
- *Postini Message Center User Guide (PDF)*
Instructions on using the Message Center
- *Postini Message Center User Guide (Microsoft)*
Editable instructions on using the Message Center
- *Customizing the Postini Message Center User Guide*
Instructions on how to customize the Microsoft Word version of the *Postini Message Center User Guide*

The “Contact Support” link that appears at the bottom of the Message Center now includes your company name. For example, “Contact Jumbo Inc. Support”. The company name is the value of the Customer Name field in the Organization General Settings.

Troubleshoot the Message Center

The Message Center seems slow or is unavailable for short periods of time. Or, navigating to the Message Center displays the “Page Could Not Be Loaded” error message. Why?

There is either a network issue between your ISP and the data center server, or the data center is experiencing a high-volume or slow performance situation.

The data center is designed to prioritize good email traffic over quarantined email in suboptimal conditions. This ensures prompt delivery of valid email traffic regardless of Message Center availability.

In event of such a slowdown, try logging in later the same day. Such issues rarely last long.

Why do user logins sometimes fail although the user name and password are both typed correctly? The user is authenticated using Privately-Managed Passwords (PMP).

Did the user incorrectly type their login information previously? After a failed login, there are a number of seconds during which additional logins for that user will fail, even if login information is typed correctly. The user should wait a couple of seconds and try again.

Login fails with the error message: “Your authentication could not be verified”.

Either the browser’s cookies are disabled, or the session has timed out.

1. Log out of the Message Center.
2. Re-enable cookies.
3. Log in again.

The Message Center labels messages as being in a category (for example, Special offer/Sexually Explicit spam), but that category filter is disabled.

This indicates that:

1. The message was quarantined due to its Bulk Email rating and any triggered categories that are enabled.
2. It fits the profile of the labeled category more closely than any other category.

Why I can’t delete more than a 100,000 messages in the Message Center?

If more than 100,000 messages are quarantined in Message Center for a user, the Delete All button on the Junk, Trash, and Delivered tabs is removed automatically. This helps prevent performance issues in the new Message Center.

Chapter 11

Quarantine Summary & Notifications

About Notifications

User notifications are messages sent by the service to notify users of important account activity, such as a welcome message when their Message Center account is created, or a note when a virus-infected message is quarantined. Notifications include:

- Welcome New User
- Password Reset
- Virus
- My First Spam
- New Spam
- Quarantine Summary
- Suspension
- Attachment Manager
- Early Detection / Pending Quarantine

This chapter describes how to set up notifications for organizations and users, and how to customize the text of the messages.

Configuring Notifications for an Organization

Notifications are configured at the organization level. For example, you can turn off or turn on all notifications for an organization.

When an organization is created, the notification settings are copied from the parent organization.

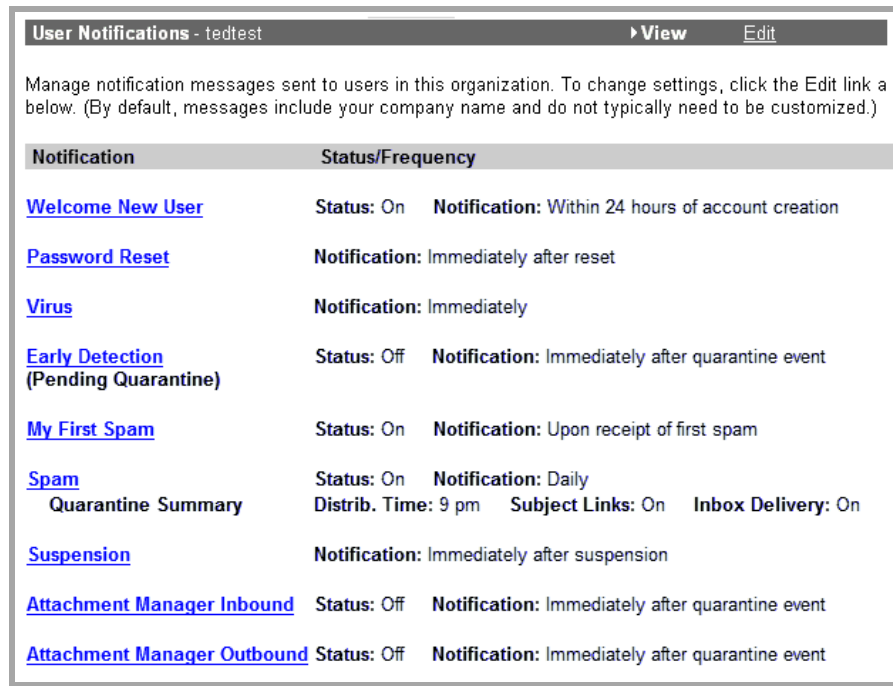
Changes to notification settings are not propagated to sub-orgs. However, notification messages for an organization can be linked from one organization to another as described in “Editing User Notifications Text” on page 649.

To set up notifications for an organization:

1. Go to **Orgs and Users > Orgs**.
2. Choose the organization from the Choose Org pull-down list, or click the name of an organization in the organization list.

We recommend that you set notifications for organizations that contain your users. (Although they can be set at the account and email config orgs, those settings do not apply to any users.)

3. In the Organization Management page, scroll to the Organization Settings section and click the **Notifications** icon.
4. The User Notifications page lists the notifications and their settings. You can turn notifications on or off, and customize the content of notifications. The first step is turn on notifications. See “About Customizing User Notifications” on page 649 for customizing the notification content.



The screenshot shows the 'User Notifications' page for an organization named 'tedtest'. At the top, there are 'View' and 'Edit' links. Below the header, a text block explains that users can manage notification messages and change settings by clicking the 'Edit' link. The main content is a table with two columns: 'Notification' and 'Status/Frequency'. The table lists various notification types such as 'Welcome New User', 'Password Reset', 'Virus', 'Early Detection (Pending Quarantine)', 'My First Spam', 'Spam Quarantine Summary', 'Suspension', 'Attachment Manager Inbound', and 'Attachment Manager Outbound', each with its corresponding status and frequency settings.

Notification	Status/Frequency
Welcome New User	Status: On Notification: Within 24 hours of account creation
Password Reset	Notification: Immediately after reset
Virus	Notification: Immediately
Early Detection (Pending Quarantine)	Status: Off Notification: Immediately after quarantine event
My First Spam	Status: On Notification: Upon receipt of first spam
Spam Quarantine Summary	Status: On Notification: Daily Distrib. Time: 9 pm Subject Links: On Inbox Delivery: On
Suspension	Notification: Immediately after suspension
Attachment Manager Inbound	Status: Off Notification: Immediately after quarantine event
Attachment Manager Outbound	Status: Off Notification: Immediately after quarantine event

5. Click the Edit link in the gray menu bar of the User Notifications page.

User Notifications - View Edit

Set when the following notifications are sent. You may also enable the Quarantine Summary. All notifications for a user can be routed to another mailbox (go to [Users](#)).

Welcome New User	When On, users receive notice within 24 hours of account creation. <input type="button" value="On"/>
Password Reset	Sent immediately after a password reset, if the administrator opts to send it.
Virus	Control frequency of notification, or turn Off to send no virus notifications. <input type="button" value="Immediately"/>
Early Detection	When On, users receive a notice immediately after a potential threat is placed in the Pending Quarantine. <input type="button" value="Off"/>
My First Spam	Sent when the first spam message gets quarantined in a new user's Message Center. No notification is sent if the user previously logged in to the Message Center. <input type="button" value="On"/>
Spam	When On, users receive notices based on the frequency set. <input type="button" value="On"/> <input type="button" value="Daily"/>

The Quarantine Summary is an email notice that includes a list of sender addresses and subjects of newly quarantined messages. Set Inbox Delivery to On to allow customers to deliver quarantined messages to their inbox. Set Subject Links to Off to prevent users from linking to full message text in the Message Center.

Regular Notice

Quarantine Summary

Subject Links:

Delivery Time:

Inbox Delivery:

Account Suspended	Sent immediately after a user is suspended, if the administrator opts to send it.
Attachment Manager Inbound	Choose recipient of notification. Applies to any filter that has either the Quarantine Redirect or User Quarantine disposition. <input type="button" value="Off"/>
Attachment Manager Outbound	Choose recipient of notification. Applies to any filter that has either the Quarantine Redirect or User Quarantine disposition. <input type="button" value="Off"/>

6. Following are descriptions of each notification. Make your changes to the notifications configuration and click **Save**.

Welcome New User

Determines whether new activated users receive the New Service Welcome email. When a Message Center account is created for a user, the user automatically receives an email within 24 hours that includes the login URL, and temporary password details. A user must change the temporary password within 30 days, or an administrator has to reset the password for that user.

The default setting is On.

Password Reset

You can use the User Notifications page to reset the user's password, and you can also choose to notify the user that the password was reset. See "User Settings" on page 133 for guidelines on how to automatically send this notification when you reset a password.

Virus

When a message carrying a known virus is identified, the message is quarantined and the recipient is sent a notification. The intent is to let users know when they have received messages that may have valid content, but whose attachments include viruses.

There are three options for the frequency of notifications:

- Immediately
- No more than once per day
- Disable notification

We recommend the "No more than once per day" option. During a virus outbreak, a user does not need to see multiple notification emails per day. In the notification message, the user is asked to visit the Message Center. If desired, this message can be customized.

The virus alert frequency is the default for all users in the organization. You can override the frequency value in two ways:

- Users with modify permission can override this setting. Users without modify permissions will not see an option to change frequency in their Message Center setting.
- Administrators can modify the frequency setting for a specific user.

The default setting is Immediately.

Early Detection

Determines whether a user receives a notification when a message is sent to the Pending Quarantine due to Early Detection Filtering. When this notification is turned On, users will receive an immediate message every time a potential threat or high-risk message is sent to the Pending tab in Message Center.

My First Spam

Determines whether a new user receives notification of the first spam message quarantined for that account in the Message Center. The notification is sent regardless of whether the user has logged in to the account. This ensures that users are aware of the services and initial activity, even if they forget to log in after receiving the Welcome notice.

The default setting is On.

Spam

Determines whether a user receives a periodic Spam notification when at least one new spam message has been quarantined since the last log-in to the Message Center (not the Administration Console). The frequency of the notification is configurable.

The default frequency of the spam notification is seven days. The optimal notification intervals are between three to seven days. Fewer than every three days may be considered a nuisance by some users, and more than seven days may not leave enough notice to review quarantined messages before the system automatically expires them two weeks from the time of receipt.

The notification day is determined using the user's UID number, a unique identifier for the user account, and is therefore not configurable.

The default settings are:

- Notification: On
- Frequency: Every 7 Days
- Quarantine Summary: Selected

Subject Links: On

Delivery Time: 9 pm

Inbox Delivery: Off

Quarantine Summary

The Quarantine Summary is an HTML-formatted email that lists the messages that have been quarantined. This is a convenient option that allows users to scan their quarantine without logging in to the Message Center. For more information, see:

- “About Quarantine Summary” on page 282
- “Configuring the Quarantine Summary” on page 284
- “Customizing the Quarantine Summary” on page 286
- “Quarantine Summary & Message Center Localization” on page 288

Account Suspended

This notification can be immediately sent to a user whose account has been suspended by an administrator. When an administrator suspends an account through the User management pages, there is an option to notify the user. This message may be customized.

Any modifications to organizational settings apply to all users in that organization.

Attachment Manager (Inbound and Outbound)

This notification is sent immediately when a message has been quarantined because of an Inbound or Outbound Attachment Manager rule. The notification is sent each time a message is quarantined. Messages can be sent to the Attachment Manager Quarantine Redirect address, to the user, or both.

The possible settings are:

Off: Attachment Manager does not send notifications.

Send to Quarantine Redirect: When a message is quarantined because of Attachment Manager filters, Attachment Manager sends a notification to the Quarantine Redirect address configured in Attachment Manager. Usually, this is an administrator address.

Send to User: When a message is quarantined because of Attachment Manager filters, Attachment Manager sends a notification to the intended recipient’s address. The recipient can then contact administrators to have the message delivered.

Send to Both: When a message is quarantined because of Attachment Manager filters, Attachment Manager sends a notification to the Quarantine Redirect address and to the intended recipient’s address.

Inbound and Outbound Attachment Manager settings are configured separately.

The default setting is Off for both Inbound and Outbound.

Note: The timestamps for Attachment Manager notifications do not necessarily correlate with the recipient's organization time zone settings. Attachment Manager uses GMT, and organizations can be configured to any time zone.

User Settings for Notifications

On a user's Notifications settings page, you can:

- See whether the user has ever logged in to the Message Center
- See whether the user has ever received a Welcome notification (sent when the user is first added to the service)
- Specify the address where the user's notifications are sent

To view the notification settings:

1. Click a user address on the Users or User Summaries page.
2. On the User Overview page, under Settings, click **Notifications**.

You can view and set the following fields:

Notification Address

You can specify the address where the user's notifications are sent. Normally the Notice Address field is left blank, and notices are delivered user's primary address. However, if an administrator is managing the user's service, you can add the administrator's address here.

First Login to Message Center (Yes/No)

Displays whether the user has ever logged in to the Message Center. This field, also called *Active*, is displayed in a user's User Summary as well as Notification settings.

Welcome Sent (Yes/No)

The Welcome Sent field can be viewed in the user Notifications settings. Displays whether the user has already received the initial Welcome notification.

Virus Notification Interval

See "Configure Virus Settings for an Organization" on page 318 for details.

Disabling and Redirecting Notifications

You can disable notifications to users in three ways. Use the method that works best for you.

1. Turn off notifications for the organization that contains the users

Use this method if you do not want to tell your users about the service and do not want to route virus/spam information to a help desk staff member or mail administrator.

2. Enable Quarantine Redirect for Spam and Virus Messages for the organization that contains the users

Use this method if you do not want to tell your users about the service, and you want help-desk staff or administrators to regularly check one common quarantine containing all quarantined messages.

3. Set a notification address for the users

Use this technique if you do not want to tell your users about the service, and you want help-desk staff or administrators to be notified and check individual user quarantines. This must be configured user-by-user.

The three methods are compatible with one another, so you can use multiple methods to achieve your desired user interaction. Instructions for configuring the different methods are outlined below.

Turning off Notifications

Use the instructions in the section “Configuring Notifications for an Organization” on page 273 to turn off the Welcome New User, My First Spam, and New Spam notifications, as well as to set the Virus notification frequency to *Disable notifications*.

Enabling Quarantine Redirect

Enable quarantine redirect for an organization containing users so that all quarantined traffic is routed to the configured quarantine. The owner of the common quarantine receives notifications associated with the quarantined spam messages (e.g. Spam and My First Spam). Virus quarantine notifications are not sent. Other notifications (e.g. Welcome New Users, Suspension) are delivered to users.

To enable Quarantine Redirect:

1. In the Administration Console, go to **Orgs and Users > Orgs**, and select an organization from the list.
2. In the Inbound Services section, click the **Spam Filtering** icon.
3. Under Spam Disposition, select **Quarantine Redirect**.
4. Enter the address of the quarantine redirect user. This must be an address on the same server.
5. Optionally: Select the **Apply settings to sub-orgs** check box.
6. Click **Save**.
7. In the Inbound Services section, click the **Virus Blocking** icon.
8. Repeat steps 3 - 6 for Virus Disposition.

Note: The quarantine that contains all quarantined messages is subject to a 5,000 message display limit when accessed via the Administration Console. See “Manage Quarantined Messages” on page 135 for more details.

Configuring Notification Addresses

Manually configuring large numbers of users by navigating through the Administration Console can be slow. Use the Administration Console to configure a small number of users, and use a batch command to configure large numbers of users. See the Message Center Examples in the “Examples of Common Tasks” chapter of the *Batch Reference Guide* for more information.

To configure the Notification Address for a single user:

1. In the Administration Console, go to **Orgs and Users > Users**.

2. Enter the user address in the Find User field, then click **Search**.
3. On the User Overview page, under Settings, click **Notifications**.
4. In the Notification Address field, enter the address to which you want send notifications.
5. Click **Save**.

To configure the Notification Address for all users:

See the Notification Examples in the *Batch Reference Guide* for sample batch commands to modify the notice_address field to point to the mailbox where you wish to have the notifications delivered.

Note: Make sure to change the Default User to ensure that new users are created with the same setting. See “Manage Default User Settings” on page 116 for more details on changing a Default User.

About Quarantine Summary

The Quarantine Summary is an optional feature. Please contact your account manager for more information on your service package.

The Quarantine Summary is an HTML-formatted email containing a comprehensive list of all the messages that have been quarantined in the Message Center since the previous Quarantine Summary. In addition to being a reminder, it also allows users to quickly scan the list to prevent falsely quarantined messages from going undetected. This message eliminates the need to log in and review messages in the Message Center.

Administrators can set the frequency and distribution of the Quarantine Summary, and customize the message for each organization. The message contains a plain-text version in case your mail client does not support HTML.

The Quarantine Summary message contains the sender, subject, and received time, with the subject optionally linking to the actual message in quarantine. The total number of messages quarantined is also listed.

Here are the categories of messages listed in a Quarantine Summary:

- Viruses
- Junk Mail
- Delivered & Deleted Messages

Note: Quarantine Summary messages are only sent to users with Message Center User Access.

The Quarantine Summary is sent to the user's primary email address, or notice address. If there are no spam or virus messages quarantined, no Quarantine Summary is sent. The default message looks something like this:

These messages were quarantined before they reached your inbox as potential spam and virus-infected messages. The quarantined messages can be delivered from your personal Message Center.

Virus Infected Messages 3 messages [Message Center >>](#)

Sender	Subject	Date/Time
youroldpal@ao1l.com	a letter from 3 of your friends...	Jan 4, 4:26 am
youroldpal@ao1l.com	a letter from 7 of your friends...	Jan 4, 4:26 am
youroldpal@ao1l.com	a letter from 9 of your friends...	Jan 4, 4:26 am

Junk Email Messages 3 messages [Message Center >>](#)

Sender	Subject	Date/Time
rhonda@wanna.com	make 15K working from home monthly!	Jan 4, 4:26 am
rhonda@wanna.com	make 25K working from home monthly!	Jan 4, 4:26 am
rhonda@wanna.com	make 45K working from home monthly!	Jan 4, 4:26 am

Delivered & Deleted Messages 4 messages

Sender	Subject	Date/Time	Status
rhonda@wanna.com	make 5K working from home monthly!	Jan 4, 4:26 am	Deleted
rhonda@wanna.com	make 35K working from home monthly!	Jan 4, 4:26 am	Deleted
youroldpal@ao1l.com	a letter from 5 of your friends...	Jan 4, 4:26 am	Delivered
youroldpal@ao1l.com	a letter from 11 of your friends...	Jan 4, 4:26 am	Delivered

Accessing Messages from the Quarantine Summary

The Quarantine Summary links to the Message Center and each individual message.

If you are currently logged in, or if you have selected the **Remember my Address and Password** on the Message Center Log In page, click the message subject link to open your Message Center. Otherwise, click the subject links to open the Message Center log in page.

The Subject links in Quarantine Summary are disabled for those using cross-authentication, as the links are not supported with cross-authentication.

Log in to your message center.

Log in Address
example: joe234@service.com

Password
note: password is case-sensitive

Remember my Address and Password ([what is this?](#))

LOG IN

[Log In Help](#)

Configuring the Quarantine Summary

You must configure these options for the Quarantine Summary for an organization.

- Turn Quarantine Summary on or off.

By default, the quarantine summary is turned off for an organization. The enabling/disabling of the quarantine summary is not propagated down the organization hierarchy.
- Set the frequency of delivery, and optionally customize the Quarantine Summary message for an organization. By default, Quarantine Summary notification is scheduled for daily deliver.
- Enable or disable the subject links to the message.

To configure the Quarantine Summary:

1. In the Administration Console, go to **Orgs and Users > Orgs**, and select an organization from the list.

We recommend that you set notifications for user organizations (though they can be set at the account and email config levels).
2. On the Organization Management page, under Organization Settings, click **Notifications**.

- The User Notifications page lists the notifications and their settings. You can turn notifications on or off, and customize the content of the notification. Click the **Edit** link in the gray menu bar of page.

Notification	Status/Frequency
Welcome New User	Status: On Notification: Within 24 hours of account creation
Password Reset	Notification: Immediately after reset
Virus	Notification: Organization default
Early Detection (Pending Quarantine)	Status: Off Notification: Immediately after quarantine event
My First Spam	Status: On Notification: Upon receipt of first spam
Spam Quarantine Summary	Status: On Notification: Every 7 days Distrib. Time: 9 pm Subject Links: On Inbox Delivery: On
Suspension	Notification: Immediately after suspension

- Turn on or off the quarantine summary, set the frequency and time of delivery, and turn on or off the message links and inbox delivery.

When On, users receive notices based on

On Every 7 days

The Quarantine Summary is an email notification of newly quarantined messages. Set Inbox Delivery to turn messages to their inbox. Set Subject Links to turn the Message Center.

Regular Notice

Quarantine Summary

Subject Links: On

Delivery Time: 9 pm

Inbox Delivery: Off

Frequency

The default is every seven days. The frequency range is one to ten days.

Subject Links

By default, the message links in the Quarantine Summary and Message Center are active. However, the SEC requires most financial institutions to archive all messages that have been viewed by their employees. To meet this requirement, you can disable the message subject links that go directly to the full message in the Message Center quarantine and Quarantine Summary. This forces the user to deliver a message to the inbox in order to view it. The delivered message is tracked by your company's own archiving methods.

Note: Disabling links only takes effect on user accounts, not on the administrative quarantine view.

Delivery Time

This option determines what time the quarantine summaries are created and distributed to the organization.

If you later change the time of day at which quarantine summaries are generated and delivered to a time that would cause the next summary session to start less than eight hours since the last session ended, then the next summaries are not generated until the following 24 hour period.

The time zone and the local time of day when quarantine summaries are delivered can be set at the Org level.

The Time Zone setting is used to show the end-user what time each message arrived, and to set the distribution time of the notice. This is set in General Settings, not in Notifications.

Inbox Delivery

When Inbox Delivery is enabled, the Quarantine Summary contains a "Deliver" link for every quarantined message, including messages quarantined for spam and viruses. When you click this link, the quarantined message is delivered to your inbox. The link used for Inbox Delivery contains a one-time security key, used only for Inbox Delivery, to ensure that this function is secure.

Customizing the Quarantine Summary

To customize the Quarantine logo and text for an organization:

1. In the Administration Console, go to **Orgs and Users > Orgs**, and select an organization from the list.

We recommend that you set notifications for user organizations (though they can be set at the account and email config levels).

2. On the Organization Management page, under Organization Settings, click **Notifications**.

Notification	Status/Frequency
Welcome New User	Status: On Notification: Within 24 hours of account creation
Password Reset	Notification: Immediately after reset
Virus	Notification: Organization default
Early Detection (Pending Quarantine)	Status: Off Notification: Immediately after quarantine event
My First Spam	Status: On Notification: Upon receipt of first spam
Spam Quarantine Summary	Status: On Notification: Every 7 days Distrib. Time: 9 pm Subject Links: On Inbox Delivery: On
Suspension	Notification: Immediately after suspension

3. Click the **Spam** link.
4. Enter a URL for the logo image you want to use, and enter text for the message body.
 - **Logo:** Add a URL where the logo can be found on a public web site. The recommend logo size is 120w x 34h pixels.
 - **Message Text:** The maximum number of characters is 500, and the message text does not support HTML.

Quarantine Summary Notification - Archive Stable Enron Users

Customize your Quarantine Summary notification.

Logo Enter URL where logo can be found.
(example: http://www.domain.com/logo.gif)

Message Text Enter the text for the Quarantine Summary - it will be placed at the top of the message, above the quarantine tables.
(No more than 1000 characters.)

These messages were quarantined before they reached your inbox as potential spam and virus-infected messages. The quarantined messages can be delivered within your personal Message Center.

Save Cancel

See “About Customizing User Notifications” on page 649 for more information on this.

Quarantine Summary & Message Center Localization

When you enable language localization, static text in the Quarantine Summary, along with the default top text, is displayed in the chosen language.

If you are using the new Message Center, these language settings also affect your users' default Message Center language. See "Message Center and Message Center Classic" on page 250 for more information.

You can change the language and encoding of the quarantine summary, and control the character set and date format with this setting. This setting is configured for organizations that contain users.

1. In the Administration Console, go to **Orgs and Users > Orgs**, and select a user organization from the list.
2. On the Organization Management page, under Organization Settings, click **General Settings**.
3. Find the Timezone, Region and Language, and Character Encoding settings toward the bottom.

Timezone	Set this organization's local time zone. This is only relevant for the Quarantine Summary feature. (GMT-08:00) Pacific Time (US & Canada); Tijuana
Region and Language	Set your language. English United States
Character Encoding	Set your character encoding. Unicode (UTF-8)

4. Select your timezone, region and language, and the character encoding you want to use.

The Message Center supports a subset of the languages supported in the Quarantine Summary.

Feature	Support Languages
Quarantine Summary	Chinese (Traditional and Simplified), Dutch, English, French, German, Greek, Italian, Japanese, Korean, Polish, Portuguese, Spanish, Russian
Message Center	English, French, German, Japanese, Spanish
Message Center Classic	English

Note: User's can override the org language setting for the Message Center if they have permission to change their regional settings in the Message Center. See "Control What Users Can View and Modify" on page 255 for more information.

5. The Region and Language setting also determines your date format.

Language	Date Format
English (US)	9/14/2006 4:00 PM
English (UK)	14/09/2006 16:00
German	14.09.2006 16:00
Spanish	14/09/2006 16:00
Japanese	2006/9/14 16:00
Dutch	14-9-2006 16:00
All other languages	2006-9-14 16:00

Setting Languages Using Batch commands

You can change the language of the Quarantine Summary with the following batch command:

```
modifyorg < org name >, lang_locale=< code >
```

For information on using batch commands, see the lang_locale field in the "Batch Organization Fields" chapter of the *Batch Reference Guide*.

The following languages are available:

Language	Code	Encoding
English	en_us.utf8	English (U.S.) UTF-8
	en_us.iso-8859-1	English (U.S.) ISO 8859-1
	en_uk.utf8	English (U.K.) UTF-8
	en_uk.iso-8859-1	English (U.K.) ISO 8859-1
Deutsche/ German	de.utf8	German UTF-8
	de.iso-8859-1	German ISO 8859-1
Español/ Spanish	es.utf8	Spanish (Spain) UTF-8
	es.iso-8859-1	Spanish (Spain) ISO 8859-1
	es_mx.utf8	Spanish (Mexico) UTF-8
	es_mx.iso-8859-1	Spanish (Mexico) ISO 8859-1

Language	Code	Encoding
Français/ French	fr.utf8	French UTF-8
	fr.iso-8859-1	French ISO 8859-1
Greek	gr.utf8	Greek UTF-8
Italiano/Italian	it.utf8	Italian UTF-8
	it.iso-8859-1	Italian ISO 8859-1
Japanese	ja_jp.utf8	Japanese UTF-8
	ja_jp.euc-jp	Japanese EUC-JP
	ja_jp.shift-jis	Japanese SHIFT-JIS
	ja_jp.iso-2022-jp	Japanese ISO-2022-JP
Korean	ko_kr.utf8	Korean UTF-8
	ko_kr.euc-kr	Korean EUC-KR
Netherlands/ Dutch	nl.utf8	Dutch UTF-8
	nl.iso-8859-1	Dutch ISO 8859-1
Polish	pl.utf8	Polish UTF-8
Portuguese	pt.utf8	Portuguese UTF-8
	pt.iso-8859-1	Portuguese ISO 8859-1
Russian	ru.utf8	Russian UTF-8
Chinese	zh_cn.utf8	Chinese (Simplified) UTF-8
	zh_cn.gb2312	Chinese (Simplified) GB2312
	zh_tw.utf8	Chinese (Traditional) UTF-8
	zh_tw.big5	Chinese (Traditional) Big5
	zh_tw.big5-hkscs	Chinese (Traditional) Big5 Hong Kong

Troubleshooting: User Notifications

How can I change the name of the company that appears in the “From” header of notifications?

The notifications use the value of the “Customer Name” field, which is specified per organization. If you are customizing notifications, this field corresponds to the token, <-isp->.

To change the name in the From field of the notifications:

1. In the Administration Console, go to **Orgs and Users > Orgs**.

2. Click the name of an organization in the organization list.
3. On the Organization Management page, under Organization Settings, click **General Settings**.
4. Change the Customer Name field, then click **Save**.
5. To change the email address as well, change the Support Contact setting.

See “Default Notifications with Tokens” on page 654 for information on customizing notifications and a list of all tokens.

In a custom notification, why are header fields such as Date, To, From, & Subject put into the body of a mail message?

The field that contains the custom notification has an extra line break between two fields or above the first field in the text input field, which contains notification text. According to the SMTP RFC 2821, section 2.1, there is a <CRLF> (Carriage Return, Line Feed) character right at the beginning of a new line between the headers & the body of a message. Remove the extra <CRLF> to resolve the issue.

To remove the extra <CRLF> tag:

1. In the Administration Console, go to **Orgs and Users > Orgs**.
2. Click the name of an organization in the organization list.
3. On the Organization Management page, under Organization Settings, click **Notifications**.
4. Click the name of the affected notification.
5. Look for a line break at the top of the notification template, or between two of the header lines near the top of the template.
6. Remove the line break, then click **Save Text**.

See “Customizing Notifications” on page 649 for information on customizing notifications and tips for formatting.

Why do my custom notifications get bounced by my mail server?

Your template does not include the Date, To, From, and Subject headers listed in the default templates. The template headers are used when generating your notifications. Since the headers are common to all email messages, their absence causes your mail server to reject your notifications. See “Default Notifications with Tokens” on page 654 for more details on this.

Chapter 12

Spam Filters

About Spam Filters

Your message security service detects spam by applying hundreds of rules to each message that passes through the data center. It can block obvious spam immediately, then divert more borderline spam to a Quarantine for later evaluation. From there, you or your users can review the Quarantine for any legitimate messages that were falsely quarantined and need to be forwarded to the user's Inbox. Otherwise, spam is deleted automatically.

When your service is activated, all types of spam are typically filtered at a uniform level of aggressiveness. One group of users, however, might have its own idea about what constitutes spam, or how aggressively to filter it. A travel agency might have a zero-tolerance policy for adult content, for example, but want to receive special offers, such as "trips to Hawaii." Another group might want to change its *spam disposition*, by changing how its spam is quarantined, or not quarantining it at all.

Filtering aggressiveness affects how the protection service handles messages that may or may not be spam. More aggressive spam filter levels will quarantine messages that are borderline cases. This will cause more spam to be caught, but may increase false positives. More lenient spam filters will allow borderline messages through, which reduces false positives but potentially lets more spam through.

For each of your organizations, you can adjust the overall aggressiveness of filtering, filter specific categories of spam more aggressively, and choose a spam disposition. Some of these settings are made at the org level, and some for a Default User. You can also adjust individual user's filtering, or allow users to do this themselves at the Message Center.

Where Spam Filtering Is Managed

You manage spam filtering at the following locations:

- **Organization level** Enable *Blatant Spam Blocking* for users in the org, and choose a *spam disposition*—the method of disposing of filtered spam, for example, by changing how it's quarantined, or by not quarantining it at all. Configure *Null Sender Disposition* to dispose of messages that do not contain an SMTP-envelope sender address.

If your service is provisioned with Outbound Services, then you also have the option to turn on *Null Sender Header Tag Validation*. For more information on this feature, see “Configure Null Sender Header Tag Validation” on page 299.

- **Default User** Define user-level spam settings that will apply to new users added to the org. This includes enabling spam filtering in the first place, adjusting how aggressively to filter spam, and filtering specific spam categories even more aggressively. Making these settings for a Default User is how you apply a single filtering policy across an organization.
- **Specific User** You can modify user-level spam settings for an individual user, as well. But this isn't recommended if you want to maintain spam filtering policies across an org.
- **Message Center** You can optionally allow users to modify their own filter levels by granting them appropriate User Access permissions to the Message Center. See “Control What Users Can View and Modify” on page 255.

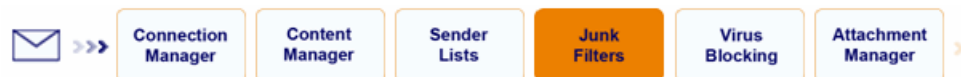
For more information on these levels of management, see “What Settings Are Made Where” on page 73.

Types of Spam Filters

When spam filtering is enabled for a user, the user's messages are processed through the following filters:

- If *Blatant Spam Blocking* is enabled for the user's organization, the user's most obvious spam is bounced or blackholed (deleted), before it reaches your email servers. This eliminates more than half of users' spam, so neither you nor they ever have to deal with it.
- Each user (and Default User) has a *Bulk Email* filter that sets a base level of aggressiveness for filtering the remaining spam, which is typically sent to a separate Quarantine for review.
- Each user (and Default User) can also optionally adjust four additional *Category* filters to filter spam containing particular content even more aggressively (sexually explicit content, special commercial offers, racially insensitive material, or get-rich-quick schemes).
- *Null Sender Disposition* lets you choose how to dispose of messages that do not include an SMTP-envelope sender address. These types of messages are usually Non-Delivery Reports (NDRs). When the system receives an inbound message, it checks for the SMTP-envelope sender address. If there is no sender address, the message is disposed of according to the Null Sender Disposition settings.
- *Null Sender Header Tag Validation* is the process by which the system examines each inbound message for the presence of an SMTP-envelope sender address *and* for the message security service's digital signature. If your message security service has been provisioned with Outbound Services and you have them configured for your mail server, then the system tags the Received field on outbound messages with a digital signature. When this filter is on and the system receives an inbound message, it checks for the SMTP-envelope sender address *and* for the digital signature. If there is no sender address *and* the message doesn't have the system signature, then the message is disposed of according to the Null Sender Disposition settings. If the system signature is present, then the message bypasses this filter, and is evaluated by the others.

When Spam Filters Apply



Spam category filters are applied after all other filtering, including Content Manager filters, and any applicable Approved Senders list (the user's own list, or one defined for the organization). Blatant Spam Blocking occurs before most filters, but doesn't block messages from approved senders. That means:

- **Approved senders bypass Spam Filters**
Even if their messages contain spam-like content.
- **Messages with approved content bypass the category filters**
But it will be blocked if it occurs in obvious spam detected by Blatant Spam Blocking.
- **Messages marked as advertisements are blocked**
If the Subject line of a message contains the prefix "ADV:" (for "advertisement"), the message is considered spam, regardless of approved content.
- **Virus Blocking overrides Spam Filters**
Virus Blocking scans all messages that either pass through the spam filter, are allowed to bypass spam filtering or are quarantined as spam. For example, if a message is quarantined as junk, but also determined to be infected with a virus, the message will be processed according to the virus filter disposition.

See "How Email Security Works" on page 29 for details.

How Spam Is Identified

As a message passes through the spam filters, the message security service applies hundreds of rules to the message envelope, header, and content, all in a matter of milliseconds. Each rule describes some attribute typical of spam, and has a numerical value based on the likelihood that the attribute indicates spam. An equation is then formulated based on the weighted significance and combination of all rules triggered, and the resulting value is the message's *spam score*. This score is measured against the sensitivity threshold set by the user's spam filters, and a decision is made: spam or valid email.

Specifically, a Bulk Email filter sets a base level for filtering all types of spam, and individual category filters can be adjusted to filter a specific category of spam even more aggressively. The Bulk Email filter and category filters work independently of each other, but parameters from all filters collectively provide the final *spam score*, which can categorize the message as spam. A category filter thus multiplies the Bulk Email level and *increases* the number of messages that get identified as spam.

You can see a message's spam score, whether or not it's tagged as spam, by looking at the message header. For details, see "Interpreting Header Fields" on page 637.

Why Catch Rates Might Vary

Developing an effective technology for filtering spam is an ongoing effort since spammers are always evolving tactics to avoid detection. To combat new and ever-changing threats, the message security service continually calibrates its detection and filtering mechanisms, always striking a balance between catching the most spam while lowering the rate of falsely quarantined messages.

As we make adjustments, you might notice slight variances in catch rates for certain spam categories. Or you might see an increase in falsely quarantined messages. If this happens, you might want to increase or decrease your own spam filter levels accordingly: Increase sensitivity to catch more spam, or decrease levels to prevent false quarantines. For details, see “Fine-Tune Spam Filters” on page 303.

When to Use Content Manager Along With Blatant Spam Blocking

If you experience messages with undesirable content like profanity not being caught by your spam filters, you can add Content Manager filters to catch those messages.

If the objectionable content is limited to a few words and the other content does not score as spam, then the message would not trigger the spam filters. To stop these types of messages, you can create content filters that look for exactly the offending language you wish to prohibit.

For information about creating content filters for these kinds of messages, see “Block Messages with Profanity” on page 367.

Configure Spam Settings for an Organization

You configure Blatant Spam Blocking (BSB), which deletes the most obvious spam, and Spam Disposition, which determines how spam messages are managed for a user organization.

You will enable spam filtering and set filter levels for the default user (the template use for an organization). See “Enable and Adjust Spam Filters” on page 301 for more information.

Configure Blatant Spam Blocking

Orgs > Organization Management >  Spam Filtering

Blatant Spam Blocking (BSB) is an org-level setting on the Spam Filters page that detects and deletes the most obvious spam before it reaches your email server. This feature identifies more than half of all spam. Messages are either bounced or blackholed (deleted) without reaching the intended recipient or any Quarantine.

Specifically, BSB calculates the message's spam score. If the score is below 0.00001 (a perfectly valid message has a score of 100), the message is overwhelmingly deemed spam, and blocked. See "Interpreting Header Fields" on page 637 for details on spam scores.

Blatant Spam Blocking applies to all users in an org, but works only for users whose Filter Status is On (see "Enable and Adjust Spam Filters" on page 301).

The Reports page has statistics regarding how many messages are caught by Blatant Spam Blocking (see "Reports" on page 551).

To configure Blatant Spam Blocking:

1. Go to the Organization Management page for the relevant org.
2. Under Inbound Services, click **Spam Filtering**.
3. Under Blatant Spam Blocking, choose one of the following options.
 - **BSB Off:** Disables this feature for the org.
 - **Bounce:** Bounces obvious spam back to the sender with the error message "ERROR 571 Message refused."
 - **Blackhole:** Deletes obvious spam without sending a return error. From the sender's perspective, the message has been accepted.

Note: Depending on your service package, Blatant Spam Blocking might always be set to a Blackhole disposition.

Enable BSB without Additional Filtering

Sometimes you might want to enable *only* Blatant Spam Blocking for an organization, without any additional filtering.

1. Enable Blatant Spam Blocking for the organization, with either the Bounce or Blackhole Disposition.
2. Under Spam Disposition, select **Message Header Tagging**.
3. For the org's Default User (and any existing users), make sure the Filter Status is On (go to Spam Filters on the user's Overview page).

All obvious spam will be eliminated without reaching the data center or your server. Any remaining spam detected by the filters is tagged with a spam score written in the Header, and then delivered to users.

Configure Null Sender Disposition

Null Sender Disposition is an org-level setting on the Spam Filters page that lets you choose how to dispose of messages that do not include an SMTP-envelope sender address.

To configure Null Sender Disposition:

Select one of the following options:

- **Ignore:** Let the message bypass this filter. Other filters still apply.
- **User Quarantine:** Send the message to the recipient's quarantine.
- **Blackhole:** Delete the message.
- **Bounce:** Return the message to the sender.

You can enter text to serve as the bounce message. If you enter text, it must begin with 4 or 5, followed by two digits, a space, and your text. This structure follows the format of SMTP reply codes. For example: 554 Transaction failed.

If you leave this field blank, the following message is used:

571 Domain does not accept delivery report messages

Note: In order to deliver valid messages that do not include an SMTP-envelope sender address, like voicemail or vacation responders, use Content Manager to create a custom filter. See “Create Filters to Allow Valid Null-Sender Messages” on page 368 for more information.

Configure Null Sender Header Tag Validation

Note: These options are available only if you have been provisioned with Outbound Services. If you configure Outbound Services for your mail server, then the system adds a digital signature to each of your outbound messages.

Null Sender Header Tag Validation is the process by which the system examines NDRs for the presence of an SMTP-envelope sender address *and* for the message security service's digital signature.

While this filter is an aspect of spam filtering, it runs at the very beginning of the message filtering process to immediately dispose of messages like invalid NDRs.

Whether or not you have configured Outbound Services for you mail server, we recommend that you turn this filter on. When the filter is on and it catches a message, the system looks ahead to Content Manager to see whether it is configured to let messages bypass the junk filters and allow valid email that does not have an SMTP-envelope sender address. Under these circumstances, you can let valid messages pass through to their recipients' inboxes.

If this filter is off, then the system does not look ahead to Content Manager and you do not have the option to let valid null-sender-address messages pass through to their recipients' inboxes.

For information about how to create a Content Manager filter that allows valid null-sender-address messages, see "Create Filters to Allow Valid Null-Sender Messages" on page 368.

To configure Null Sender Header Tag Validation:

Use the following options to turn Null Sender Header Tag Validation on or off, and to set the length of time during which the system can accept the digital signature:

- **On/Off:** Select **On** or **Off** to turn Null Sender Header Tag Validation on or off.
On: Any message that does not include an SMTP-envelope sender address, but does include the message security service's digital signature bypasses this filter. All other messages that do not include an SMTP-envelope sender address are disposed of according to your Null Sender Disposition settings, and according to how Content Manager is configured.
Off: Any message without an SMTP-envelope sender address is disposed of according to your Null Sender Disposition settings.
- **Validate reports up to ___ hours after message delivery:** Enter the number of hours that the digital signature is considered valid. After that number of hours, the signature expires, and messages with an expired signature are treated the same as messages with no signature.

Configure Spam Disposition for an Organization

To determine what to do with filtered spam, you select a *spam disposition*. Do this at the org-level, which sets the disposition for all users in that organization.

To configure Spam Disposition:

1. Go to the Organization Management page for the org.
2. Under Inbound Services, click **Spam Filtering**.
3. Choose the Spam Disposition:
 - **User Quarantine:** Filtered spam for each user in the org is sent to a separate User Quarantine. Administrators can manage this Quarantine from the user's Overview page.

If Quarantine Summary is also enabled for the org (under Notifications), each user receives a periodic summary of recently quarantined messages. If User Access is enabled for the org, as well, users can manage their own quarantined messages in the Message Center. See “Manage Quarantined Messages” on page 135 and “Enable / Disable Message Center Access” on page 252.

- **Quarantine Redirect:** Delivers all users’ filtered spam to a single administrator’s Quarantine—the one associated with the address entered here. Enter the primary address (not an alias) of a user who has been added to the message security service, has administrative privileges for this org, and is located under the same email config as this organization.

Select this option if you don’t want to sort quarantined spam by user, and if you don’t want users to manage their own spam. The administrator must review and deliver all users’ legitimate messages from the shared Quarantine—either from the administrator’s User Quarantine in the Administration Console or from the administrator’s Message Center. (The Administration Console can display 5,000 messages at once, Message Center can display an unlimited number of messages, and Message Center Classic can display 500 messages.)

If Quarantine Summary is enabled for the org (under Notifications), this administrator receives a periodic summary of recently quarantined messages for the entire org. If you choose this disposition, make sure to disable User Access permissions to the Message Center for all users in the org.

See “Manage Quarantined Messages” on page 135 and “Enable / Disable Message Center Access” on page 252.

WARNING: The administrator’s Quarantine should be checked regularly to forward any legitimate messages that were accidentally quarantined.

- **Message Header Tagging:** Sends filtered spam for this org to your email server with a spam score written in the header. The message can then be processed at a dedicated location on your server or on each user’s email client. No spam messages are filtered.

For this disposition to be effective, you must set up rules on the receiving email server for processing spam based on its spam score.

WARNING: With this disposition, all spam for users in this org is delivered to your email server intact, along with “good” traffic. This is an advanced setting for administrators who want to create their own rules for filtering spam, or who don’t want to filter spam beyond what is caught by Blatant Spam Blocking. This setting is not otherwise recommended.

Enable and Adjust Spam Filters

[Users tab](#) > [User Overview](#) >  [Spam Filtering](#)

You enable spam filtering and adjust how aggressively you want to filter under *Spam Filtering* on a user's Overview page. Doing this for a Default User applies these settings to all new users in any org the Default User is assigned to. Doing this for any other user applies the settings only to that user. You can set an overall level of aggressiveness for filtering all types of spam (Bulk Email), then adjust separate filters for more aggressive filtering of specific spam categories.

Note: Messages from approved senders or messages that contain approved content bypass all spam filtering.

To enable and adjust user-level spam filters:

1. Open a user's Spam Filters page.

2. Set Filter Status to **On**.

This enables both Blatant Spam Blocking (if it's also enabled for the org), and the category filters. If this setting is Off, no spam filtering occurs.

3. Under Filter Sensitivity, set the Bulk Email and individual category filters.

- Adjust the Bulk Email filter for how aggressively to filter spam that gets by Blatant Spam Blocking. Bulk email sets a base level for filtering all types of spam, including spam in the individual categories.
- Optionally set filter levels for more aggressive filtering of individual spam categories, which include Sexually Explicit, Get Rich Quick, Special Offers, and Racially Insensitive. When the individual category filters are on, they multiply the Bulk Email spam level and *increase* the number of messages that get identified as spam.

Important: Recommend Settings:

In order to achieve the most effective spam filtering—capturing the most spam, while minimizing the quarantining of valid messages (referred to as a “false positive”)—we recommend the following settings for your Spam Filters:

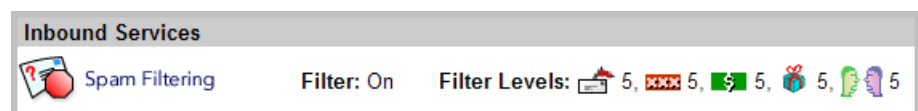
- Bulk Filter: Set to **2**
- Category Filters (such as “Special Offer” filter): Set to **Off**

If you receive primarily non-English messages, we recommend:

- Bulk Filter: Set to **1**
- Category Filters (such as “Special Offer” filter): Set to **Off**

User may adjust their filter values higher for more stringent filtering, but should be aware that some valid messages might be captured, and should therefore check their quarantines frequently. For more tips on settings, see “Fine-Tune Spam Filters” on page 303.

4. Click **Save** when you have finished.



How spam is handled when it is identified by these filters depends on the spam disposition defined for the user's organization. For more information, see "Configure Spam Disposition for an Organization" on page 300.

Fine-Tune Spam Filters

Adjusting spam filters requires striking a good balance between catching the most spam possible while not falsely identifying legitimate messages as spam. Do this at service initiation, and periodically afterwards, to accommodate continual calibrations that the message security service makes to the filtering mechanism.

As you increase filter levels to be more aggressive, you catch more spam, but you also increase the opportunity for false positives. Users typically prefer receiving a few spam messages over having legitimate messages tagged as spam, so it's best to approach fine-tuning conservatively. The best approach involves repeated testing, and then monitoring your success after each adjustment.

We recommend the following:

1. Add your company's customers, vendors, and other common addresses and domains to your Approved Senders list.
2. Make sure Blatant Spam Blocking is enabled for your orgs, which automatically blocks the most obvious spam.
3. Before adding users to an org, configure the org's Default User so the Bulk Email filter is set to **2** and all Category filters are set to **Off**. View spam reports for the org, and get feedback from users to monitor the effectiveness of these settings.
4. If, after that, too much spam of all types is getting through the filters, increase users' Bulk Email filters by one level, and leave all category filters off. Do this for the org's Default User to apply to new users, and for existing users via each user's Overview page.
5. If a specific category of spam is getting through (such as special offers), increase the strength of that category filter by one level for all users.
6. If users in an org are in a financial or legal industry, considering enabling Industry Heuristics filters for the org. (Industry Heuristics is an optional feature not available with all service packages. For more information, contact your account manager.)

When you go through the configuration process, keep in mind:

- The lower the setting for Bulk Email, the higher a category filter setting must be to have an appreciable effect.
- Whenever you increase the Bulk Email filter, try resetting category filters to a low level, and then increase them as needed.
- Make small adjustments as needed. Change only one filter at a time and monitor results before you make additional changes.
- Raising a category filter's level rather than the Bulk Email filter level is more likely to falsely quarantine legitimate messages.

Phishing Attacks

Spam Filtering also provides protection against phishing attacks.

A *phishing attack* is a type of spam disguised as valid email that is designed to trick recipients into providing information or visiting a hostile web site. For instance, a common type of phishing attack is a message, supposedly from a bank, claiming that a credit card and password are needed. A URL is provided to a site at which users can enter credit card information. That information is then used illegally.

Because phishing attacks are sent in mass, they are normally detected and stopped as spam. If you see a number of phishing attacks getting through, you can work to stop them with the following:

- Troubleshoot why the phishing attack got through. See “Troubleshoot Spam that Gets Through” on page 306.
- If the attacks always contain a key phrase, you may be able to use Content Manager to block the messages. See “Create or Edit a Content Manager Filter” on page 340.
- If the attacks come from the same IP address, set up a manual block for that IP address. See “Manual IP Block Configuration” on page 457.

Botnet Attacks

A *botnet* is a particularly dangerous spamming technique that is rising in popularity. In a botnet, a spammer exploits a virus or system vulnerability to take control of many machines at once, then sends spam or viruses through them all. Because a botnet spam attack comes from many different IP addresses, many conventional filters do not work.

The message security service uses special techniques to identify and stop botnet attacks. Our botnet-detection engines track a huge body of email to detect messages launched by botnets immediately after they begin.

These filters are automatic. You don't need to take any steps to enable them.

Early Detection Filtering

Early Detection Filtering works only when you have Spam Filtering turned on, which is the default setting.

You can turn on Early Detection Filtering from the Virus Settings page (see “Configure Virus Settings for an Organization” on page 318).

Your message security service checks for new antivirus-definition file updates every minute, but there is always some delay between the discovery of a virus and its inclusion in a definition file. Live viruses that have not been included in definition files are referred to as *zero-hour threats*.

When a message is not immediately identifiable as virus infected, but has an executable file attached, that message is sequestered in the Early-Detection Quarantine.

Messages are held in the Early-Detection Quarantine for 8 hours to allow time for virus-definition files to be updated, and then those messages are scanned again for viruses based on the updated definitions. Those messages are then disposed of according to your Virus Blocking settings.

Administrators and users who have access to the Pending tab in Message Center can see messages in the Early-Detection Quarantine.

Outbound Spam Scanning

Outbound Spam Scanning is designed to improve the deliverability of messages, address the misconfiguration of mail servers as open relays, and block internal senders of spam.

From time to time, an open relay transmitting mail through the Postini servers causes the Postini servers to be associated with spammy behavior, which then results in blocking all mail from the offending domain.

There may also be occasions where someone in your organization is sending spam, or when computers on your network are infected as part of a botnet.

With Outbound Spam Scanning, messages are evaluated on an individual basis according to content: valid messages are transmitted normally, and offending messages are bounced (with a 500 reply code).

Outbound messages are evaluated by the following sequence of filters:

1. Outbound Virus Blocking
2. Outbound Content Manager
3. Outbound Spam Scanning
4. Outbound Attachment Manager

These filters operate somewhat differently than Inbound filters. With Inbound filters, if a message is approved by Content Manager, then it bypasses the Spam Filters regardless of spammy content. With Outbound filters, even if a message is approved by Content Manager, it is still scanned for spammy content by Outbound Spam Scanning.

There are no controls in the Administration Console with which you can configure Outbound Spam Scanning. Configuration is handled by Postini administrators. If you see an undue number of bounce messages, contact Postini Customer Care to discuss your options.

The number of messages caught by Outbound Spam Scanning is reflected in Outbound reports that include the number and percentage of bounced messages.

Troubleshoot False Positives

On rare occasions, legitimate messages can be falsely filtered as spam (often called *false positives*). Or conversely, messages might get past the filters and reach users' inboxes.

Some common reasons for false positives include:

- **Filter levels are too aggressive.**

The message might have characteristics that make it look like spam, such as disclaimers, URLs, dollar signs, multiple exclamation points, and little or no body content apart from a link, image, or file attachment. Depending on your filter levels, these characteristics can increase the likelihood of a message being caught.

In particular, aggressive category filters can falsely tag valid messages as spam. Try lowering category settings, beginning with the Special Offer filter. Businesses tend to receive legitimate email containing commercial content, so false positives in this category are more likely. An aggressive Bulk Email filter can falsely tag valid emails, too, but should do so less often than a category filter.

- **A listserv or news group server sent the message.**

Mailing lists share many characteristics of spam. If the sender address is always the same, for example, *list_name@domain.com*, add it to the user-level Approved Recipients list.

- **The message was sent by an automated email service and appeared “spoofed.”**

This might include a message from a group reservation or auction site. Add these addresses to your Approved Senders list.

- **The sender appears on the org-level or user-level Blocked Senders list.**

Remove it from this list.

Examining the spam score in a message's header can also provide clues to why it was identified as spam. See “Interpreting Header Fields” on page 637.

Troubleshoot Spam that Gets Through

If too much spam is getting through to users' inboxes, follow these steps to determine why:

1. **Has the user has been added to the message security service? If not, and Non-Account Bouncing is turned off for the user's domain, and no Catchall user is enabled for the domain, then mail is delivered to the user without filtering.**

Search for the address on the User's tab. If a user isn't found, add the address to the service.

- If the address is associated with another user that has already been added, add the new address as a *user alias*. See "Manage User Aliases" on page 140.
- If the address could instead be recognized by the service via *domain aliasing*, create a domain alias for the user's domain. See "Add a Domain for Filtering" on page 236

To ensure that valid users are added to the service, consider adding your users automatically. See "Add Users Automatically to an Org" on page 126.

2. Is the user's spam filtering turned on?

Go to Spam Filtering on the user's Overview page and verify that the Filter Status is On.

If the user has User Access permissions to turn their own filters on and off at the Message Center, and the filters have been turned off, instruct the user not to do this, and consider removing that particular permission. See "Control What Users Can View and Modify" on page 255.

3. Are the user's category filters set high enough to catch spam?

Go to Spam Filtering on the user's Overview page and verify that the Bulk Email and other category filters are set high enough (see "Fine-Tune Spam Filters" on page 303). If they aren't, adjust them accordingly. If they look OK, go to the next step.

4. Was the message sent to a distribution list rather than an individual user?

If a message is sent to a distribution or mailing list that hasn't been added to the message security service as a user or user alias, it passes through to users without spam filtering. Review the message's header to determine the TO address (see "Interpreting Header Fields" on page 637), then search for that address on the Users tab. If the list isn't found, add it as a user.

You might then add additional lists as user aliases for that user (all lists will therefore share the same User Quarantine). This protects all your distribution lists, and the users on those lists. See "Add / Delete / Move Users" on page 120 and "Manage User Aliases" on page 140.

5. Was the message sent directly to and accepted by your mail server, bypassing the protection service?

- a. Sometimes users' email is delivered to them from more than one email server. Messages from another server that isn't mapped to an email config in the message security service don't go through the data center and therefore aren't filtered. Many email clients put these messages in the same inbox as filtered messages, so users might believe they received spam from a your protected server. Review the message headers to make sure they include an email server registered with the service. If they don't, inform the user.
- b. Some spammers don't follow DNS standards for selecting MX records. They send email to the highest numbered server, or randomly pick one from port scans. To determine if the message actually passed through the data center, review the message headers for the strings listed below (the # sign will be replaced by various numbers). If any of these strings exist in the header, the message did pass through the data center.

```
exprod#mx#.postini.com  
chipmx#.postini.com  
chip#mx#.postini.com
```

- c. If these strings don't exist in the message header, the message was delivered directly to your email server, bypassing data center filters. To remedy this, set up your email server or firewall to accept email only from the data center's IP ranges. See "Setting Up Secure Mail Delivery" on page 495.

6. Did a local user (within your organization) send the message?

Unless your email server is reconfigured to send all email outside the server, rather than delivering locally to local users, messages exchanged among users on the same server aren't processed by the data center, and therefore aren't filtered for spam. Review the headers to see if the email was sent from someone on the recipient's same server. If it was, reconfigure this server to send all email outside, so it's processed by the data center.

7. Was the sender's address in the user- or org-level Approved Senders list?

If the sender or sender's domain is on an Approved Senders list—either the user's personal list, or a list defined for the user's org—messages from those senders are delivered, regardless of spam-like content. This is also the case if the spammer has spoofed the sender address so it matches an Approved sender. Review the user- and org-level lists and delete any known spammers.

Remember that users don't have visibility of their org's Approved Senders list, so they might be confused as to why spam from a sender on this list would not be filtered.

8. Has the user added his or her own address or domain as an Approved mailing list, at the Message Center?

If so, all spam addressed to the user, regardless of any spam settings, is delivered to that user's inbox. Log in to the Message Center and remove that user's address or domain from this list. Then let the user know why adding your own address or domain here is not a good idea.

9. Does the email content have enough spam characteristics to trigger filtering?

In general, if all prior steps have turned out to be false, the spam did not have sufficient spam characteristics to be filtered. Confirm this by checking the message header for its spam score (see "Interpreting Header Fields" on page 637).

In this case, please enclose the message as an attachment to an email and send the message to Support. By sending the spam as an attachment, analysis can be performed on copy of the original email with headers intact; otherwise, the message will be unusable. Data center engineers evaluate these message to make improvements to the filtering engine. The messages are used for statistical analysis.

If you have further questions, please contact Support.

When Spam Still Gets Through

If you find that a large amount of spam is still slipping through the filters, follow the steps below:

1. Add repeat spammers to the user- or org-level Blocked Senders list.

This may be effective for a short time, as long as the spammers do not change their addresses. Spammers frequently rename their sending domains or addresses, however, in which case it's better to set up a manual IP block (see below).

2. Set up manual IP blocks against the offending sites to prevent more spam from the same IP address:

Spammer can change their sending domains or addresses, but it's more difficult to change their sending IP addresses. Blocking the IP addresses from your server can therefore be an effective way to eliminate spam from those sources.

- a. Locate the sender's IP. Different email clients have different methods for doing this. In Outlook, open the spam message in your mailbox and select View -> Options. The Options window appears. Scroll down in the Internet headers window until you see the IP address following the phrase "Received: from source". This is the IP address of the spammer (or the open relay/intermediary used by the spammer).

WARNING: Don't inadvertently block the protection service IP, as that IP also appears in the header. Blocking IP Addresses requires "Manual IP Blocking" privileges. If the options listed below aren't available, contact an administrator who has the necessary privileges.

- b. In the Administration Console, go to the Inbound Servers tab, for the mail server that's getting too much spam. (Choose the server's email config from the Choose Org list at the top of most pages, then click the tab.)
- c. On the Connection Manager page, click the "Block an IP" link located in the lower right-hand section of the page.
- d. Fill out the Manual IP Blocking form with the IP address or range, select a disposition, and set duration to 9,000 days. Due to UNIX calendar overflow, do not set an expiration over 9999 days. This amount of time will cause the automatic block to take precedence over the manual block. Click Submit when you're done.

Chapter 13

Virus Blocking

Levels of Protection

Your message security service offers multiple levels of protection against viruses, including the use of virus-detection engines, early-detection filtering, protection against zero-hour threats, and antivirus heuristics. This section describes each level of protection.

Olympus Library of Virus Definitions

Google works as an Antivirus Development Partner with McAfee, and uses the same technology employed in McAfee Antivirus software to develop the Olympus library of virus definitions. The email protection service checks for virus-definition updates every minute from McAfee, and typically receives updates before they are available to all McAfee customers.

Incoming email is first scanned for viruses by the McAfee antivirus engine.

Authentium Antivirus Engine

The message security service also checks every minute for virus definition updates from Authentium.

Any incoming email that is determined to be virus free by the Olympus library is subjected to a second scan from the Authentium Antivirus engine.

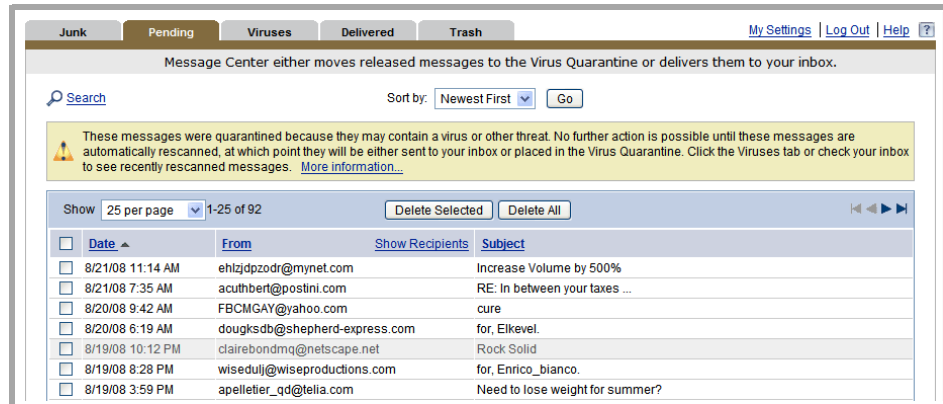
Early Detection Filtering

Even though your message security service checks for new antivirus-definition file updates every minute, there is always some delay between the discovery of a virus and its inclusion in a definition file. Live viruses that have not been included in definition files are referred to as *zero-hour threats*.

When you turn on Early Detection Filtering, a message that is not immediately identifiable as virus infected but has an executable file attached, is sequestered in the Early-Detection Quarantine.

Messages are held in the Early-Detection Quarantine for 8 hours to allow time for virus-definition files to be updated, and then those messages are scanned again for viruses based on the updated definitions. Those messages are then disposed of according to your Virus Blocking settings.

Administrators and users who have access to the Pending tab in Message Center can see messages in the Early-Detection Quarantine.



If you don't provide access to Message Center (for example, to prevent users from forwarding possible viruses from the Pending tab), you can view these messages in your own administrative quarantine by using the Early Detection (Pending) filter. For information about viewing your administrative quarantine, see "Access a Quarantine" on page 137.

Headers for messages in the Early-Detection Quarantine include the following line:

```
X-pstn-neptune-cave-rslt: pbox
```

Early-Detection Filtering is targeted to the following situations:

- You want to let executable files pass through your email system. You can configure Attachment Manager to let executable files through, and have Early-Detection Filtering examine those files for viruses. Files that are virus infected are disposed of per your Virus Blocking settings, and clean files are allowed through to their destinations.
- Implementations of the message security system that do not include Attachment Manager. In this case, you can use Early-Detection Filtering to scan messages for harmful attachments.
- Low-volume or target-specific attacks (for example, if a small number of your users are the subject of an attack by messages with virus payloads).

Additional Zero-Hour Threat Protection

The following additional zero-hour threat protection is available to you:

Attachment Manager (optional feature)	“System Threats” filter catches potentially harmful files.
Virus Blocking	The service uses heuristics to detect malformed MIME attachments and messages to augment McAfee and Authentium virus scanning.
McAfee Antivirus	McAfee’s virus heuristics engine catches some viruses before patterns can be isolated. McAfee also uses the service’s log data to help detect outbreak patterns.
Authentium Antivirus (optional feature)	Authentium’s HoloCheck™ Heuristic Technology provides a separate methodology of heuristic detection. This second scan engine provides broader coverage for inbound mail.
Advanced Antivirus Heuristics	Evaluates whether messages that are considered to be part of a botnet attack are also virus infected. All messages with attachments are quarantined.

Advanced Antivirus Heuristics

Advanced Antivirus Heuristics also examines message attachments, and works in conjunction with the spam filtering engine as part of your protection against botnet virus attacks. The heuristics provide protection against emerging threats for which antivirus signatures have not yet been released.

To apply advanced antivirus heuristics, you need to configure Spam Filtering and Virus Blocking.

How it works: Spam Blocking filters botnet attacks based on the sending behavior (botnets send messages through networks of compromised computers). When the botnet protection identifies a suspicious message, advanced antivirus heuristics scan the message, and if triggered, process the message as a virus. This helps assure that virus-infected messages are deleted or sequestered in the virus quarantine, rather than treated as junk messages.

When a message is disposed of in this fashion, the associated virus name that appears in reports is PSTN-MalwareDetection.

For more information, see “ Interpreting Header Fields” on page 637 and “ Reports” on page 551

Attachment Scanning

Virus Blocking scans messages for both complete and incomplete MIME headers (MIME headers as separate attachments from the rest of the content of an email message). Next, Virus Blocking opens and scans uncompressed and unencrypted files. Compressed file attachments are opened and recursively scanned.

Attachment Manager offers an additional layer of protection against zero-hour threats, as you can set policies to catch all executables, and you can configure Attachment Manager to bounce or quarantine system threats. Attachment Manager can filter password-protected ZIP files and other compressed attachments separately from standard compressed files.

For more details, see “ Attachment Manager” on page 403.

About Virus Blocking

Viruses, when detected, can either be deleted, quarantined in a user or administrator quarantine, or tagged as viruses in the message email headers.

Virus Blocking can be configured for incoming and outgoing messages. Contact your account manager to check whether your service package includes outgoing message support.

When Virus Blocking Occurs



During message processing, messages are filtered by Connection Manager (attack protection), Content Manager, Senders Lists, and Junk Filters. Virus Blocking then scans the messages and attachments for viruses. Clean messages are passed along to Attachment Manager so they can be filtered according to your attachment policies. As a last step, messages are passed to Early Detection Filtering so that any zero-hour threats can be stopped.

The Virus Blocking disposition has precedence over other filter dispositions. When Virus Blocking is enabled:

- All messages that are either quarantined by a filter or pass through all the filters are scanned for viruses. If a message contains a virus, it is processed according to the virus disposition. For example, if a message has been quarantined by the Junk Filter because of spam content, but the message also contains a virus, then the message is processed according to your Virus Blocking settings (e.g., the message could be deleted instead of placed in the user's quarantine).
- All message attachments are scanned and processed for viruses, regardless of whether Attachment Manager filtering is enabled.
- No Approved Senders, Attachment Manager, or Content Manager rule can override Virus Blocking to deliver a message. Even if the message is from an approved sender, the message is scanned for viruses.

See "Message Processing Order" on page 36 for details.

- When a statistically significant quantity of virus messages is quarantined from an IP, the Connection Manager will block the sending IP as a Virus Outbreak.

Order of Virus Filtering

For most customers, all incoming messages are first scanned by the McAfee Antivirus engine. The Authentium Antivirus engine then scans all inbound messages that are determined to be clean by the McAfee antivirus engine. The message service checks for virus definition updates every minute from both McAfee and Authentium.

For customers added after June 2007 on System 20 and System 7, the message service scans all incoming messages first with the Authentium Antivirus engine, and then all clean messages are scanned again by McAfee. This change of order is for optimization and measurement purposes, and does not alter the effectiveness of your anti-virus protection in any way. All messages continue to be scanned by two engines before delivery to your inbox.

Virus Definition File Updates

Virus Blocking updates the antivirus definition files for its McAfee Antivirus engine and Authentium Antivirus engine every minute. This information is for your reference only. You do not need to take any action to receive the benefits of the service's definition-file updates. The following sections outline the update details.

McAfee Virus Definition Files

Virus Blocking uses DAT files provided by McAfee that contain virus patterns for all known viruses. McAfee provides Hourly DAT files that are updated at least every hour. Most McAfee customers have access to only the Weekly DAT files, which are the numbered files listed on the McAfee Virus Information Library web site (<http://vil.nai.com>).

Virus Blocking checks for new DAT files once per minute, thereby ensuring that the most recent virus patterns are always used when processing your mail traffic.

Authentium Virus Definition Files

Virus Blocking attempts to download Authentium virus definition files once per minute. For reference, Authentium provides the following virus definition files:

Daily Definitions	These are virus definition files numbered in increments of 10 (e.g. 50340 from 2/3/2005, or 50350 from 2/4/2005).
Unscheduled Definitions	These are virus definition files posted outside the daily scheduled updates.

All definition files are publicly documented on the Authentium web site at:

<http://www.authentium.com/support/AVMatrix/VirusDefList.aspx>

Configure Inbound Virus Blocking

To configure virus blocking for incoming messages, you edit settings in these areas of the Administration Console:

- **Default user:** Turn virus blocking on/off for users in an organization, and set the notification interval.
- **Organization:** Choose how virus-infected messages are disposed of; whether to: block viruses for unregistered users, check for zero-hour threats, clean viruses from messages before delivery; and configure other settings for all users in the organization.
- **User Access:** Set whether users can change their virus settings in the Message Center.

Configuration of these settings is described below.

Configure Virus Settings for Users

You turn virus blocking on/off and set the notification interval for users by editing the default user's virus settings. If the user isn't registered in the service, the user does not receive virus-blocking protection unless you turn on Non-Account Virus Blocking for the organization to which the user belongs.

If you want to change these settings for all users, you can change the default user and all existing users by batch file. See "Manage Default User Templates" and "Manage a User's Settings" for details.

Following are the steps to configure virus settings for the default user. You can also follow steps in the event a particular user has accidentally disabled virus protection. If you wish to prevent users from configuring these virus settings using the Message Center, see "Configuring User Access to Virus Settings."

To configure virus settings for users:

1. In the Administration Console, go to **Orgs and Users > Users**.
2. Search for the user if necessary (see "Search for Users" on page 111). Click the user address.
3. Under Inbound Services, click **Virus Blocking**, then configure your default settings:

Virus Blocking	<p>Whether or not virus filtering is enabled for the user.</p> <p>Values: On/Off/Not Allowed. Default is On.</p> <ul style="list-style-type: none">• On: Virus-infected messages are quarantined unless the Message Header Tagging option is configured in the Organization that contains the user.• Off: Virus-infected messages are delivered.• Not Allowed: Virus-infected messages are delivered, and users cannot enable Virus Blocking.
Virus Notification Interval	<p>How frequently the receives notifications of quarantined viruses.</p> <p>Values: Organization default, Immediately, One per day, Disable notifications. Default is Organization default.</p> <ul style="list-style-type: none">• Organization default: Applies the default from the Notifications settings for Virus Blocking.• Immediately: Every virus quarantined generates a notification.• One per day: Only the first virus quarantined each day generates a notification.• Disable notifications: Viruses are silently quarantined. See "Quarantine Summary & Notifications" on page 273 for more information on notifications.

4. Click **Save**.

Configure Virus Settings for an Organization

The virus settings for a user organization allow you to configure the disposition of virus-infected messages and other processing options. For details on configuration of virus notification settings see “Configuring Notifications for an Organization” on page 273.

To configure virus blocking for an organization:

1. In the Administration Console, go to **Orgs and Users > Orgs**, then select an organization that contains the users for whom you want to configure virus settings.
2. Under Inbound Services, click **Virus Blocking**, then configure your settings:

Non-Account Virus Blocking	<p>Prevents virus-infected messages sent to unregistered users from reaching your mail server.</p> <p>Values: On or Off. Default is Off for customers added before June 2007, and On for customers added after June 2007.</p> <ul style="list-style-type: none">• On: Your service automatically deletes virus-infected messages that are sent to unregistered users (addresses in a domain associated with this organization but that are not registered with your service). <p>This feature is compatible with Automatic Account Creation, and we recommend turning on Non-Account Virus Blocking with Automatic Account Creation.</p> <p>Non-Account Virus Blocking affects only virus filtering, and does not provide other types of filters, such as spam filtering or Content Manager filters. For full mail filtering, add all your addresses as users or aliases.</p> <ul style="list-style-type: none">• Off: Messages sent to unregistered users are not scanned for viruses. <p>Note: Messages that are blocked by Non-Account Virus Blocking appear in the Inbound Traffic Report as “account messages” for the recipient address (see “Inbound Traffic Reports and Non-Account Virus Blocking” on page 558).</p>
-----------------------------------	---

**Early
Detection
Filtering**

Quarantines messages that *may* contain viruses.

You need to configure Spam Filtering in order to implement Early Detection Filtering.

Values: On or Off. The default is Off.

- **On:** Your message security service quarantines messages that may be zero-hour threats. Those messages are held in the Pending quarantine for a period of 8 hours until the virus-definition files have had a chance to update, and then the messages are scanned again for viruses and processed according to your Virus Blocking settings.

Authorized users can view quarantined messages in the Message Center's Pending tab, and deliver those messages during the time they are in the Early-Detection Quarantine. Messages delivered under these circumstances are not subject to virus blocking.

Before you can turn on early detection filtering, you have to click **View Confidentiality Waiver** and agree to the terms of the waiver.

If you turn on Early Detection Filtering, you need to set Inbound Attachment Manager to ignore executables so they will not be caught by Attachment Manager and can be evaluated by Early Detection Filtering.

- **Off:** Messages that may be zero-hour threats are not quarantined.

**Virus
Cleaning
(Message
Center
Classic Only)**

This setting applies **only** to Message Center Classic.

Values: On or Off. The default is On.

- **On:** In most cases, viruses cannot be cleaned from messages. (Most viruses spread by emailing themselves using a built-in SMTP server. These messages do not have valid content, so they cannot be cleaned.)
- **Off:** Users will not see the option to Clean and Deliver quarantined messages.

User Access has the related configuration "Deliver As-Is". This configuration allows a user to deliver a virus-infected message. For configuration steps, see "Enable / Disable Message Center Access" on page 252.

Note: The "Deliver As-Is" configuration is available with *Message Center Classic* only. You cannot deliver any virus-infected messages from the latest version of Message Center.

Message Fragment Bouncing	<p>Bounces fragmented messages.</p> <p>Values: On or Off. The default is On.</p> <ul style="list-style-type: none"> • On: Messages containing fragments are bounced, returning “Error 571 - Domain Does Not Accept Fragment Messages”. • Off: Messages containing fragments are quarantined. <p>RFC2046, section 5.2.2.1 provides a facility for fragmenting email messages. Since this would bypass all known virus scanning technologies, all fragmented messages are either quarantined or bounced for your users’ protection.</p>
Virus CC	<p>The address to CC for Virus Notifications.</p> <p>Value: An email address on the same server as recipient.</p> <p>These CC-ed notifications provide insight into the extent of your users’ virus troubles.</p>
Virus Disposition	<p>Choose how to dispose of messages with recognized viruses.</p> <p>Values: Bounce, User Quarantine, Quarantine Redirect, or Message Header Tagging. Default is User Quarantine.</p> <ul style="list-style-type: none"> • Bounce: Infected messages are immediately bounced upon detection. • User Quarantine: Infected messages are quarantined in the recipient’s Message Center. • Quarantine Redirect: Infected messages for users in an organization are routed to one common quarantine. This quarantine redirect address must be that of a registered administrator account. • Message Header Tagging: Infected messages are sent to your mail server with an X-pstnvirus custom header indicating the virus. <p>WARNING: If Message Header Tagging is selected, then your users receive viruses unless your mail server has rules to handle them.</p>
Apply settings and filters to existing sub-orgs	<p>Propagate Virus Blocking settings to all sub-organizations.</p> <p>Values: On/Off. The default is Off.</p>

3. Click **Save**.

Configuring User Access to Virus Settings

If you allow user access to the Message Center, we highly recommend turning off permissions to change virus settings. Otherwise, users may be able to turn off virus scanning.

1. In the Administration Console, go to **Orgs and Users > Orgs**, and select an organization from the list.
2. Under Organization Settings, click **User Access**.
3. On the User Access page, set Virus Settings to Read, or clear all the check boxes to turn them off.

See “Enable / Disable Message Center Access” on page 252 for further details.

Virus Notifications

When a virus is quarantined, notifications to users can be triggered. These notifications can be customized and the interval between notifications can be set. In general, most users do not need to be notified when viruses are quarantined. See “Quarantine Summary & Notifications” on page 273 for more information.

Virus Outbreak Events

When a statistically significant quantity of virus messages is quarantined from an IP, the Connection Manager can be configured to block the server as an attacker. See “Automatically Blocking Attacks” on page 453 for details.

Troubleshooting Virus Blocking

Why was this virus delivered despite virus blocking?

In most cases, the user receiving the message was not registered in the service. Following is the process for troubleshooting and determining what happened:

1. **Check the headers of the virus-infected email to determine the recipient, and see whether the message was sent directly to and was accepted by your mail server, bypassing the service:**
 - a. Many email clients put messages from different servers into the same inbox, so a user may believe the virus-infected message was received from a server protected by the service. Review the email headers to make sure that they include your email server. If they do, continue to the next step. If they do not, inform the recipient of this condition.
 - b. Some viruses propagate by a method that does not follow DNS standards for selecting MX records. They send an email to the highest numbered server, or randomly pick one from port scans. To determine if the email actually passed through the service, review the message headers for the strings listed below (the pound sign is replaced by various numbers). If any of these strings exist in the header, write down the addresses in the To field and continue to the next step. If none of the strings exist, the message was delivered directly to your email server.

```
exprod#mx#.postini.com  
chipmx#.postini.com  
chip#mx#.postini.com  
eu#sys#amx#.postini.com
```

Resolution: The message was delivered directly to your email server and did not go through the service. To remedy this, set up your email server or firewall to only accept email from the service's IP ranges. See "Setting Up Secure Mail Delivery" on page 495 for details on how to prevent this.

2. **Check whether virus blocking is enabled and make sure it is not set to Message Header Tagging.**
 - a. Click the Orgs and Users tab, and search for the organization that contains the user who received the message.
 - b. Click **Virus Blocking**.
 - c. If the Virus Disposition is set to Message Header Tagging, then all messages containing viruses are delivered to your mail server. Perform the resolution below. Otherwise, continue to the next step.

Resolution: As necessary, configure a different disposition, or configure your mail server to dispose of all messages that contain the custom header `x-pstn-virus`.

3. **If the Virus Disposition is set to User Quarantine or Quarantine Redirect, check whether the recipient of the message has a user account.**
 - a. Click the **Users** tab and enter the address in the Find User field.
 - b. Click **Search** to determine if the user exists.
 - c. If the user does exist, click its address, then click **Virus Blocking** to make sure that Virus Blocking is On.
 - d. If the user does not exist, perform the resolution below. Otherwise, continue to the next step.

Resolution: Create a user account for the email address, or add it as an alias to the already existing primary user account.

At this point, you have confirmed that virus filtering is configured properly. The following steps show you how to proceed in this case:

1. **Check whether the virus has been recently discovered by McAfee or Authentium:**

The email may contain a virus that the virus engine did not know about. There is a lag time between the initial outbreak of a virus and the implementation of an update to the antivirus definition file that allows the virus protection engine to detect (and thus quarantine) the virus. This time is usually very short. During this time, new viruses may not be detected by virus blocking.

- a. If you do not know the McAfee and Authentium names for the virus, search the Internet for the name of the virus. Searching should include web sites for any other virus protection software you use. This often shows you the McAfee and Authentium names for the virus. If not, then use common search engines using other names for the virus.
- b. Search the McAfee web site for the name of the virus; this tells you if/when the antivirus definition files provided by McAfee first protected you from this virus.

`http://vil.nai.com`

- c. If your service package includes Authentium Antivirus, also check Authentium to find out when it first protected you from this virus.

`http://www.authentium.com/support/AVMatrix/portal.aspx`

- d. If the date of the message is before the protection date and time, then follow the resolution below. Otherwise, proceed to the next step.

Resolution: This is the source of the virus delivery. No further analysis is required, and McAfee or Authentium has the definition on record.

2. **Check the file size of the virus attachment.**

If the virus was delivered after the protection date and time determined above, then compare the file size of the virus attachment with the documented size of the virus listed on the web site of McAfee or Authentium. If the size of your virus is significantly smaller, then follow the resolution below. Otherwise, proceed to the next step.

Resolution: The virus payload was truncated, making the virus inert and preventing detection. Viruses like this can be deleted since they pose no threat.

3. If you are still unable to find it, the submit a copy of the original virus-infected message as an attachment or as comments to Support.

Support escalates to McAfee and/or Authentium in the event they are not aware of the virus.

Virus Blocking seems to block legitimate messages.

Virus Blocking either quarantines or blocks all fragmented messages, since fragmented messages cannot be properly scanned. Message fragmenting is not used widely since most mail messages can be sent within the SMTP standard using the common networking technologies and processing power of today's computers.

See "Configure Virus Settings for an Organization" on page 318 for details on the Virus Fragment Blocking setting.

Health Check: Update Virus Settings

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration.

Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust. Use the instructions below to make any adjustments if necessary to your virus settings.

To update your virus settings for Health Check, do the following:

1. Set both "Message Fragment Bouncing" and "Non Account Virus Blocking" to ON:

- a. In the Administration Console, go to **Orgs and Users > Orgs**, then select an organization that contains the users for whom you want to configure virus settings.
- b. Under Inbound Services, click **Virus Blocking**.



- c. Configure your settings as shown below, and then click **Save**.

Message Fragment Bouncing

This setting bounces fragmented messages.

Values: On or Off. The default is On.

On: Messages containing fragments are bounced, returning “Error 571 - Domain Does Not Accept Fragment Messages”.

Off: Messages containing fragments are quarantined.

RFC2046, section 5.2.2.1 provides a facility for fragmenting email messages. Since this would bypass all known virus scanning technologies, all fragmented messages are either quarantined or bounced for your users' protection.

Non-Account Virus Blocking

This setting prevents virus-infected messages sent to unregistered users from reaching your mail server.

Values: On or Off. Default is Off for customers added before June 2007, and On for customers added after June 2007.

For additional details and instructions on your virus settings, see “Configure Virus Settings for an Organization” on page 318.

2. Set the "Virus Outbreak" sensitivity in Connection Manager to VERY HIGH.

A virus outbreak is a DoS attack whereby a statistically significant amount of virus traffic relative to valid email traffic is received from a particular sending server over a time period. This setting identifies a sudden spike in the volume of virus-laden messages relative to total inbound messages.

To configure Connection Manager:

- a. In the Administration Console, go to **Orgs and Users > Orgs**, then select an organization that contains the users for whom you want to configure Connection Manager.
- b. Click **Inbound Servers**, and select **Connection Mgr** on the tab bar.
- c. Click **Edit**.
- d. In the Sensitivity drop-down list for Virus Outbreak, select **Very High**.
- e. Click **Submit**.

For more information about Connection Manager and setting Virus Outbreak sensitivity level, see “Connection Manager” on page 453.

3. To protect against zero hour viruses (emerging threats in the environment), do either of the following:

Set "Early Detection Filtering" to ON

See "Set Early Detection Filtering to ON" on page 326.

--or--

Set "System Threats" to Bounce or Quarantine, and set both "Binary Scanning" and "Scan Inside Compressed Files" to ON

See "Set "System Threats" to Bounce or Quarantine, and set both "Binary Scanning" and "Scan Inside Compressed Files" to ON" on page 326

Set Early Detection Filtering to ON

Early Detection Filtering provides protection against zero hour viruses. Messages that contain suspicious content and messages with executable file attachments (for example, .exe, .vbs, and .cmd files) are temporarily quarantined for deeper analysis and rescanned by the service's antivirus engines with updated signatures.

If Early Detection determines that the message is uninfected, it's automatically released and delivered as normal to the user.

To enable Early Detection Filtering for an organization:

1. In the Administration Console, go to **Orgs and Users > Orgs**, then select an organization that contains the users for whom you want to configure Early Detection Filtering.
2. Under Inbound Services, click **Virus Blocking**.
3. For Early Detection Filtering, select **On**.
4. Click **Save**.

Early Detection Filtering works only when you have Spam Filtering turned on (the default setting).

Set "System Threats" to Bounce or Quarantine, and set both "Binary Scanning" and "Scan Inside Compressed Files" to ON

Attachment Manager offers an additional layer of protection against harmful files and zero-hour threats.

To configure Attachment Manager:

1. Go to **Orgs and Users > Orgs** and select an organization that contains your users.
2. Click the Attachment Manager icon in the Inbound Services or Outbound Services section.
3. Click **Filters** in the gray bar.

4. Under Scanning Options near the top of the page, select the check boxes for **Scan inside compressed file types** and **Enable binary scanning**.
5. Under System Threats, select **Bounce** or **User Quarantine** from the drop-down lists for Executables and Compressed Files.
6. Under Custom File Types, delete any custom executable file types specified in the Approve field, and copy them to Bounce or User Quarantine.
7. Click **Save** at the bottom of the page.

Note: System Threat filters approve, bounce, or quarantine a collection of compressed and executable file formats, including .exe, .zip, .tar, and many others, as well as attachments with multiple file extensions, such as .tar.gz.

Binary scanning is an optional method for identifying file attachments; it identifies an attachment by checking its binary content instead of the file extension. You can enable binary scanning from the Attachment Manager Filters page. When you enable binary scanning, Attachment Manager will then use binary scanning to identify file types for all of your filters (Custom File Types, System Threats, and Productivity filters).

See “ Attachment Manager” on page 403 for more details and instructions.

Related Topics

- **Health Check: Update User Settings**
- **Health Check: Approved Senders List Cleanup**
- **Health Check: Update Settings for Executable Attachments**
- **Configure Virus Settings for an Organization**
- **Configure Inbound Virus Blocking**
- **Attachment Manager**

Chapter 14

Content Manager

About Content Manager

Content Manager scans email messages for specific content—*words, phrases, or text patterns*—and then takes an action on any messages that contain that content. For example, you can set up Content Manager to quarantine any inbound message that contains specific text in its subject line. Use Content Manager to help secure your network, enforce email content policies, prevent leakage of proprietary information, and protect private information.

To use Content Manager, you must first configure it for one or more organizations in your organization hierarchy. You can then do either of the following:

- Create custom content filters to specify the content to scan for
- Set up content compliance policies, which include comprehensive, predefined content filters

Two versions of Content Manager are available:

- **Inbound Content Manager:** Scans email messages sent to your users from outside your network. Inbound Content Manager is included with most service packages.
- **Outbound Content Manager:** Scans messages that your users send to others outside your network. Outbound Content Manager requires the *Outbound Services* option.

Note: For information about the options your service package includes, contact your account manager.

Content Manager Features

You can use Content Manager to filter both inbound and outbound email messages. To filter messages, you can create *custom content filters* and set up *content compliance policies*.

Custom Content Filters

A custom content filter comprises up to three *content rules* and a *message disposition*. Each rule contains a word or phrase that you specify. Or, a rule can contain a text pattern, called a *regular expression*, rather than specific text. Content Manager scans messages for content that matches one or more rules in the filter. If a message contains a content match, Content Manager takes action on the message according to the message disposition for the filter.

For instructions on creating a content filter, see “Create or Edit a Content Manager Filter” on page 340.

Compliance Policies

A compliance policy comprises a *lexicon*—a predefined set of words, phrases, and text patterns—and a *message disposition*. Content Manager scans messages for content that matches content in the lexicon. If a message contains a match, Content Manager takes action on the message according to the message disposition. Currently, Content Manager includes compliance policies for *social security numbers* and *credit card numbers*. Use these policies to help protect personal information and enforce compliance at your company.

Important: The lexicons are designed to provide a high level of filtering accuracy. However, because patterns for social security and credit card numbers are highly variable, these lexicons may not capture all messages that contain social security or credit card numbers. In addition, these lexicons may capture messages that contain numerical patterns that are not social security or credit card numbers.

For instructions on setting up a compliance policy, see “Set Up a Compliance Policy” on page 345.

Regular Expressions

Instead of creating simple content filters that can find only single words or phrases, you can use regular expressions to create more efficient or sophisticated content filters. A regular expression, also called a *regex*, is a method for matching text with patterns. For example, a regular expression can describe the pattern of a telephone number, an email address, a URL, or your company's employee identification numbers. It can also describe a list of words.

For more information about using regular expressions, see “About Using Regular Expressions” on page 349.

File Attachment Scanning

You can create content filters that scan all parts of an email message, including any text-based file attachments. If you set up a compliance policy, file attachments are scanned automatically.

For details, see “Attachments That Content Manager Scans” on page 335.

Outbound Message Scanning

Outbound Content Manager filters messages that your users send to addresses outside your network. Outbound Content Manager is an optional feature.

If you filter outbound messages based on recipient, the following apply:

- The filter is applied if *any* recipient (rather than *all* recipients) meets the criteria.
- Filters consider the To and Cc recipients, but not the Bcc recipients.

For example, if you create a filter to block email to all but one domain, then all recipients of the message must be in that domain. If any recipient has an address outside the domain, then the message is delivered to all recipients.

To use Outbound Content Manager, your message security service must include *Outbound Services*. For more information about your message security service features, contact your account manager.

Before using Outbound Content Manager, you must enable Outbound Services. For instructions, see “Outbound Concepts” on page 508.

What You Can Do with Content Manager

The following are the general ways you can use custom content filters and compliance policies in Content Manager.

Note: Some of the examples that follow include creating filters for outbound email. Content Manager can scan outbound email only if you’ve set up Outbound Services. For details, refer to the following guide:

Outbound Services Configuration Guide

Enforce content rules for your organization

You can create content filters to enforce a corporate policy against specific types of content in email messages. For example, you could enforce a policy against football betting pools by creating an inbound or outbound filter that quarantines messages that contain the words “football”, “bet”, and “pool.”

Monitor or review messages with specific content

You can monitor or review messages that contain specific content rather than bounce or quarantine them. For example, if you want to receive copies of any outbound messages that contain social security numbers, you could set up the Social Security Numbers compliance policy to place copies of these messages in an administrator's quarantine for review.

Encrypt messages that contain personal or confidential information

If your message service includes the Message Encryption option, you can encrypt email messages that contain personal or confidential information. For example, you could create a content filter to encrypt any outbound messages that contain a credit card number.

Note: For details about the Message Encryption option, refer to the *Encryption Services Administration Guide*.

Protect proprietary information

You can use Content Manager to help prevent recipients outside your company from receiving messages with proprietary information. For example, you could create a content filter that scans outbound messages for references to proprietary information, such as the code name for a new product your company is developing. If a message contains the code name, Content Manager can “bounce” the message back to the sender, along with a message stating that the message violates your email policy.

Allow certain content to bypass spam filters

You can use Content Manager to assure that no incoming resumes are ever quarantined, regardless of spam-like message content. For example, you could create a content filter that looks for the word “resume” in the subject or body of the message and allows messages that contain that word to bypass the spam filters.

Temporarily stop junk mail

If you experience severe problems with specific junk messages, you can create a content filter to block these messages. However, take caution when creating such filters, because they may increase the chances of blocking legitimate messages. For details, see “How to Use Content Manager in a Spam Outbreak” on page 364.

Important: In general, use Content Manager for enforcing company content policies, not for filtering spam.

How Content Manager Works

Content Manager works with the junk, virus, and attachment filters of your message security service to provide you with additional control and protection of your email.

Where Content Filters Apply

Content Manager is an organization-level feature. Therefore, content filters apply only to the user accounts in the user organization in which you create those filters. If you want a content filter to apply to all users on your message security service, ensure that you create the same filter in all the user organizations in your organization hierarchy. For details about organization hierarchies, see “Organization Management” on page 81.

When Content Filters Apply



The message security service applies Inbound Content Manager filters after Connection Manager (attack blocking), but before Sender Lists, Junk Filters, Virus Blocking, and Attachment Manager. As a result:

- **Messages with approved content are not filtered as spam.**

If a message is captured by a content filter or compliance policy with a disposition of **Approve**, it bypasses the Junk Filters, even if it contains spam-like content.

- **Approved senders can optionally bypass content filters.**

If you configure Inbound Content Manager to allow all email from organization-level approved senders, your message security service delivers any messages from these senders, even if their messages contain content that a content filter would otherwise bounce or quarantine. Messages from senders that are on only an individual user’s approved senders list cannot bypass content filters.

- **Content Manager approved or quarantined messages are scanned for viruses.**

A message infected with a virus, or that contains an attachment prohibited by an attachment filter, isn’t delivered to users, even if it contains approved content.

How Content Manager Scans Email Messages

Message Components Scanned

When you create a custom content filter, you can choose to scan specific parts of an email message, including the headers, subject line, sender, recipient, or body. You can also choose to scan all parts of a message—that is, the entire message—including any unencrypted attachments. If you set up a compliance policy, Content Manager always scans all parts of a message, including any unencrypted binary attachments.

Types of Content Scanned

In any part of an email message, Content Manager scans the text-based or HTML content, as well as any MIME (base-64) sections for binary attachments (the sections that usually appear as “gibberish” in the message source). If you choose the option to scan the entire message, Content Manager also *decodes and then scans* sections in MIME and quoted-printable encoding (for non-ASCII text). In this case, Content Manager also scans the actual text content of binary attachments.

When Content Scanning Occurs

Content Manager scans all information transmitted during the DATA phase of an SMTP session. It does not scan sender or recipient content transmitted during the MAIL FROM or RCPT TO phase of an SMTP session.

How Quickly Content Scanning Occurs

Content Manager takes just milliseconds to scan a message according to all content rules and then execute the disposition of any filter that captures it. Therefore, the use of Content Manager does not affect the speed at which the message security service processes your email.

Attachments That Content Manager Scans

When you create a content filter, you can choose to scan any part of a message or all parts of a message. If you select the **Body** option for a filter rule, Content Manager also scans any plain-text attachments. If you select the **Entire Message** option, Content Manager scans text-based content in many types of file attachments, including:

- Text files
- HTML files
- Documents created with Microsoft Office 2003 or earlier versions (Word, PowerPoint, and Excel)
- Forwarded email messages
- Various types of other files with text-based content

Note: For binary file attachments, such as Microsoft Office documents, Content Manager decodes and then scans the MIME (base-64 encoded) parts of the email message.

Content Manager *does not* scan attachments that are:

- ZIP or other types of compressed files
- Microsoft 2007 Office documents
- Over 100 MB
- PDF files

How Outbound Content Manager Works

Outbound Content Manager filters the messages that your users send to recipients outside your network. You create outbound content filters in the same way you create inbound content filters, except that the **User Quarantine** and **Blackhole** dispositions are not available.

Note:

- If a user forwards a message to someone outside your network, Outbound Content Manager scans it. The user who forwarded the message is considered the sender.
- If your message security service routes an outbound message back through your email server (a process called *rejection*), Outbound Content Manager scans the message again. For details, see “Outbound Concepts” on page 508.
- Before using Outbound Content Manager, you must enable Outbound Services. For details, see “Outbound Concepts” on page 508.

Content Filter Limitations

You can create approximately 40 to 60 custom content filters *per organization* in your organization hierarchy, depending on the number and complexity of the rules you specify for the filters. This limit applies to the overall number of filters you create for both Inbound Content Manager and Outbound Content Manager.

The value you specify for a rule—that is, the text for which you want to scan messages—must be in ISO 8859-1 (Latin) character encoding.

Important: If you use regular expressions to specify filter values, additional limitations apply. For details, see “About Using Regular Expressions” on page 349.

About Message Dispositions

For each content filter or compliance policy that you set up in Content Manager, you must specify a message disposition. A disposition tells Content Manager what action to take on a messages it captures. For example, Content Manager can send the message to the user’s or an administrator’s quarantine in Message Center, delete (blackhole) it, or return it to the sender (bounce it). It can also send a copy of the message to an administrator’s quarantine, but let the message through to its intended recipient.

For details about the dispositions you can use, see “Message Dispositions” on page 379.

Order of Precedence of Filters and Policies

Custom content filters and compliance policies take precedence over encryption settings.

If your service includes the Message Encryption option, both content filters and compliance policies take precedence over encryption settings. For example, assume an email message contains body text the matches a content filter *and* a confidential header that matches an encryption setting. If the content filter is configured to **Copy to Quarantine**, Content Manager quarantines the message, and does not deliver or encrypt it.

The least severe disposition takes precedence over more severe dispositions.

If two or more custom content filters or compliance policies contain a match for a message, the filter or policy with the least severe disposition takes precedence. The following is the order, from least severe to most severe:

1. **Deliver**
 - **Bypass junk filters** (Inbound only)
 - **Encrypt** (optional feature; Outbound only)
2. **Copy to Quarantine**

3. **Bounce**

4. **Delete (Blackhole)**

For example, assume an email message contains text that matches two separate content filters. If one filter is configured to **Copy to Quarantine** and the other is configured to **Bounce**, Content Manager quarantines the message instead of bouncing it.

Note: The order of disposition precedence *does not* apply to virus-infected messages: your message security service always quarantines or deletes them.

For details about dispositions, see “Message Dispositions” on page 379.

Compliance policies take precedence over custom content filters with the same dispositions.

If a content filter and a compliance policy *both* contain a match for a message, and they both have the same message disposition, the compliance policy takes precedence. For example, assume an email message contains a number that matches both a content filter you created *and* the Credit Card Numbers policy. If both the content filter and the policy are configured to **Copy to Quarantine**, Content Manager reports, and the message header indicates, that the message was quarantined based on the policy, not the custom filter.

View Content Manager Filters and Policies

The Content Manager filter-list page for an organization shows a list of the available compliance policies and any custom content filters you created for that organization. This page is available for both Inbound Content Manager and Outbound Content Manager.

Note: Outbound Content Manager is an optional feature. For details about using Outbound Content Manager, see “How Outbound Content Manager Works” on page 335.

To view Content Manager filter and policies for an organization:

1. Go to **Orgs and Users > Orgs**, and select an organization that contains the users whose messages you want to filter.
2. Under **Inbound Services** or **Outbound Services**, click the **Content Manager** icon.

The Content Manager filter list appears, showing the current filters and settings.

Inbound Content Manager - Archive Stable Users

Filter inbound messages based on their content. Filters apply to this organization and new sub-orgs you add. To copy the following settings to existing sub-orgs, click [Edit Settings](#) and apply the settings and filter definitions to sub-orgs.

Content Filtering: **ON** Quarantine Administrator: wflintstone@arc.in.dev1.postini-corp.com
 Approved Senders: **OFF** Bounce Message: ERROR 582: This message violates our email policy. [Edit Settings](#)

You are currently using 32% of your allowed filter space

Content Manager applies filters in the following order. To change the order, click the up and down arrows or change the sequence numbers and click [Update Priority List](#). Click [Save Priority List](#) to save the filter list order. To edit a filter, clicks its name.

[Update Priority List](#) | [Add Custom Filter](#) [Printer-friendly](#)

Filter Name	Status	Description	Routing	Copy to Quarantine	% of Total
1 Social Security Numbers	ON	Compliance Policy: Protects social security numbers	Deliver	Quarantine Administrator	<input type="text"/>
2 Credit Card Numbers	OFF	Compliance Policy: Protects credit card numbers	Deliver	Quarantine Administrator	<input type="text"/>
3 filter_1	OFF	Entire Message does not match regex "ab" OR...	Delete (Blackhole)	Quarantine Administrator, cmburns@arc.in.dev1.postini-corp.com, Recipient (+2)	<input type="text"/>

If this is the first time you've accessed this page, none of the policies are on, nor are there any filters configured. See "Configure Content Manager" on page 338.

Configure Content Manager

You configure Content Manager at the organization level. When configuring Content Manager, you can:

- **Turn Content Manager on or off:** Before you can create a new content filter or set up a compliance policy, you must turn on Content Manager.
- **Specify the account that receives quarantined messages:** If you create a content filter or set up a policy that copies captured messages to an administrator's quarantine, specify the email address for the account.
- **Choose your approved senders policy:** Choose whether to allow all inbound messages from approved senders to bypass content filters and policies.
- **Create a custom bounce message:** If you create a content filter or set up a policy that returns captured messages to their senders, customize the message that the senders receive.
- **Apply settings and filters to existing suborganizations:** Quickly configure Content Manager for existing suborgs with the settings and filters of their parent organization.

WARNING: Applying settings to suborgs also overwrites any existing content filters you've set up in those suborgs.

To configure Content Manager:

1. Access Content Manager for the organization that contains the users whose messages you want to filter. For details, see “View Content Manager Filters and Policies” on page 337.

Inbound Content Manager - Archive Stable Users

Filter inbound messages based on their content. Filters apply to this organization and new sub-orgs you add. To copy the following settings to existing sub-orgs, click **Edit Settings** and apply the settings and filter definitions to sub-orgs.

Content Filtering: ON **Quarantine Administrator:** wflintstone@arc.in.dev1.postini-corp.com
Approved Senders: OFF **Bounce Message:** ERROR 582: This message violates our email policy. [Edit Settings](#)

You are currently using 32% of your allowed filter space

Content Manager applies filters in the following order. To change the order, click the up and down arrows or change the sequence numbers and click **Update Priority List**. Click **Save Priority List** to save the filter list order. To edit a filter, clicks its name.

[Update Priority List](#) | [Add Custom Filter](#) [Printer-friendly](#)

Filter Name	Status	Description	Routing	Copy to Quarantine	% of Total
1 Social Security Numbers	ON	Compliance Policy: Protects social security numbers	Deliver	Quarantine Administrator	<input type="text"/>
2 Credit Card Numbers	OFF	Compliance Policy: Protects credit card numbers	Deliver	Quarantine Administrator	<input type="text"/>
3 filter 1	OFF	Entire Message does not match regex "ab" OR...	Delete (Blackhole)	Quarantine Administrator, cmburns@arc.in.dev1.postini-corp.com, Recipient (+2)	<input type="text"/>

2. Click the **Edit Settings** link.
3. Specify settings to configure Content Manager. For details about the settings, see “Content Manager Configuration Settings” on page 372.

After you enable Content Manager, you can:

- **Create custom content filters.** For details, see “Create or Edit a Content Manager Filter” on page 340.
- **Set up compliance policies.** Policies are available for:
 - Social security numbers
 - Credit card numbers

For details, see “Set Up a Compliance Policy” on page 345.

Create or Edit a Content Manager Filter

A content filter can contain up to three content rules and a message disposition (what Content Manager does with the captured message). A rule specifies the following:

- **The content to scan for:** The content, or rule value, can be an exact word, phrase, or string of characters. Or, it can be a text pattern in the form of a *regular expression*. For more information, see “About Using Regular Expressions” on page 349.
- **The location to scan:** Message locations include the subject line, sender, recipient, body text, or header—or the entire message, including attachments.
- **The type of filter to use:** A filter type specifies how the filter scans for content—for example, a filter can look for an exact match of a word or phrase, or it can look for any text that begins with a specific string of characters.

Tip: After you create or edit a content filter, you can apply your changes to all suborganizations. For details, see “Configure Content Manager” on page 338.

To create a content filter:

1. Go to the Content Manager filter-list page for the organization that contains the users whose messages you want to filter. For details, see “View Content Manager Filters and Policies” on page 337.
2. Ensure that **Content Filtering** is **On**. For details about turning on Content Manager, see “Configure Content Manager” on page 338.
3. Click the **Add Custom Filter** link.

The Add Filter page appears (this example uses the Inbound page):

Inbound Content Manager - Archive Stable Users

Add or edit a content filter. The settings for new filters apply to this organization and new sub-orgs you add. You can copy settings to existing sub-org on the [Settings](#) page.

Filter Name

Filter Status When On, scans email messages using this filter's rules. If a message matches a rule, Content Manager applies the selected routing.

Rules Create up to three rules for filtering messages. A filter applies to IM messages only if the location is **Body** or **Sender**. [More information and examples...](#)

Match:

1.

2.

3.

Routing Select the primary routing for messages that match for this filter.

Deliver Bypass junk filters
 Bounce
 Delete (Blackhole)

Copy to Quarantine Copy messages that match this filter to one or more quarantines regardless of routing.
[Add quarantine address](#)

4. Under **Filter Name**, enter a descriptive name for the filter.
5. Under **Filter Status**, select **ON**.
6. Under **Rules**, in the **Match** drop-down list, choose whether Content Manager executes this filter's disposition if an email message contains a match for *any rule* or *all rules* you specify.
7. Under **Rules**, specify up to three rules for this filter. For details about the options for creating rules, see "Filter Rules" on page 374.
8. Click **Save**.

To edit a content filter:

1. Go to the Content Manager filter-list page for the organization that contains the filter you want to edit. For details, see "View Content Manager Filters and Policies" on page 337.
2. Ensure that the Content Manager **Filter Status** is **On**. For details about turning on Content Manager, see "Configure Content Manager" on page 338.

- Click the name of a filter you want to edit. For example:

Inbound Content Manager - Archive Stable Users

Filter inbound messages based on their content. Filters apply to this organization and new sub-orgs you add. To copy the following settings to existing sub-orgs, click **Edit Settings** and apply the settings and filter definitions to sub-orgs.

Content Filtering: **ON** Quarantine Administrator: wfintstone@arc.in.dev1.postini-corp.com
 Approved Senders: **OFF** Bounce Message: ERROR 582: This message violates our email policy. [Edit Settings](#)

You are currently using 32% of your allowed filter space

Content Manager applies filters in the following order. To change the order, click the up and down arrows or change the sequence numbers and click **Update Priority List**. Click **Save Priority List** to save the filter list order. To edit a filter, clicks its name.

[Update Priority List](#) | [Add Custom Filter](#) [Printer-friendly](#)

Filter Name	Status	Description	Routing	Copy to Quarantine	% of Total
1 Social Security Numbers	ON	Compliance Policy: Protects social security numbers	Deliver	Quarantine Administrator	<input type="text"/>
2 Credit Card Numbers	OFF	Compliance Policy: Protects credit card numbers	Deliver	Quarantine Administrator	<input type="text"/>
3 filter 1	OFF	Entire Message does not match regex "ab" OR...	Delete (Blackhole)	Quarantine Administrator, cmburns@arc.in.dev1.postini-corp.com, Recipient (+2)	<input type="text"/>

- Edit information about the filter. For details, see “Content Manager Filter Settings” on page 374.
- Click **Save**.

Set Up Common Content Filters

The following table provides instructions for creating common types of content filters. For each filter, also select the **Routing** method you want to apply—that is, the action you want Content Manager to take if the filter captures a message.

To capture messages that contain this content:	Enter the following:
Specific word or phrase in the message Subject	Match: Any Rule Select Location: Subject Line Select Filter Type: matches regex Value: Enter the word or phrase, in the following regex syntax: <ul style="list-style-type: none"> For a single word, enter: <code>\word\W</code> For a phrase, separate words with <code>\s</code>: <code>\word\sword\W</code> <p>Tip: To capture messages don't contain any other text in the Subject line, select equals for the Filter Type, and enter the word or phrase <i>without</i> using regex syntax.</p>

To capture messages that contain this content:	Enter the following:
<p>Specific word or phrase in the message body</p>	<p>Match: Any Rule</p> <p>Select Location: Body</p> <p>Select Filter Type: matches regex</p> <p>Value: Enter the word or phrase, in the following regex syntax:</p> <ul style="list-style-type: none"> • For a single word, enter: <code>\Wword\W</code> • For a phrase, separate words with <code>\s</code>: <code>\Wword\sword\W</code>
<p>Specific word or phrase in any part of a message, including attachments</p>	<p>Match: Any Rule</p> <p>Select Location: Entire Message</p> <p>Select Filter Type: matches regex</p> <p>Value: Enter the word or phrase, in the following regex syntax:</p> <ul style="list-style-type: none"> • For a single word, enter: <code>\Wword\W</code> • For a phrase, separate words with <code>\s</code>: <code>\Wword\sword\W</code>
<p>Specific type of attachment</p>	<p>Match: Any Rule</p> <p>Select Location: Header</p> <p>Select Filter Type: contains text</p> <p>Value: File name or just the file extension. For example: <code>viralfile.exe</code> or <code>.exe</code></p> <p>Note: The header for attachments appears in messages only if the sender's or recipient's email client supports attachment headers.</p> <p>Tip: For more attachment-filtering options for specific files or types of files, use Attachment Manager. For details, see "Attachment Manager" on page 403.</p>

To capture messages that contain this content:	Enter the following:
<p>Attachment of any type</p>	<p>Match: Any Rule</p> <p>Select Location: Header</p> <p>Select Filter Type: contains text</p> <p>Value: Content-Disposition: attachment; filename=</p> <p>Note: The header for attachments appears in messages only if the sender's or recipient's email client supports attachment headers.</p>
<p>Sender address from one or more specific domains</p>	<p>Match: Any Rule</p> <p>Select Location: Sender</p> <p>Select Filter Type: contains text</p> <p>Value: Domain of sender, such as badsender.com</p> <p>Note: Use the more general contains text as opposed to equals to allow for variations in the From syntax employed by different mail servers and clients.</p> <p>Tip: To enter another domain, create another rule. Alternatively, enter a list of several domains by selecting matches regex and entering regular expression. For details, see "Examples of Regular Expressions" on page 356.</p>
<p>Two specific words, but only if they <i>both</i> appear anywhere in the message body</p>	<p>Match: All Rules</p> <p>Rule 1:</p> <p>Select Location: Body</p> <p>Select Filter Type: matches regex</p> <p>Value: Enter the word in the following regex syntax: \Wword\W</p> <p>Rule 2:</p> <p>Select Location: Body</p> <p>Select Filter Type: does not contain</p> <p>Value: Word or phrase that appears in the message body</p>

To capture messages that contain this content:	Enter the following:
Specific word or phrase, but only if another word does not appear in the same message	Match: All Rules Rule 1: Select Location: Body Select Filter Type: matches regex Value: Enter the word in the following regex syntax: <code>\Wword\W</code> Rule 2: Select Location: Body Select Filter Type: matches regex Value: Enter the word in regex syntax: <code>\Wword\W</code>

Set Up a Compliance Policy

A compliance policy contains a lexicon (a predefined content filter) and a message disposition (what Content Manager does with the captured message). The following policies are currently available:

- **Social security numbers:** Use this policy to scan messages for text in the pattern of a social security number. For details, see “Social Security Numbers Policy” on page 381.
- **Credit card numbers:** Use this policy to scan messages for text in the pattern of a credit card number. For details, see “Credit Card Numbers Policy” on page 383.

Tip: After you set up a compliance policy, you can apply your changes to all suborganizations. For details, see “Configure Content Manager” on page 338.

To set up a compliance policy:

1. Go to the Content Manager filter-list page for the organization that contains the users whose messages you want to filter. For details, see “View Content Manager Filters and Policies” on page 337.
2. Ensure that Content Filtering is **On**. For details about turning on Content Manager, see “Configure Content Manager” on page 338.

3. Click the link for the compliance policy you want to set up:
 - **Social Security Numbers**
 - **Credit Card Numbers**

Inbound Content Manager - Archive Stable Users

Filter inbound messages based on their content. Filters apply to this organization and new sub-orgs you add. To copy the following settings to existing sub-orgs, click [Edit Settings](#) and apply the settings and filter definitions to sub-orgs.

Content Filtering: **ON** Quarantine Administrator: wflintstone@arc.in.dev1.postini-corp.com
 Approved Senders: **OFF** Bounce Message: ERROR 582: This message violates our email policy. [Edit Settings](#)

You are currently using 32% of your allowed filter space

Content Manager applies filters in the following order. To change the order, click the up and down arrows or change the sequence numbers and click [Update Priority List](#). Click [Save Priority List](#) to save the filter list order. To edit a filter, clicks its name.

[Update Priority List](#) | [Add Custom Filter](#) [Printer-friendly](#)

Filter Name	Status	Description	Routing	Copy to Quarantine	% of Total
1 Social Security Numbers	ON	Compliance Policy: Protects social security numbers	Deliver	Quarantine Administrator	
2 Credit Card Numbers	OFF	Compliance Policy: Protects credit card numbers	Deliver	Quarantine Administrator	
3 filter_1	OFF	Entire Message does not match regex "ab" OR...	Delete (Blackhole)	Quarantine Administrator, cmburns@arc.in.dev1.postini-corp.com, Recipient (+2)	

The policy setup page appears. For example:

Turn this policy **on** or **off** and set the primary routing for messages that match lexicon content. Copy these settings to existing sub-orgs on the [Settings](#) page.

Policy Name Social Security Numbers

Description This policy includes a lexicon that recognizes social security numbers. [More information...](#)

Filter Status When On, scans email messages using this filter's rules. If a message matches a rule, Content Manager applies the selected routing.

Routing Select the primary routing for messages that match for this filter.

Deliver Bypass junk filters
 Bounce
 Delete (Blackhole)

Copy to Quarantine Copy messages that match this filter to one or more quarantines regardless of routing.
[Add quarantine address](#)

1. [Remove](#)

4. Under **Filter Status**, select **ON** or **OFF** to activate or deactivate the policy.
5. Under **Routing**, select the routing option you want to apply. For more information about routing options, see “Message Dispositions” on page 379.
6. Under **Copy to Quarantine**, add the quarantines to which you want messages sent. For more information about quarantine options, see “Message Dispositions” on page 379.

7. Click **Save**.

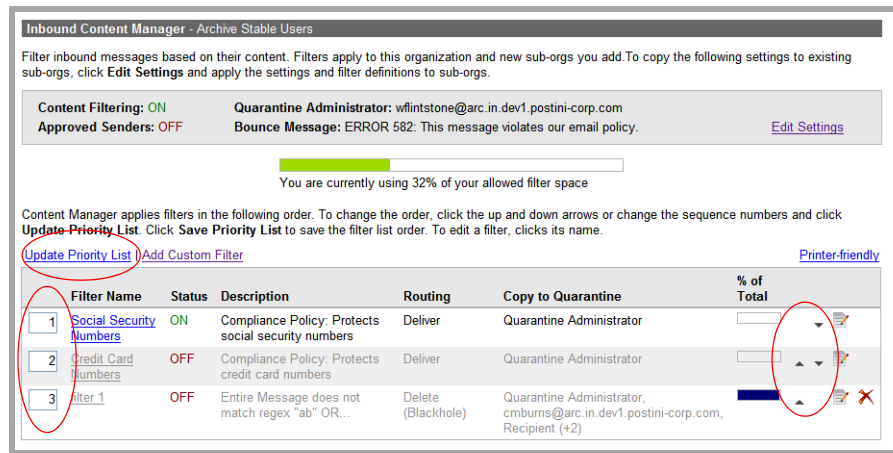
Note: For information about how report data is interpreted based on your configuration of filters, see the notes for Domain/Account and Filter Name reports in “Content Manager Reports” on page 572.

Reorder Content Filters and Policies

Content Manager applies filters and policies in the order in which they are listed.

To reorder the filter list:

1. Enter new order numbers for the filters and policies and click **Update Priority List**, or click the Up or Down arrow for a filter.



The screenshot shows the 'Inbound Content Manager - Archive Stable Users' interface. At the top, there are settings for 'Content Filtering: ON', 'Approved Senders: OFF', 'Quarantine Administrator: wfintstone@arc.in.dev1.postini-corp.com', and 'Bounce Message: ERROR 582: This message violates our email policy.' Below this is a progress bar indicating 'You are currently using 32% of your allowed filter space'. A table lists three filters with columns for Filter Name, Status, Description, Routing, Copy to Quarantine, and % of Total. The 'Update Priority List' link and the filter table are circled in red.

Filter Name	Status	Description	Routing	Copy to Quarantine	% of Total
1 Social Security Numbers	ON	Compliance Policy: Protects social security numbers	Deliver	Quarantine Administrator	
2 Credit Card Numbers	OFF	Compliance Policy: Protects credit card numbers	Deliver	Quarantine Administrator	
3 Filter 1	OFF	Entire Message does not match regex "ab" OR...	Delete (Blackhole)	Quarantine Administrator, cmburns@arc.in.dev1.postini-corp.com, Recipient (+2)	

2. Click **Save Priority List**.

Delete and Disable Content Filters

If you want to stop using a content filter or compliance policy, you can do any of the following:

- Delete a specific custom content filter that you created
- Temporarily disable a specific compliance policy that you set up
- Temporarily disable all custom content filters and compliance policies at once

Tip:

- If you disable filters and policies, their configurations are saved, so you can use them again at any time.
- After you delete or disable a content filter or policy, you can apply your changes to all suborganizations. For details, see “Configure Content Manager” on page 338.

To delete a content filter:

1. Go to the Content Manager filter-list page for the organization that contains the filter you want to delete. For details, see “View Content Manager Filters and Policies” on page 337.
2. Click the filter name.
3. Click **Delete**.

To disable compliance policies only:

1. Go to the Content Manager filter-list page for the organization that contains the compliance policy you want to disable. For details, see “View Content Manager Filters and Policies” on page 337.
2. Click the policy name.
3. Under **Filter Status**, select **OFF**.
4. Click **Save**.

To disable all content filters and policies at once:

1. Go to the Content Manager Edit Settings page for the organization for which you want to disable content filters. For details, see “Configure Content Manager” on page 338.
2. Under **Content Filtering**, select **OFF**.
3. Click **Save**.

Note: On the filter-list page, the settings in the **Status** column for individual compliance policies does not change. However, all policies are disabled.

About Using Regular Expressions

Content Manager includes a powerful string-matching tool called *regular expressions*, often abbreviated as *regex*. With regular expressions, you can create filters that can match patterns of text rather than only single words or phrases.

Regular expressions are a standard tool in many systems and scripting languages. Regular expressions can be simple or highly complex. This document provides information about how to use regular expressions with Content Manager, and can help you create simple expressions. You can find more detailed information—including tutorials and examples—on many web sites, such as the following:

- www.regular-expressions.info
- www.regexlib.com

Uses for Regular Expressions

Using regular expressions, you can create content filters that can find:

- **Text patterns**

Use this option to scan messages for patterns of letters, numbers, or a combination of both. For example, you can create regular expressions that match phone numbers, addresses, employee numbers, and account numbers. Or, you can create one regular expression that can find many different variations of a word, such as `viagra`, `vi@gra`, `vlagr@`, and so on.

- **Lists of words**

Use this option to scan messages for specific categories of words, such as profanity, financial terms, and legal terms.

- **Complete words**

Use this option to create more specific filters. For example, you can create a regular expression that matches the word `foot` but not `football`. In this case, a regular expression can help to reduce the number of legitimate messages that the filter captures.

- **Text with variable characters**

Use this option to scan messages for patterns that contain specific text along with text that varies. For example, you can create a single regular expression that matches a URL in the pattern `www.[variable].com`, such as `www.abc1.com`, `www.abc2.com`, and `www.abc3.com`.

Regular Expressions Syntax

To create a regular expression, you must use specific syntax—that is, special characters and construction rules. For example, the following is a simple regular expression that matches any 10-digit telephone number, in the pattern `nnn-nnn-nnnn`:

```
\d{3}-\d{3}-\d{4}
```

Note: Content Manager supports only POSIX ERE syntax and equivalent shorthand characters. For more information, see “Content Manager Support for Regular Expressions” on page 355.

The following table describes some of the most common special characters for use in regular expressions. These characters are categorized as follows:

Character	Description
Anchors	
^	<p>(caret) Matches the start of the line or string of text that the regular expression is searching. For example, a content rule with a location Subject line and the following regular expression:</p> <p><code>^abc</code></p> <p>captures any email message that has a subject line beginning with the letters abc.</p>
\$	<p>(dollar) Matches the end of the line or string of text that the regular expression is searching. For example, a content rule with a location Subject line and the following regular expression:</p> <p><code>xyz\$</code></p> <p>captures any email message that has a subject line ending with the letters xyz.</p>
Metacharacters	
.	<p>(dot) Matches any single character, except a new line.</p>
 	<p>(pipe) Indicates alternation—that is, an “or.” For example:</p> <p><code>cat dog</code> matches the word cat or dog</p>
\	<p>Indicates that the next character is a literal rather than a special character. For example:</p> <p><code>\.</code> matches a literal period, rather than any character (dot character)</p>
Character Classes	
[...]	<p>Matches any character from a set of characters. Separate the first and last character in a set with a dash. For example:</p> <p><code>[123]</code> matches the digit 1, 2, or 3</p> <p><code>[a-f]</code> matches any letter from a to f</p> <p>Note: Regular expressions in Content Manager are <i>not</i> case sensitive. Therefore, using this formatting to specify a character set in lowercase letters also includes the equivalent uppercase letters.</p>

Character	Description
[^...]	<p>Matches any character <i>not</i> in the set of characters. For example:</p> <p><code>[^a-f]</code> matches any character that's <i>not</i> a letter from a to f</p> <p>Note: Regular expressions in Content Manager are <i>not</i> case sensitive. Therefore, using this formatting to specify a character set in lowercase letters also excludes the equivalent uppercase letters.</p>
[:alnum:]	<p>Matches alphanumeric characters (letters or digits):</p> <p>a-z, A-Z, or 0-9</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[:alnum:]</code>.</p>
[:alpha:]	<p>Matches alphabetic characters (letters):</p> <p>a-z or A-Z</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[:alpha:]</code>.</p>
[:digit:]	<p>Matches digits:</p> <p>0-9</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[:digit:]</code>.</p>
[:graph:]	<p>Matches visible characters only—that is, any characters except spaces, control characters, and so on.</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[:graph:]</code>.</p>
[:punct:]	<p>Matches punctuation characters and symbols:</p> <p>! " # \$ % & ' () * + , \ - . / : ; < = > ? @ [] ^ _ ` { }</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[:punct:]</code>.</p>
[:print:]	<p>Matches visible characters and spaces.</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[:print:]</code>.</p>

Character	Description
[:space:]	<p>Matches all whitespace characters, including spaces, tabs, and line breaks.</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[[:space:]]</code>.</p>
[:word:]	<p>Matches any word character—that is, any letter, digit, or underscore:</p> <p>a-z, A-Z, 0-9, or _</p> <p>Note: This character class must be surrounded with another set of square brackets when you use it in a regular expression, for example: <code>[[:word:]]</code>.</p>
Shorthand Character Classes	
\w	<p>Matches any word character—that is, any letter, digit, or underscore:</p> <p>a-z, A-Z, 0-9, or _</p> <p>Equivalent to <code>[[:word:]]</code></p>
\W	<p>Matches any non-word character—that is, any character that's <i>not</i> a letter, digit, or underscore.</p> <p>Equivalent to <code>[^[:word:]]</code></p>
\s	<p>Matches any whitespace character. For example, use this character to specify a space between words in a phrase:</p> <p><code>stock\s tips</code> matches the phrase stock tips</p> <p>Equivalent to <code>[[:space:]]</code></p>
\S	<p>Matches any character that's not a whitespace.</p> <p>Equivalent to <code>[^[:space:]]</code></p>
\d	<p>Matches any digit from 0-9.</p> <p>Equivalent to <code>[[:digit:]]</code></p>
\D	<p>Matches any character that's <i>not</i> a digit from 0-9.</p> <p>Equivalent to <code>[^[:digit:]]</code></p>

Character	Description
Group	
(...)	<p>Groups parts of an expression. Use grouping to apply a quantifier to a group or to match a character class before or after a group. For example, in the following expression:</p> <pre>\W(dog cat mouse)\W</pre> <p>the <code>\w</code> character class applies before and after each word in the group. The expression would match things like dog+cat or *dog*.</p>
Quantifiers	
{n}	<p>Match the preceding expression exactly <i>n</i> times. For example:</p> <pre>[a-c]{2}</pre> <p>matches any letter from a to c only if two letters occur in a row. Thus, the expression would match ab and ac but not abc or aabbc.</p>
{n,m}	<p>Match the preceding expression a minimum of <i>n</i> times and a maximum of <i>m</i> times. For example:</p> <pre>[a-c]{2,4}</pre> <p>matches any letter from a to c only if the letters occur a minimum of 2 times and a maximum of 4 times in a row. Thus, the expression would match ab and abc but not aabbc.</p>
?	<p>Indicates that the preceding character or expression can match 0 or 1 times. Equivalent to the range <code>{0,1}</code>. For example, the following regular expression:</p> <pre>colou?r</pre> <p>matches either colour or color, because the <code>?</code> makes the letter u optional.</p>

Content Manager Support for Regular Expressions

Content Manager provides robust support for regular expressions. However, because Content Manager filters large volumes of email messages, it does not support all regular-expressions syntax standards or features.

Regex Syntax Support

There are many variations of regular-expressions syntax and features. Content Manager supports only the *POSIX Extended Regular Expressions (ERE)* standard and shorthand notation for some character classes. It doesn't support other standards, such as Perl or .NET regular expressions.

Case Sensitivity in Regular Expressions

Content Manager ignores case for letters and character sets in regular expressions, so you need not specify both lowercase and uppercase letters in your expressions. For example, if your regular expression includes the character set `[a-z]`, it matches any lowercase character from **a** to **z** and any uppercase character from **A** to **Z**.

Similarly, if you include literal characters or words in your regular expression, the expression matches both lowercase and uppercase letters, regardless of the case you use. For example, if your expression includes the literal text `viagra`, it matches **VIAGRA**, **Viagra**, **ViAgrA**, and so on.

Complexity (Component) Limitations

To ensure that content filters with regular expressions do not cause processing delays for your email, Content Manager limits the complexity of regular expressions. A regular expression can have up to 100 *components*. Content Manager considers each special character, character set, and string of literal characters as a separate component. For example, the regex `\wc[i|!]alis\w` contains the following 9 components: **\W** , **c** , **[** , **i** , **|** , **!** , **]** , **alis** , **\W**

Regex Character Limitations

Content Manager does not support regular expressions with the following special characters, because they could cause delays in processing your email:

- * (asterisk): Matches 0 or more occurrences of the preceding item
- + (plus sign): Matches 1 or more occurrences of the preceding item

Range Limitations:

Content Manager does not support the following types of ranges, because they could cause delays in processing your email:

- **Ranges more than {0,25}**
 - A valid range: `(a|b|c){0,10}`
 - An invalid range: `(a|b|c){0,26}`
 - An invalid range (equivalent to a *): `(a|b|c){1,}`
- **Nested ranges**
 - A valid range: `(a|b|c){5,10}`
 - An invalid range: `((a|b|c){0,5}){5,20}`
 - An invalid range: `((a|b|c){0,5})?`

Examples of Regular Expressions

The following examples illustrate the use and construction of simple regular expressions. Each example includes the type of text to match, one or more regular expressions that match that text, and notes that explain the use of the special characters and formatting.

Important: If you create your own regular expression, use the built-in regex tester to verify that your expression will catch the text you expect and that you haven't created an overly general expression.

Match Whole Word Only

Usage example	Match the word hell . Don't match the word hello , shell , shellac , and so on.
Regex example	<code>(\W ^)hell(\W \$)</code>
Note	<ul style="list-style-type: none">• <code>\W</code> matches any character that's not a letter, digit, or underscore. It prevents the regex from matching letters before or after the word. <p>Important: When creating a regex to match whole words, ensure that you include the <code>\W</code> character class, to help to avoid capturing legitimate messages.</p> <ul style="list-style-type: none">• <code>^</code> matches the start of a new line. Allows the regex to match the word if it appears at the beginning of a line, with no characters before it.• <code>\$</code> matches the end of a line. Allows the regex to match the word if it appears at the the end of a line, with no characters after it.

Note: You can also use the rule filter "matches any word in" to create a rule that matches a specific word. Include the word you want to match in the rule value.

Match Exact Phrase Only

Usage example	Match the phrase stock tips .
Regex examples	<p>1: <code>(\W ^)stock\tips(\W \$)</code></p> <p>2: <code>(\W ^)stock\s{0,3}tips(\W \$)</code></p> <p>3: <code>(\W ^)stock\s{0,3}tip(s){0,1}(\W \$)</code></p>

Notes

- `\w` matches any character that's not a letter, digit, or underscore. It prevents the regex from matching characters before or after the phrase.
- In example 2, `\s` matches a space character, and `{0,3}` indicates that from 0 to 3 spaces can occur between the words **stock** and **tip**.
- `^` matches the start of a new line. Allows the regex to match the phrase if it appears at the beginning of a line, with no characters before it.
- `$` matches the end of a line. Allows the regex to match the phrase if it appears at the the end of a line, with no characters after it.
- In example 3, `(s)` matches the letter **s**, and `{0,1}` indicates that the letter can occur 0 or 1 times after the word **tip**. Therefore, the regex matches **stock tip** and **stock tips**. Alternatively, you can use the character `?` instead of `{0,1}`.

Match Word or Phrase in a List

Usage example	Match any word or phrase in the following list: <ul style="list-style-type: none">• baloney• darn• drat• foeey• gosh darnit• heck
Regex example	<code>(\W ^)(baloney darn drat foeey gosh\darnit heck)(\W \$)</code>
Notes	<ul style="list-style-type: none">• <code>(...)</code> groups all the words, such that the <code>\w</code> character class applies to all of the words within the parenthesis.• <code>\w</code> matches any character that's not a letter, digit, or underscore. It prevents the regex from matching characters before or after the words or phrases in the list.• <code>^</code> matches the start of a new line. Allows the regex to match the word if it appears at the beginning of a line, with no characters before it.• <code>\$</code> matches the end of a line. Allows the regex to match the word if it appears at the the end of a line, with no characters after it• <code> </code> indicates an "or," so the regex matches any one of the words in the list.• <code>\s</code> matches a space character. Use this character to separate words in a phrase.

Note: You can also use the rule filter "matches any word in" to create a rule that matches specific words. The rule filter "matches any word" does not, however, match phrases. Include the words you want to match in the rule value.

Match Word with Different Spellings or Special Characters

Usage example	Match the word viagra and some of the obfuscations that spammers use, such as: <ul style="list-style-type: none">• vi@gra• v1agra• v1@gra• v!@gr@
Regex example	<code>v[i!1][a@]gr[a@]</code>
Notes	<ul style="list-style-type: none">• <code>\w</code> is not included, so that other characters can appear before or after any of the variants of viagra. For example, the regex still matches viagra in the following text: viagra!! or ***viagra***• <code>[i!1]</code> matches the characters i, !, or 1 in the second character position of the word.

Tip: For information about using regular expressions to match obfuscations for profane words, see “Block Messages with Profanity” on page 367.

Match Word with Variable Characters

Usage example	Match any URL that contains the text badmail.com , such as: <ul style="list-style-type: none">• badmail1.com• badmail12.com• badmail3.com• badmail.junk.com• badmail-junk.com
Regex example	<code>badmail(\w.+%\-){0,25}\.com</code>

Notes

- `[\w.+ \-]` matches any word character (a-z, A-Z, 0-9, or an underscore), a period, a plus sign, a percent sign, or a hyphen. These are the only valid characters in a URL. Note that the `\-` (which indicates a hyphen) must occur *last* in the list of characters within the square brackets.
- `{0,25}` indicates that from 0 to 25 characters in the preceding character set can occur after the text **badmail**. Content Manager supports matching of up to 25 characters for each character set in a regular expression.
- The `\` before the dash and period “escapes” these characters—that is, it indicates that the dash and period are *not* a regex special characters themselves. Note that there is no need to escape the period within the square brackets.

Match Any Email Address from a Specific Domain

Usage example Match any email address from the domains **yahoo.com**, **hotmail.com**, and **gmail.com**.

Regex example `(\W|^)[\w.+ \-]{0,25}@(yahoo|hotmail|gmail)
\.com(\W|$)`

Notes	<ul style="list-style-type: none"> • <code>\w</code> matches any character that's not a letter, digit, or underscore. It prevents the regex from matching characters before or after the email address. • <code>^</code> matches the start of a new line. Allows the regex to match the address if it appears at the beginning of a line, with no characters before it. • <code>\$</code> matches the end of a line. Allows the regex to match the address if it appears at the the end of a line, with no characters after it. • <code>[\w.\-]</code> matches any word character (a-z, A-Z, 0-9, or an underscore), a period, a plus sign, or a hyphen. These are the most commonly used valid characters in the first part of an email address. Note that the <code>\-</code> (which indicates a hyphen) must occur <i>last</i> in the list of characters within the square brackets. • The <code>\</code> before the dash and period “escapes” these characters—that is, it indicates that the dash and period are <i>not</i> a regex special characters themselves. Note that there is no need to escape the period within the square brackets. • <code>{0,25}</code> indicates that from 0 to 25 characters in the preceding character set can occur before the <code>@</code> symbol. Content Manager supports matching of up to 25 characters for each character set in a regular expression. • The <code>(...)</code> formatting groups the domains, and the <code> </code> character that separates them indicates an “or.”
--------------	---

Match Any IP Address in a Range

Usage example	Match any IP address within the range 192.168.1.0 to 192.168.1.255 .
Regex examples	<p>1: <code>192\..168\.1\.</code></p> <p>2: <code>192\..168\.1\.\d{1,3}</code></p>

Notes	<ul style="list-style-type: none"> • The <code>\</code> before each period “escapes” the period—that is, it indicates that the period is <i>not</i> a regex special character itself. • In the example 1, no characters follow the last period, so the regex matches any IP address beginning with 192.168.1., regardless of the number that follows. • In example 2, <code>\d</code> matches any digit from 0 to 9 after the last period, and <code>{1,3}</code> indicates that the from 1 to 3 digits can appear after that last period. In this case, the regex matches any complete IP address beginning with 192.168.1.. Note that this regex also matches invalid IP addresses, such as 192.168.1.999.
--------------	--

Match an Alphanumeric Format

Usage example	<p>Match the purchase order numbers for your company. This number has various possible formats, such as:</p> <ul style="list-style-type: none"> • PO nn-nnnnn • PO-nn-nnnn • PO# nn nnnn • PO#nn-nnnn • PO nnnnnn
Regex example	<code>(\W ^)po[#\-]{0,1}\s{0,1}\d{2}[\s-]{0,1}\d{4}(\W \$)</code>
Notes	<ul style="list-style-type: none"> • <code>\W</code> matches any character that’s not a letter, digit, or underscore. It prevents the regex from matching characters before or after the number. • <code>^</code> matches the start of a new line. Allows the regex to match the number if it appears at the beginning of a line, with no characters before it. • <code>\$</code> matches the end of a line. Allows the regex to match the number if it appears at the the end of a line, with no characters after it. • <code>[#\ -]</code> matches a pound sign or a hyphen after the letters po, and <code>{0,1}</code> indicates that one of those characters can occur zero or one times. Note that the <code>\ -</code> (which indicates a hyphen) must occur <i>last</i> in the list of characters within the square brackets. • <code>\s</code> matches a space, and <code>{0,1}</code> indicates that a space can occur zero or one times. • <code>\d</code> matches any digit from 0 to 9, and <code>{2}</code> indicates that exactly 2 digits must appear in this position in the number.

How to Use Content Manager in a Spam Outbreak

On rare occasions, malicious senders create new junk messages that don't have any text or patterns in common with previous junk messages. During a large-scale spam outbreak, a few of these messages may initially pass through the spam filters. During such outbreaks, your message security service immediately begins collecting data to update spam filters. Once updated, the filters begin blocking the spam messages. Therefore, you do not need to take any action or change your message security service configuration.

However, if your users are repeatedly receiving a specific type of junk message, you can block those messages by creating a content filter in Content Manager. For this filter, you can specify unique text that the junk messages contain. Or you can use a regular expression to specify a unique text *pattern* in the messages, rather than specific text. For more information about regular expressions, see "About Using Regular Expressions" on page 349.

Important: When using content filters to block spam, it is recommended that you do the following:

- **Analyze headers first:** To verify that a content filter can help block spam messages, analyze the headers to determine why the messages passed through the spam filters. Headers, for example, can tell you whether the recipient address is for an account on your message security service, or whether the sender is on your Approved Senders list. To analyze headers, use the Header Analyzer, which is available at <http://www.google.com/postini/headeranalyzer>.
- **Use content filters for spam carefully.** The use of content filters to block spam may increase the number of legitimate messages that are quarantined, so use these types of filters with caution.
- **Use content filters for spam temporarily.** The message security service continuously updates the spam filters, so it usually starts blocking new types of spam quickly. Also, the longer a content filter remains active, the more likely it will capture legitimate messages.
- **Watch for evolving spam:** New types of spam can change rapidly, so any content filter you create for spam may be effective for only a short period. For example, malicious senders might create similar messages that your content filters won't block.

To create a temporary content filter for new spam:

1. Review the junk messages to find unique text. This text must be specific to these messages and not likely to occur in legitimate messages.

Tip: Instead of looking for exact text, you can look for a unique text pattern in the junk messages. You can then use this pattern to create a regular expression. See “About Using Regular Expressions” on page 349.

2. Create a filter:
 - a. Specify a name that identifies the spam.
 - b. Set the rule location to **Body** and the filter type to **contains**.
 - c. Set the rule value to the unique text of the email. Or create a regular expression to scan messages for a unique pattern of characters.
3. Set **Copy to Quarantine to Recipient**. This disposition sends any captured messages to Junk Quarantines in your users’ Message Centers.
4. Save the filter to begin quarantining messages that contain the unique text or pattern.
5. Tell your users to check their quarantines more frequently for any legitimate messages that contain a match for the new content filter.

Content Manager Tips and Best Practices

Use Regular Expressions Whenever Possible

When you create a filter rule, you can choose among several filter types—that is, how the filter looks for the content you enter. Typically, the most effective filter type is **matches regex**, even for simple filters that look for only single words.

For example, you can use the **matches regex** option to find only the word `hell` and not other words that contain the characters in the word `hell`, such as `hello` or `shell`. If you were to select the **contains** filter type, the filter would catch message with the words `hello` or `shell`.

For an example of a regex that matches a whole word, see “Match Whole Word Only” on page 357.

Use Multiple Regular Expressions for a Filter

You can enter up to three regular expressions for a filter—one expression per filter rule. You might want to enter multiple regular expressions for the following reasons:

- **To avoid the regex complexity or word list limitation**

If your regular expression exceeds the component (complexity) limitation for a rule, you can enter two or three shorter expressions. For example, if your expression for a word list contains more than 48 words, you can enter two or three shorter lists, for a total of up to 144 words.

For details about components in regular expressions, see “Content Manager Support for Regular Expressions” on page 355.

- **To increase the filter’s effectiveness**

Often, you can increase the number of patterns a filter matches by creating multiple regular expressions. For example, to match obfuscations for the word **viagra**, you can create up to three different regular expressions for the filter, each of which matches different types of obfuscations, as shown in the following table:

This regular expression...	Matches these types of obfuscations...
<code>v[!1][a@][g9]r[a@]</code>	<ul style="list-style-type: none"> • vi@gra • v1agra • v1@gra • via9ra
<code>v[\W_]{1,3}i[\W_]{1,3}a[\W_]{1,3}g[\W_]{1,3}r[\W_]{1,3}a{1,3}</code>	<ul style="list-style-type: none"> • v**i**a**g**r**a • v_i_a_g_r_a • v~i~a~g~r~a • v/i/a/g/r/a • v i a g r a
<code>\\v{1,5}i{1,5}a{1,5}g{1,5}r{0,5}a{0,5}</code>	<ul style="list-style-type: none"> • Viagra • Viiaggrraa • vviiiaggrraaa • viag

Note: Alternatively, you can often create a single, more complex expression that matches many word obfuscations. But creating multiple, simpler expressions is usually easier, and helps you to avoid the complexity limitation for a rule.

Block Messages with Profanity

To prevent users from sending or receiving email messages with profane words, you can create content filters with regular expressions. If you want to catch only specific profane words, you can enter them in a regular expression word list. For an example, see “Match Word or Phrase in a List” on page 359.

On the other hand, if you want to catch many of the common variations, or obfuscations, of profane words, it's best to create a separate regular expression for each word.

For examples of regular expressions for common profane words, please view this topic in online Help version on this guide.

Allow Approved Senders to Bypass Content Filters

Depending on your compliance policies, consider allowing your Approved Senders to bypass Content Manager filters. An Approved Senders list is an organization-level feature that lets messages from senders on the list bypass the Junk Filters. For details, see “Approved and Blocked Sender Lists” on page 387.

To allow messages from senders on your Approved Senders list to bypass content filters, go to the Content Manager Edit Settings page, and select **Allow email from Approved Senders to bypass the Content Manager filters**. For details, see “Configure Content Manager” on page 338.

Create a Custom Filter to Restrict Outgoing Messages to a Specific Domain

If you need to restrict some users to sending messages to a particular domain (for example, to sending messages only within your company domain), follow these steps:

1. Create a separate org for those users for whom you want to restrict outgoing messages, and add all the relevant users to that org.
2. Under Outbound Services for that org, open Content Manager.

3. Add a new custom filter with the following properties:
 - **Filter Status:** ON
 - **Rules:**
 - Match:** Any Rule
 - Select Location:** Recipient
 - Select Filter Type:** does not contain
 - Filter Value:** @<your domain>
 - **Routing:** Bounce
 - **Copy to Quarantine:** Optionally, specify a quarantine to which messages are copied

With this filter in place, any outgoing messages from the new user org that are not addressed to your domain are bounced, and optionally quarantined.

Create Filters to Allow Valid Null-Sender Messages

Note: For information about how to create a custom filter in the Content Manager interface, see “Create or Edit a Content Manager Filter” on page 340.

The Null Sender Disposition spam filter (see “Types of Spam Filters” on page 295) is designed to stop messages like spam-related NDRs that do not include an SMTP-envelope sender address. While you may want to eliminate the bulk of those types of messages, there are some null-sender messages that are valid and that you want to be able to deliver, for example, voicemail messages and out-of-office or vacation responses. You can use Content Manager in combination with the Null Sender Disposition spam filter to block nuisance messages but still let valid message through by creating a pair of Content Manager filters that deliver null-sender messages with specific text in the subject line, but block other null-sender messages.

To create a custom filter that allows valid null-sender messages:

1. Under Rules, set Match to: All Rules.
2. Set the first rule in the filter to:
 - Select Location: Sender
 - Select Filter Type: is empty
3. Set the second rule in the filter to:
 - Select Location: Subject Line
 - Select Filter Type: matches regex
 - Value (text field): voicemail|vacation|out of office

Note: Enter whatever regex is appropriate for the type of messages you want to permit.
4. Set Routing to: Deliver, Bypass junk filters.

To create a custom filter that deletes other null-sender messages:

1. Under Rules, set Match to: Any Rule.
2. Set the first rule in the filter to:
 - Select Location: Sender
 - Select Filter Type: is empty
3. Set Routing to: Delete (Blackhole).
4. If you want to copy the deleted messages to one or more quarantines, you can set Copy to Quarantine to the appropriate value.

To set priority for the two null-sender filters:

In order for these filters to work together properly, you need to give the first rule (allow valid null-sender messages) priority over the second rule (delete other null-sender messages).

For instructions on setting filter priority, see “Reorder Content Filters and Policies” on page 347.

Test Content Filters First

Before actually deploying a new content filter, you can test its effectiveness first. Testing your filters first can also help you to prevent deploying filters that capture too many legitimate messages.

To test a content filter:

1. When creating the filter, select a message disposition of either **BCC-Quarantine** or **Log and Deliver**. Neither of these dispositions prevent messages from being delivered.
2. After a period of time, create a Filter Name report to determine how many messages the filter captured. For example, you can determine the daily catch rate for your filter, by creating a new report each day.

For details about the Filter Name report, see “Filter Name (Inbound, Outbound)” on page 575.

Troubleshoot Content Manager

I created a content filter rule with a full file name for the value and a location of Entire Message. However, the filter didn't capture a message that contained an attachment with that file name. Why?

Content Manager does not scan the file name of attached files. Some email programs include the names of attached files in the headers. If the file name does not appear there, Content Manager won't capture the message.

A content filter captured messages that don't contain any words, phrases, or patterns I specified in the filter rules. Why?

If the message contains a file attachment, the value you specified in the filter rule might appear in the attachment. If you selected **Body** for the filter's rule location, Content Manager still scans any plain-text attachments, including attached email messages. If you selected the location **Entire Message**, Content Manager also scans binary attachments, such as Microsoft Office files.

If you can't find the value in the attachment, check the source code of the email message itself. If the message includes a binary attachment (such as a Microsoft Office file), Content Manager scans the MIME encoded sections of the message for those attachments. These sections appear as long, random strings of characters without spaces in the message source. To prevent Content Manager from matching words in the MIME encoded sections, use a regular expression to match entire (whole) words only. For details, see "Match Whole Word Only" on page 357.

I created a content filter to find specific words, but messages with those words in file attachments are getting through. Why?

If a message contains a binary attachment, such as a Microsoft Office file, Content Manager does not scan the text content of that attachment unless you select **Entire Message** for the rule location.

Content Manager Reference

Content Manager Filter List

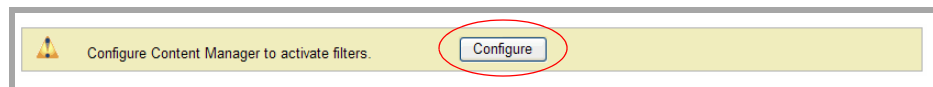
Use this page to view Content Manager settings and filters, or to access other pages on which you can:

- Configure Content Manager
- Set up compliance policies
- Create or edit content filters

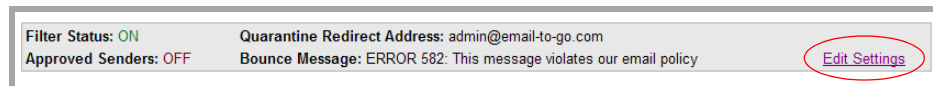
See “About Content Manager” on page 329.

Configure Content Manager:

If you have not yet configured Content Manager, a **Configure** button appears. Click the button to configure Content Manager settings:



If you already set up Content Manager, click **Edit Settings**:



See “Content Manager Configuration Settings” on page 372.

Set Up a Content Compliance Policy:

Use compliance policies to protect personal information in email messages. Click a policy name to set it up:

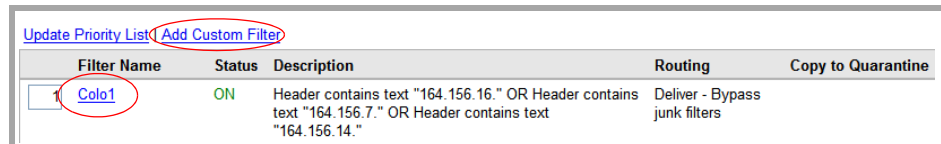
	Filter Name	Status	Description	Routing	Copy to Quarantine
<input type="checkbox"/>	1 Social Security Numbers	ON	Compliance Policy: Protects social security numbers	Deliver	Quarantine Administrator

See:

- “Social Security Numbers Policy” on page 381
- “Credit Card Numbers Policy” on page 383

Create or Edit a Content Filter:

Create content filters to block or monitor messages with specific content. To create a new content filter, click **Add Custom Filter**. To edit an existing filter, click the filter name:



Update Priority List Add Custom Filter				
Filter Name	Status	Description	Routing	Copy to Quarantine
<input type="checkbox"/> Colo1	ON	Header contains text "164.156.16." OR Header contains text "164.156.7." OR Header contains text "164.156.14."	Deliver - Bypass junk filters	

See “Content Manager Filter Settings” on page 374.

Content Manager Configuration Settings

Use this setting...	To...
Content Filtering	<p>Turn Content filtering ON or OFF.</p> <p>ON: Compliance policies and any configured filters are active.</p> <p>OFF: Compliance policies and any configured filters are inactive.</p> <p>Important: By default, Content filtering is on or off for only the organization from which you made access. To turn it on or off for the suborganization below, select the Apply settings and filter definitions to existing suborgs check box. We recommend that you configure company-wide settings in a top-level organization, and propagate them to suborgs in your organization hierarchy.</p>

Use this setting...	To...
<p>Quarantine Administrator</p>	<p>Specify the email address of the administrator who receives messages captured by a filter for which you have configured the Copy to Quarantine option. Content Manager sends messages that the filter captures to the administrator's quarantine in Message Center. If all administrators share one account (for example, admin@jumboinc.com), enter the email address for that account here.</p> <p>Note:</p> <ul style="list-style-type: none"> Any message limits set for the organization or user account apply. See "Set an Organization's Message Limits" on page 93. The account cannot be deleted. <p>For Outbound Content Manager:</p> <ul style="list-style-type: none"> The administrator's quarantine does not indicate whether a message was outbound or inbound. If you want to distinguish between them, consider adding another administrator account to which to redirect only outbound messages.
<p>Approved Senders</p> <p><i>Inbound Content Manager only</i></p>	<p>Specify whether to allow messages from senders on the Approved Senders list to bypass the content filters.</p> <p>The Approved Senders list is an organization-level feature that you use to specify the addresses of senders whose messages bypass the spam filters. For details, see "Approved and Blocked Sender Lists" on page 387.</p>
<p>Bounce Message</p>	<p>Specify a custom message that senders receive if their messages are captured by a content filter with the disposition of Bounce.</p> <p>You can specify a message of up to 100 ASCII characters.</p>
<p>Apply settings to existing sub-orgs</p>	<p>Apply Content Manager settings to all suborganizations in your hierarchy below the current organization. Use this option to avoid having to configure Content Manager with the same settings in multiple suborgs.</p> <p>Note: After you apply settings to suborgs:</p> <ul style="list-style-type: none"> You can still change the settings for any suborg at any time. Additional changes you make to the settings in this org are <i>not</i> automatically applied to suborgs. To apply new changes to suborgs, select this option again, and then click Save. <p>WARNING: This setting overwrites any existing configuration settings and content filters in the suborgs.</p>

Content Manager Filter Settings

Use this page to:

- Create a new content filter, or edit an existing filter.
- Delete a content filter.

Alternatively, you can temporarily disable all content filters for an organization, by turning off Content Manager. See “Configure Content Manager” on page 338.

General Filter Settings

Use this field...	To...
Filter Name	Enter a descriptive name for the filter. The name must be unique and cannot exceed 15 characters.
Filter Status	Select ON or OFF to turn the filter on or off.

Filter Rules

Use this field...	To...
Match	<p>Specify how the filter applies your rules to messages:</p> <ul style="list-style-type: none">• Any Rule: Content Manager executes the selected disposition on a message if it contains a match for <i>at least one</i> of the three rules in this filter. Important: This option usually captures more messages, so use it with caution.• All Rules: Content Manager executes the selected disposition on a message if it contains matches for <i>all</i> the rules in this filter.

Use this field...	To...
Select Location	<p>Select the part of the message you want Content Manager to scan:</p> <ul style="list-style-type: none"> • Subject Line: Scans the Subject field in a message. • Body: Scans the body text in a message. Does not scan file attachments, except plain-text files. • Header: Scans the complete SMTP headers of a message, including subpart headers. • Sender: Scans the From field in a message. • Recipient: Scans the To field in a message. • Entire Message: Scans the body, headers, sender, recipient, and subject. It also scans text-based file attachments, such as Microsoft Office documents. For more information about which types of attachments are scanned and size limits, see “Attachments That Content Manager Scans” on page 335.

Use this field...	To...
Select Filter Type	<p>Select the scanning method that Content Manager uses for this filter.</p> <ul style="list-style-type: none"> • starts with: If text in the specified location begins with the specified value, this filter captures the message. • ends with: If text in the specified location ends with the specified value, this filter captures the message. • contains text: If text in the specified rule location contains the specified rule value, this filter captures the message. This option matches whole words and parts of words. For example, if you specify the value <i>foot</i>, and a message contains the word <i>foot</i>, <i>footlocker</i>, or <i>football</i> in the specified location, this filter captures the message. To capture messages with the word <i>foot</i>, without also capturing messages with the word <i>football</i>, you can use the matches regex or matches any word in option. • does not contain: If text in the specified location does <i>not</i> contain the specified value, this filter captures the message. • equals: If text in the specified location contains <i>only</i> the specified value, this filter captures the message. For example, if the value is <i>storewide holiday bargains</i> and the location is Subject Line, this filter captures the message only if the subject contains the text <i>storewide holiday bargains</i>, and no other text. • is empty: If there is no text in the specified location, this filter captures the message. Use, for example, to check for messages that have an empty sender. See “Create Filters to Allow Valid Null-Sender Messages” on page 368. • matches regex: If text in the specified location matches the regular expression you enter for the rule value, this filter captures the message. For more information, see “About Using Regular Expressions” on page 349. When you select this filter type, the Test regex link appears. Click this link to open the Test Regular Expression panel, where you can make sure your expression syntax is valid, and catches the type of content you want. For more information, see “Test Regular Expression” on page 380.

Use this field...	To...
<p>Select Filter Type (cont)</p>	<ul style="list-style-type: none"> <p>does not match regex: If the text in the specified location does not match the regular expression you enter for the rule value, this filter captures the message.</p> <p>When you select this filter type, the Test regex link appears. Click this link to open the Test Regular Expression panel, where you can make sure your expression syntax is valid, and catches the type of content you want. For more information, see “Test Regular Expression” on page 380.</p> <p>matches any word in: If the text in the specified location matches any word you enter in the rule value, this filter captures the message.</p> <p>When you enter a corresponding value for this rule, separate words with spaces, for example:</p> <p>one two three</p> <p>Use this filter when you want to match only whole words. For example, if you want to match <i>foot</i> and not also <i>football</i>, then use this filter with a value of foot.</p> <p>This filter matches only individual words and not phrases. To filter for phrases, use the regex filters.</p>

Use this field...	To...
Value	<p data-bbox="727 201 1403 264">Enter the content for which you want Content Manager to scan messages.</p> <p data-bbox="727 291 1414 384">If you selected a filter type of starts with, ends with, contains text, does not contain, equals, or matches any word in:</p> <ul data-bbox="727 415 1414 825" style="list-style-type: none"> <li data-bbox="727 415 1414 508">• The value must be a word or phrase. You can enter a regular expression only if you select a filter type of matches regex or does not match regex. <li data-bbox="727 531 1414 594">• Enter a space-separated list of ASCII characters (for example: one two three). <li data-bbox="727 617 1414 680">• The value is <i>not</i> case sensitive—that is, text in messages can match the value regardless of case. <li data-bbox="727 703 1414 825">• The number of characters you can enter is not strictly limited. However, there is a character limit for all filters in an organization combined. For details, see “Content Filter Limitations” on page 336. <p data-bbox="727 856 1414 919">If you selected a filter type of matches regex or does not match regex:</p> <ul data-bbox="727 951 1414 1194" style="list-style-type: none"> <li data-bbox="727 951 1414 1043">• The value can be a regular expression. Use regular expressions to scan messages for text patterns rather than specific words or phrases. <li data-bbox="727 1066 1414 1194">• For the special characters and construction rules you can use to create a regular expression, and examples of regular expressions, see “About Using Regular Expressions” on page 349.

Message Dispositions

Field	Value
Routing	<p>Deliver: Sends the message to the recipient's inbox, without further Content Manager processing.</p> <ul style="list-style-type: none">• Bypass junk filters (Inbound only): Sends the message to the recipient's inbox, without processing by the junk filters.• Encrypt (Outbound only): Encrypts the message, using Message Encryption. Message Encryption is an optional feature. For more information, refer to the <i>Encryption Services Administration Guide</i>. <p>Bounce: Returns the message to the sender, with a 582 error. Sender also receives the Bounce Message specified on the Content Manager Configuration Settings page. For details, see "Configure Content Manager" on page 338.</p> <p>Delete (Blackhole): Discards the message, with no notification to the sender or recipient.</p>

Field	Value
Copy to Quarantine	<p>Copies any message that matches the filter to the specified quarantine addresses:</p> <ul style="list-style-type: none"> • Quarantine Administrator • Recipient (Inbound) • Sender (Outbound) • Other User <p>To add/remove an address:</p> <ol style="list-style-type: none"> 1. Click Add quarantine address. 2. Select the quarantine. If you select Other User, enter that user's quarantine address. 3. To remove an address, click Remove. <p>Note:</p> <ul style="list-style-type: none"> • You can designate an administrator on the Content Manager Configuration Settings page. See "Configure Content Manager" on page 338. • The administrator does not receive notification when a message is placed in his or her quarantine. • In the quarantine, the message has the Block Reason of Content. • If the administrator delivers the quarantined message, the message security service sends it to the original intended recipient. • If you select the Other User option when you add a quarantine address and the user whose address you enter is subsequently deleted from the system, then messages are delivered to the recipient's quarantine.

Test Regular Expression

Field	Value
Regular Expression	<p>Enter the regular expression you want to test.</p> <p>Click Check Syntax to verify the syntax of your regular expression.</p> <p>For information about creating regular expressions, see "About Using Regular Expressions" on page 349.</p>

Field	Value
Text to Match	Enter text you want the regular expression to match. Click Test Match to see whether your regular expression matches the text you enter.
Result	If you are checking syntax, the message here tells you either: <ul style="list-style-type: none">• Your regular expression is valid.• The reasons your regular expression is not valid. If you are testing whether your expression matches text you enter, the message here tells you whether or not the expression matches the text.

Social Security Numbers Policy

Use the Social Security Numbers Policy page to:

- Turn the policy on or off.
- Select a disposition for messages captured by the policy's lexicon.

About the Social Security Numbers Lexicon

The Social Security Numbers lexicon is a predefined filter that finds U.S. social security numbers in email messages. The following table describes how the lexicon works:

Lexicon pattern matching	<p>This lexicon matches sequences of 9 digits. The digits in a valid sequence can be separated by spaces, dashes, or periods. The following are examples of the patterns this lexicon matches:</p> <ul style="list-style-type: none">• nnn-nn-nnnn• nnn nn nnnn• nnn.nn.nnnn• nnn-nn nnnn <p>The lexicon does not match different separators within the group of digits. The following are examples of patterns this lexicon does not match:</p> <ul style="list-style-type: none">• nnn-nn.nnnn• nnn.nn-nnnn <p>The lexicon does match a series of numbers followed by a period. The following are examples of patterns this lexicon does match:</p> <ul style="list-style-type: none">• nnn-nn-nnnn.• nnn.nn.nnnn. <p>The lexicon does not match a series of numbers preceded by a period. The following are examples of patterns this lexicon does not match:</p> <ul style="list-style-type: none">• .nnn-nn-nnnn• .nnn.nn.nnnn <p>The lexicon does not match a series of numbers followed by a dash (-). The following are examples of patterns this lexicon does not match:</p> <ul style="list-style-type: none">• nnn-nn-nnnn-• nnn.nn.nnnn- <p>The lexicon matches sequences of 9 digits that don't contain spaces or punctuation (in the pattern nnnnnnnn), if they occur within 4 words in the same message as the text <code>ssn</code> or <code>ss#</code> or <code>social security</code>.</p>
---------------------------------	---

Number validity checking	<p>This lexicon also checks sequences of 9 digits to determine whether they meet the requirements for a valid U.S. social security number, within the range that has been allocated. A valid social security number:</p> <ul style="list-style-type: none"> • Cannot contain a group of digits that are all 0s, such as in 000-11-1111, 111-00-1111, or 111-11-0000. • Cannot start with the digits 666, or any three-digit number greater than 728.
Filtering Accuracy	<p>The Social Security Numbers lexicon is designed to provide a high level of filtering accuracy to help reduce the risk of exposure of personal information. However, please note the following:</p> <ul style="list-style-type: none"> • Social security numbers can be represented or formatted in various ways; therefore, this lexicon may not capture all messages that contain social security numbers. • Because this lexicon looks for specific patterns of numbers, it may match numerical patterns that are not social security numbers.

Filter Status

Set this policy to **ON** or **OFF**. If you turn the policy off, the **Disposition** setting is saved.

Disposition

Select the action you want this policy to take on messages that the Social Security Numbers lexicon captures. For details about dispositions, see “Message Dispositions” on page 379.

Credit Card Numbers Policy

Use the Credit Card Numbers Policy page to:

- Turn the policy on or off.
- Select a disposition for messages captured by the policy’s lexicon.

About the Credit Card Numbers Lexicon

The Credit Card Numbers lexicon is a predefined filter that finds credit card numbers in email messages. The following table describes how this lexicon works:

Lexicon pattern matching	<p>This lexicon matches sequences of 16 digits. The digits in a valid sequence can be separated by spaces or dashes. The following are examples of the patterns that this lexicon matches:</p> <ul style="list-style-type: none">• nnnn-nnnn-nnnn-nnnn• nnnn nnnn nnnn nnnn• nnnn nnnn-nnnn nnnn• nnnnnnnnnnnnnnnnn
Number validity checking	<p>This lexicon also checks sequences of 16 digits to determine whether they meet the requirements for a valid credit card number. However, it does not determine whether a number is for a valid or active credit card account.</p> <p>To verify the validity of a credit card number, this lexicon uses the LUNH formula (a type of mathematical calculation) to determine whether the 16-digit sequence matches the requirements from the following card issuers:</p> <ul style="list-style-type: none">• Visa• Mastercard• Discover• JCB <p>Important: This lexicon does not match or verify the validity of credit card numbers that contain more or fewer than 16 digits, such as those issued by American Express or Diner's Club.</p>
Filtering Accuracy	<p>The Credit Card Numbers lexicon is designed to provide a high level of filtering accuracy, to help reduce the risk of exposure of personal information. However, please note the following:</p> <ul style="list-style-type: none">• Credit card numbers can be represented or formatted in various ways; therefore, this lexicon may not capture all messages that contain credit card numbers.• Because this lexicon looks for specific patterns of numbers, it may match numerical patterns that are not credit card numbers.

Filter Status

Set this policy to **ON** or **OFF**. If you turn the policy off, the **Disposition** setting is saved.

Disposition

Select the action you want this policy to take on messages that the Credit Card Numbers lexicon captures. For details about dispositions, see “Message Dispositions” on page 379.

Chapter 15

Approved and Blocked Sender Lists

About Sender Lists

You can approve or block specific senders and recipients, based on the email address or domain.

The message security service detects spam by applying hundreds of rules to each message that passes through. It blocks obvious spam outright, and diverts what is possibly spam to the Quarantine. If you discover that some quarantined messages are actually good mail that just look like spam, add the senders of those messages to an appropriate approved-senders list. If a number of quarantined senders are from the same domain, such as the same company, add the domain to an appropriate approved-senders list. Messages from those senders are then delivered to user's in your organization, regardless of the spam-like content.

To avoid the risk of increasing spam traffic, approve only specific senders whose messages might look like spam, rather than approving all of your known senders. Also, avoid approving too many domains, as that can increase the risk of spoofing. For more information see "Deciding Which Approved Senders to Add" on page 396".

Administrators configure sender lists at the org level and user level in the Administration Console.

Users configure their personal sender lists in the Message Center.

At the org level in the Administration Console you can configure:

- Approved Senders (individual email addresses and entire domains)
- Blocked Senders (individual email addresses and entire domains)

At the user level in the Administration Console, you can configure:

- Approved Senders (individual email addresses and entire domains)
- Blocked Senders (individual email addresses and entire domains)
- Approved Recipients (individual email addresses and entire domains)

At the user level in the Message Center, you can configure:

- Approved Senders (individual email addresses)
- Approved Domains (individual domains)
- Approved Mailing Lists/Email Lists (individual list addresses)
- Blocked Senders (individual email addresses)
- Blocked Domains (individual domains)

Approved Senders

Messages from individual senders or entire domains are delivered to user inboxes, regardless of spam-like content. Approved senders always circumvent junk email filters. However, if virus blocking is enabled for the recipient, the message security service does not deliver a message containing a virus, even if the sender is approved.

Approved senders can optionally override Attachment Manager and Content Manager filtering.

Approved Recipients

Messages sent to approved recipients or entire domains are delivered to user inboxes, regardless of spam-like content. Messages to approved recipients always circumvent junk-email filters. However, if virus blocking is enabled for the recipient, the message security service does not deliver a message containing a virus, even if the sender is approved.

Approved senders can optionally override Attachment Manager and Content Manager filtering.

You can use the approved-recipients list to allow mailing/email lists to bypass spam filters by enter the list address.

Many mailing/email-list and newsgroup emails contain characteristics in common with spam. In fact, one person's opt-in mailing/email list can be perceived by another person as spam.

If you find mailing/email-list or newsgroup postings quarantined in the Message Center, add the mailing/email-list address to the approved-recipients list to prevent those messages from being quarantined.

The approved-recipients list evaluates the "To" and "Cc" fields on each message since mailing/email-list addresses are usually in these fields rather than the "From" field.

Never add a user to his or her *own* approved-recipients list. Since the list is based on the recipient of the email, this causes all mail to bypass filtering.

Approved Domains

Messages from an approved domain are delivered to user inboxes, regardless of spam-like content. Messages from approved domains always circumvent junk email filters. However, if virus blocking is enabled for the recipient, the message security service does not deliver a message containing a virus, even if the domain is approved.

Approved senders can optionally override Attachment Manager and Content Manager filtering.

Approved Mailing/Email Lists

Messages sent to an approved mailing/email list are delivered to user inboxes, regardless of spam-like content. Messages from approved mailing lists always circumvent junk email filters. However, if virus blocking is enabled for the recipient, the email security service does not deliver a message containing a virus, even if the mailing/email list is approved.

Approved senders can optionally override Attachment Manager and Content Manager filtering.

Many mailing/email-list and newsgroup emails contain characteristics in common with spam. In fact, one person's opt-in mailing/email list can be perceived by another person as spam.

If you find mailing/email-list or newsgroup postings quarantined in the Message Center, add that list to the approved mailing/mail list to prevent the messages from being quarantined

The Approved Mailing list evaluates the "To" and "Cc" fields on each message — a mailing/email list most often place its address in those fields rather than the "From" field.

Never add yourself to your *own* Approved Mailing list. Since the Approved Mailing list is based on the recipient of the email, this causes all mail to bypass filtering.

Blocked Senders

Messages from individual senders or entire domains are quarantined, regardless of content.

You can add specific senders, for example, who otherwise keep getting past your other filters. (This feature works only if spam filtering is turned ON.)

Blocked Domains

Messages from an entire domain are quarantined, regardless of content.

Industry Heuristics and the Blocked Sender List

If an organization has Industry Heuristics turned on, a message containing industry content coming from a Blocked Sender is still quarantined. The industry-specific content disposition is set after the Approved/Blocked Senders disposition is set and processed.

You may consider adding an address from user's list to the appropriate organization-level list to improve filtering for all users, while freeing up space for that particular user.

When Sender Lists Apply

Sender lists are evaluated before spam filtering, but after virus blocking and other filters. As a result:

- **Users can't receive viruses or email attacks from approved senders**
If a message from an approved sender contains a virus or is part of an email attack, it is stopped by virus blocking or Connection Manager, and does not reach users.
- **Messages from approved senders are not quarantined as spam**
If a message from an approved sender is tagged as spam, the message is still sent to the recipient.
- **Approved senders can optionally bypass Attachment Manager and Content Manager filters**
Depending on your organization's email policy, you can optionally deliver messages from approved senders if they contain prohibited attachments or content. See "Configure Attachment Manager" on page 406 and "Create or Edit a Content Manager Filter" on page 340.

Organization and User Sender Lists

An organization-level list applies to all users in that organization; entries in that list are not visible to users in the organization. A user-level list applies only to that user.

The user's list takes precedence over the organization-level list. For example, if a sender is blocked at the org level but approved at the user level, then that sender's messages bypass spam filters and are delivered to the user's inbox.

Administrators access organization-level and user-level lists through the Administration Console. Users access their own lists through the Message Center.

Changes to approved- and blocked-sender lists take effect within seconds.

You can opt to propagate your org-level settings to sub-orgs. See "Propagation for Approved/Blocked Sender Lists" on page 392 for details.

How Senders Are Identified

The service identifies an approved or blocked sender by looking at the address in the message's From field. First, it looks at the From address shown in the message header. If that is empty, it looks at the From address in the message's Envelope (which is typically hidden from view in email clients).

Reply-To headers aren't checked because they aren't necessarily assigned to the actual sender.

How Domains Are Evaluated

When you include a domain in a sender list, any mail from that domain is approved or blocked according to the list in which it is included. Approving or blocking a domain affects all its subdomains, too. For example, if you approve jumboinc.com, then you also approve sales.jumboinc.com and marketing.jumboinc.com.

You cannot block a Top Level Domain (TLD) using the Blocked Senders list. A TLD is the right-most part of the address, after the last period. Examples of some common TLDs include .com, .edu, .gov, .net, and .org (types of domains) and locales, such as .uk, .mx, .jp, .ie, .ca. Instead, configure an IP range block on the TLD. For details, see "Manual IP Block Configuration" on page 457.

Note: Sender lists use message and envelope headers to determine sender addresses, and do not attempt to validate the sending email servers against domain names (for example, through DNS lookups).

Editing Sender Lists in the Administration Console

You use the Administration Console to edit org-level and user-level sender lists.

Editing Approved/Blocked Senders for Organizations

By default, changes to the organization-level approved/blocked sender lists do not retroactively propagate from an organization to sub-organizations. For example, if you add an address to the approved sender list in an organization, this address isn't added to the sub-organizations.

There are character limits for sender lists at both the org and user levels. For more information, see "Size Limits for Sender Lists" on page 394.

To edit org-level sender lists:

1. Go to **Orgs and Users > Orgs**.
2. Click the organization name in the organization list.
3. Under Inbound Services, click **Sender Lists**.

4. Enter an email address or domain into the Approved Senders or Blocked Senders field, then click **Add**.

To allow or block an entire domain, use a Content Manager filter. See “Sender address from one or more specific domains” on page 344 for information about creating a domain-level filter.

WARNING: Use caution with the option, “Apply settings and filters to existing sub-orgs.” When you choose the propagation option and make a change to the sender list for an organization, that organization’s sender list overwrites its sub-organization’s lists. This completely clears any senders lists in a sub organization and could result in an unrecoverable loss of data. For more information for possible solutions, see “Propagation for Approved/Blocked Sender Lists” on page 392“.

Propagation for Approved/Blocked Sender Lists

By default, changes to an organization-level approved/blocked sender list do not retroactively propagate from the parent organization to sub-organizations. For example, if you add an address to the approved sender list in an organization, that address is not added to sub-organizations.

To propagate changes for an organization, check the “Apply settings and filters to existing sub-orgs.” box and make at least one list change. This overwrites all organization-level approved/blocked sender lists for all sub-organizations with the current list.

If you have data in sub organization sender lists that you don’t want to lose, use the following methods to update those lists:

- Manually make the changes in each sub-organization.
- Use batch commands to make many changes at once. For more information on using batch commands, see “Using Batch Commands for Approved/Blocked Lists” on page 395.

When you create a *new* organization it receives a copy of all settings, including approved and blocked sender lists, from the parent organization.

Editing Approved/Blocked Senders and Approved Recipients for Users

To edit user-level sender lists:

1. Go to **Orgs and Users > Orgs**.
2. Select the org that contains the users whose lists you want to edit, then click **Users**.
3. Click the user whose sender lists you want to edit.
4. Under Inbound Services, click **Sender Lists**.

5. Enter an email address or domain into the Approved Senders, Blocked Senders, or Approved Recipients field, then click **Add**.

For a domain, use the format *@domainname.com* or *domainname.com*.

Editing Sender Lists in Message Center

You use Message Center or Message Center Classic to edit personal sender lists.

To edit the approved-sender lists in Message Center:

1. Log in to Message Center.
2. Click the **My Settings** link in the upper-right corner of the page.
3. Click the **Approve Senders** link.
4. Under Approved Senders, enter each email address you want to add. Separate multiple addresses by commas or semicolons, or enter each address on a new line.

Click **Update Approved Senders**.

5. Under Approved Domains, enter each domain you want to add. Separate multiple domains by commas or semicolons, or enter each domain on a new line.

Click **Update Approved Domains**.

6. Under Approved Mailing Lists, enter each mailing/email-list address you want to add. Separate multiple addresses by commas or semicolons, or enter each address on a new line.

Click **Update Approved Mailing Lists**.

WARNING: Do not add a user's address or domain to the approved lists. This allows all mail addressed to the particular user or to all users in the domain to pass through filtering without checking for spam.

To edit the blocked-sender lists in Message Center:

1. Log in to Message Center.
2. Click the **My Settings** link in the upper-right corner of the page.
3. Click the **Block Senders** link.
4. Under Blocked Senders, enter each email address you want to add. Separate multiple addresses by commas or semicolons, or enter each address on a new line.

Click **Update Blocked Senders**.

5. Under Blocked Domains, enter each domain you want to add. Separate multiple domains by commas or semicolons, or enter each domain on a new line.

Click **Update Blocked Domains**.

To edit the approved mailing list in Message Center Classic:

If the postings all have the same To address, users can use *Message Center Classic* to add the address to the approved mailing list:

1. Log in to Message Center Classic.
2. Click **Junk Email Settings**.
3. Click **Yes** for “Are you trying to approve an email mailing list or newsgroup?”
4. Enter the email address of the mailing list or newsgroup you find in the To: header of all postings.
5. Click **Save to List**.

Any of these configurations allow you or the user to use a domain (e.g. jumboinc.com) instead of a full address if necessary.

WARNING: Do not add the user's address or domain to the approved mailing lists configuration. This will cause all mail addressed to this or all users in the domain to be passed through filtering without checking for spam.

To approve/block all messages from a domain in Message Center Classic:

1. Log in to Message Center Classic.
2. Click **Junk Email Settings**.
3. Enter the domain name (e.g., jumboinc.com) in the field at the top of the approved/blocked sender lists.
4. Click **Save to List**.

Size Limits for Sender Lists

The maximum number of characters for *each* approved/blocked list in the Administration Console is 4000. If each address or domain is 30 to 40 characters, each sender list can include approximately 100 to 130 addresses and domains.

The maximum number of characters for *all lists for each user* in the Message Center is 1000.

For each address, add an additional 2 characters to get an accurate count.

If you run out of space and attempt to add another address, you receive an error similar to this:

```
List length limit (4000) exceeded
```

To free up more space, delete addresses that are no longer used.

You may consider adding an address from user's list to the appropriate organization-level list to improve filtering for all users, while freeing up space for that particular user.

Using Batch Commands for Approved/Blocked Lists

Use the batch commands `modifyorg` and `modifyuser` to modify the approved/blocked sender lists. For information on batch commands, see “Batch Processing and EZCommand” on page 611.

The batch-command syntax to add an address or domain to an approved/blocked sender list is as follows:

```
modifyorg ORGNAME, approved_senders=ADDRESS_OR_DOMAIN  
  
or  
  
modifyuser USER_ADDRESS, blocked_senders=ADDRESS_OR_DOMAIN  
  
or  
  
modifyorg ORGNAME, approved_senders=+ADDRESS_OR_DOMAIN  
  
or  
  
modifyuser USER_ADDRESS, blocked_senders=+ADDRESS_OR_DOMAIN
```

ORGNAME	The name or IID of the organization associated with the approved/blocked sender list
USER_ADDRESS	The address of the user associated with the approved/blocked sender list
ADDRESS_OR_DOMAIN	The domain or email address to add

The batch-command syntax to remove an address or domain from an approved/blocked sender list is as follows:

```
modifyorg ORGNAME, approved_senders=-DOMAIN_OR_ADDRESS  
  
or  
  
modifyuser USER_ADDRESS, blocked_senders=-DOMAIN_OR_ADDRESS
```

ORGNAME	The name or IID of the organization associated with the approved/blocked sender list
USER_ADDRESS	The address of the user associated with the approved/blocked sender list
ADDRESS_OR_DOMAIN	The domain or email address to remove

Addresses or domains can be added and removed within one batch command. Each address or domain needs its own operator (+ or -). Omitting the operator adds the address or domain. You must escape each comma (,) in the list with a backlash (\).

The following example adds `angel.com` and `investor.com` to the HugelISP organization-level approved sender list, and removes `funds.com`:

```
modifyorg HugelISP, approved_senders=+angel.com\,-funds.com\  
investor.com
```

Deciding Which Approved Senders to Add

Since adding an Approved Sender effectively allows traffic through filters, you should be cautious when deciding which addresses and domains to add to your Approved Senders list. Spammers can easily send emails that falsify the sender address to take advantage of any such configuration.

You should add addresses or domains that send messages that often look like spam but are not. Following is a process you can use to determine when to add an address/domain to your Approved Senders list:

1. Use the Quarantine Delivery Activity Log to find message trends:
 - a. Go to **Orgs and Users > Orgs**.
 - b. Select an organization from the list
 - c. Click **Reports**.
 - d. Click **Quarantine Delivery > Activity Log**.
 - e. Click the link to either the daily or weekly log.
 - f. Look for trends in messages that have been delivered by your users. (For example, look for multiple emails from the same sender, same sender domain, or same subject.)
2. For delivered messages that seem to establish a trend, research the messages (your research data is used in remaining steps):
 - a. Go to Users and click the **Quarantine** icon next to the user who delivered a message.
 - b. Select the **Delivered** radio button, and click **Apply**.
 - c. Select the message in question, and click **Show Header**.
 - d. Look at the header of the message. See “Determining Whether or Not the Message is Spam” on page 642 and “Analyzing Header Fields” on page 647 for details on determining if the message should be quarantined.
3. If messages from that sender address or domain regularly have a Spam rating that is less than 1.00000, then consider adding an Approved Sender.
4. If the messages are consistently quarantined by Attachment Manager or Content Manager settings, adjust them as appropriate so that they do not get caught.

Quarantine Redirect and Approved/Blocked Senders

If you are using Quarantine Redirect (forwarding an organization's quarantined messages to one account), see “Disabling and Redirecting Notifications” on page 280 for information about how to set up notifications under these circumstances. Use the Administration Console to add approved/blocked senders to the organization that contains the quarantine-redirect account. Use Message Center to add approved mailing lists to the quarantine redirect user account.

Be sure not to add approved/blocked senders to the quarantine redirect user account rather than adding them to the account of the intended recipient.

Message Headers for Approved/Blocked Senders

The message headers include information on whether a sender is listed in an approved/blocked list. See “Attachment Manager and Content Manager Header Fields” on page 646.

Troubleshooting: Approved/Blocked Senders and Mailing Lists

Why is it that some obvious spam messages are occasionally allowed through the filters?

Spammers commonly forge sender addresses from popular domains in attempts to bypass filtering. These may be approved senders you added, or approved senders that were pre-populated for your organization. You may wish to modify the lists for your organizations to remove these approved senders. Be sure to modify any organizations that contain your users.

If an email address meets the criteria of both the approved and blocked senders lists, which one takes precedence?

The blocked senders list takes precedence in the case of a conflict. Say, for example, an email is from `sender1@domain.com`. If `sender1@domain.com` is on the approved senders list, but `domain.com` is on the blocked senders list, then the message would be blocked, as would all messages sent from `domain.com`.

When adding a new address to one of my blocked/approved senders or approved mailing list, I receive the following error: “You currently have too many addresses in your list. Try deleting old addresses which are no longer used to free up more space and then try saving your address”. Why does this message appear?

The list size is 4000 characters for each approved/blocked sender list and 1000 characters for the approved mailing list. You may consider adding an address from an user's list to the appropriate organization list to improve filtering for your user population, while freeing up space for the user.

For each address entered, you need to add an additional 2 characters to get an accurate count.

As the service regularly improves filtering, many addresses in a blocked sender list may no longer be necessary.

How does adding a particular address to the approved mailing list allow messages with similar addresses to pass through?

The approval mailing list looks for a substring in the list of recipients. For example, adding al@jumboinc.com to a user's approved sender list automatically approves other messages that include "al", such as:

```
al@jumboinc.com
postal@jumboinc.com
denial@jumboinc.com
refusal@jumboinc.com
...
```

Note: If you want to approve an address but not also approve similar addresses as a by-product of that approval, as in the example above, use a Content Manager rule. For more information, see "Content Manager."

Why is a domain or address added to the approved/blocked sender list not approved or blocked as expected?

Either:

- The address or domain was not added before the message arrived.
 - It was not added to the user or organization containing the user.
 - It was added to multiple lists. See "Message Processing Order" for further details on the processing order.
1. Compare the received date of the mail message to the last modification date/time for the user:
 - a. Go to **Orgs and Users > Users**.
 - b. Enter the user address, and click **Search**.
 - c. Click **Settings Summary**.
 - d. Look at the Modified column, and compare the date & time with those of the email message. (This assumes the last user modification was to the approved/blocked sender list.)
 2. Look at the user approved/blocked sender lists:
 - a. Click the user.
 - b. Under Inbound Services, click **Sender Lists**.
 - c. Check all lists to see if the approved/blocked sender is listed.
 3. Look at the org approved/blocked sender lists:
 - a. Select the org.
 - b. Under Inbound Services, click **Sender Lists**.
 - c. Check all lists to see if the approved/blocked sender is listed.

When using a Quarantine Redirect for either Spam or Virus messages, the approved/blocked address or domain needs to be added to the sender list for the intended recipient, and NOT to the sender list for the quarantine redirect address.

Is it possible to get a full list of aliases for a registered user, or Approved/Blocked Senders for a user or organization?

To find the list of user aliases:

1. Go to **Orgs and Users > Users**.
2. Click the user address.
3. Under Settings, click **Aliases**.

To find the list of approved/blocked senders for an organization or user:

1. Go to **Orgs and Users > Orgs**, or **Orgs and Users > Users**.
2. Click the org name or user address.
3. Under Inbound Services, click **Sender Lists**.

Filtering was working fine, then suddenly much more spam made it through the filter for a particular user. Most of the spam messages are delivered with an X-pstn header containing the text GOOD RECIP. What is happening?

That user's own e-mail address or domain was added to his/her approved sender lists. Configured this way, all messages sent to that user or to the user's domain are allowed through.

The administrator can remove this configuration using the Administration Console as follows:

1. Go to **Orgs and Users > Users**.
2. Enter the user address, then click **Search**.
3. Click the user address.
4. Under Inbound Services, click **Sender Lists**.
5. Select the offending address or domain in the appropriate list.
6. Click **Remove** to delete the address or domain.

The user can remove this configuration using Message Center as follows:

1. Log in to Message Center.
2. Click **My Settings**.
3. Click **Approve Senders**.
4. Select the user's address or domain in the list.
5. Press **Delete** on your keyboard.

6. Click **Update Approved...** for the list.

The user can remove this configuration using *Message Center Classic* as follows:

1. Log in to Message Center Classic.
2. Click **Junk Email Settings**.
3. Click **Yes** next to the text that asks if you are trying to approve a mailing list or newsgroup.
4. Select the user's address or domain from the list.
5. Click **Delete From List**.

The approved mailing list functionality checks all incoming e-mail for the configured domain or address in the "To" field. Since most, if not all, of the e-mail to a given user uses this domain or address, most spam is simply passed through the filters regardless of how spam-like the message is.

When a I attempt to add or remove an entry from a sender list, I see the error "A request could not be completed because of a system error. Try clicking 'Back' on your browser and reload that page". What should we do if this happens?

Please contact customer support to resolve this issue. Please provide the Org ID, System #, User ID, and which list you are having an issue with (ex. approved, blocked, etc.,)

There is a rare occurrence of approved/blocked senders entries being inserted improperly. When this happens, all further editing to the approved/blocked sender lists fails with the error message described above.

Health Check: Approved Senders List Cleanup

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration.

Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust. Use the instructions below to make any adjustments if necessary to your Approved Senders lists.

Approved Senders List Cleanup

The Approved Senders List enables users or administrators to allow messages from a specific address or domain to bypass spam filters. However, spammers routinely "spoof" many sending addresses, and up to 50 percent of all junk messages bypass filters because of this technique.

Periodically review your Approved Senders list for any addresses that may be at risk of being spoofed. Be sure that your own domain is not on the list since this generates high amounts of spam for your users.

Note: If you must include your domain, use the IP Lock feature to ensure that only messages coming from your own IP addresses are accepted. Domains that are configured with IP Lock are not listed in Health Check. We recommend that you set up IP Lock *only at the email config level*.

To edit your Approved/Blocked Senders for an organization:

1. Go to **Orgs and Users > Orgs** in the Administration Console.
2. Click the organization name.
3. Under Inbound Services, click **Sender Lists**.

To edit your Approved/Blocked Senders for users:

1. Go to **Orgs and Users > Orgs**.
2. Select the org that contains the users whose lists you want to edit, and then click **Users**.
3. Click the user whose sender lists you want to edit.
4. Under Inbound Services, click **Sender Lists**.

To edit Approved Senders list in Message Center:

1. Log in to Message Center.
2. Click the **My Settings** link in the upper-right corner of the page.
3. Click the **Approve Senders** link.

For complete details and instructions on editing Approved/Blocked Senders in both the Administration Console and the Message Center, see the following sections:

- “About Sender Lists” on page 387
- “Editing Sender Lists in the Administration Console” on page 391
- “Editing Sender Lists in Message Center” on page 393
- “Size Limits for Sender Lists” on page 394
- “Deciding Which Approved Senders to Add” on page 396
- “Troubleshooting: Approved/Blocked Senders and Mailing Lists” on page 397
- “Approved and Blocked Sender Lists” on page 387

Related Topics

- **Health Check: Update User Settings**
- **Health Check: Update Virus Settings**
- **Health Check: Update Settings for Executable Attachments**

Chapter 16

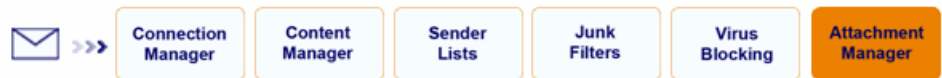
Attachment Manager

About Attachment Manager

Use Attachment Manager to filter messages based on the size or file extension of any attachments. Each of several filters can have its own *disposition*, or method of processing filtered messages. For example, you can bounce messages whose attachments exceed 200 MB, centrally quarantine messages with attachments that are .exe files, and you can user quarantine attached image files.

Attachment Manager can also send notifications to administrators or users when messages are either bounced or redirected to an administrator's quarantine.

When Attachment Filters Apply



Attachment filters are applied *after* all other filters except the Early Detection filters (which send messages to the Pending tab in the Message Center). As a result:

- **Attachment filters override content filters.**
If a message triggers an attachment filter, it can be bounced or quarantined, even if it contains content specifically allowed by a Content Manager filter.
- **Approved senders can optionally bypass attachment filters.**
If a message triggers an attachment filter that would bounce or quarantine it, but it's also from an org-level approved sender, it can still be delivered, if you configure Attachment Manager to allow email from org-level approved senders to bypass attachment filters (see “Configure Attachment Manager” on page 406).

- **With the exception of Early Detection filters, messages must pass other filters before Attachment Manager.**
Attachment Manager scans only valid messages. Message must pass through spam, senders lists, and virus filters before filtering by Attachment Manager. For example, a message infected with a virus that also triggers an attachment filter, is processed according to your Virus Disposition, not the attachment filter's disposition. For example, the message will be deleted if that's how you have configured your virus setting, instead of quarantined, approved, bounced per the attachment filter's disposition.
- **Attachment Manager approved file types do not bypass Early Detection filters.**
Even if you add .exe files (for example) as an approved file type in Attachment Manager, Early Detection may quarantine a message with a .exe file for additional scanning.

Attachment Manager is configured at the organization level, and it is turned off by default. After your initial Attachment Manager policy configurations, the Attachment Manager configuration should be reviewed whenever you set new or change existing attachment policies.

Attachment Identification Methods

Attachment Manager can identify incoming or outgoing messages with file attachments in two different ways, and automatically scans compressed files:

- **Extension scanning:** Attachment Manager examines the message's MIME (Multipurpose Internet Mail Extensions) headers to determine an attachment's extension. Sometimes, a malicious sender will try to disguise the file type by renaming the file extension. Attachment Manager verifies the real file type by checking for the MIME type as well as literal file extension.

Attachment Manager uses extension scanning by default.

- **Binary scanning:** Attachment Manager scans a portion of the attachment itself to determine its file type. This method can recognize file types more accurately than extension scanning.

Note that binary scanning now identifies Microsoft Office 2007 file types. If binary scanning cannot determine the file type of an attachment, Attachment Manager uses extension scanning as a fallback method.

Note: In some cases, binary scanning does not distinguish among some related file types, if they are generated by the same application. For example, binary scanning treats .pps (PowerPoint SlideShow) files as .ppt (PowerPoint) files.

- **Compressed File Scanning:** Attachment Manager automatically scans and identifies files inside compressed file attachments, such as .zip and .rar. files. This serves as an effective anti-virus tool since virus attacks are often delivered as executables files hidden in compressed files.

For example, if a message has a .zip file attached, Attachment Manager can apply filter rules to the .zip file and all the files contained in the .zip file. This Attachment Manager feature offers additional protection against zero-hour threats, such as virus-infected .exe files hidden in .zip files, and finer granularity of control over the file type filters.

Attachment Manager can also identify files in certain types of encrypted compressed files. If the file names in the archive are unencrypted, Attachment Manager will identify the types of files. Malicious senders typically use common compression tools to password-protect the contents of the archive, but not the file name information.

Following are technical details for the compressed file scanning feature:

- **Compressed file types:** Attachment Manager opens the most common compressed file types, including .zip, .tar, .gz, .lzh, and win.dat files. If compressed file cannot be opened and the contents scanned, Attachment Manager filters the message based on the compressed file type.
- **Files with differing dispositions:** When an attachment contains multiple files that trigger both bounce and approve/quarantine dispositions, Attachment Manager quarantines the message (the less severe action). For example:

Scenario 1: The message attachment is a .zip file that contains a .doc file. Attachment Manager is configured to quarantine .zip files but approve .doc files. This results in conflicting dispositions, and the message is quarantined.

Scenario 2: The message attachment is a .zip file that contains a .exe file. Attachment Manager is configured to quarantine .zip files, but bounce executable files. In this scenario, the message is quarantined.

Scenario 3: The message attachment is a .zip file that contains a .exe file. Attachment Manager is configured to bounce executable files. In this scenario, the message is bounced.

- **File identification:** Attachment Manager identifies the compressed file and the files within by either extension scanning (the default method) or binary scanning, whichever scanning method you've configured.
- **Nested compressed files:** When compressed files are nested within other compressed files, Attachment Manager opens and scans the contents. Attachment Manager will open many levels of nested compressed files, however, if the attachment shows the heavy nesting pattern associated with viruses, the message is identified as virus-infected and processed by the Virus Blocking filter.

Messages with Multiple Attachments

If the message has multiple attachments, Attachment Manager evaluates the message as follows:

- If only one attachment triggers a filter, Attachment Manager performs the disposition of that filter on the entire message, including all other attachments.
- If two or more attachments trigger a separate filter with different dispositions (except Ignore), Attachment Manager quarantines the message. For example, the message attachment is a .zip file that contains a .doc file. Attachment Manager has been configured to quarantine .zip files but approve .doc files. This results in conflicting dispositions, and the message is quarantined. That way, the administrator can review the message and decide what to do with it. If an administrator quarantine redirect address has not been configured, the message is sent to the user quarantine.

Configure Attachment Manager

The Attachment Manager settings are made at the organization level. You can configure Attachment Manager to:

- Send incoming messages to users' quarantines in Message Center, when those messages contain attachments that violate an attachment filter policy.
- Allow messages from senders on the organization's approved senders list to bypass the Attachment Manager filters. An individual user's approved senders list has no effect on the Attachment Manager filtering.
- Send notifications to users when messages intended for them are either bounced or redirected to an administrator's quarantine.

Before creating filters, you must enable Attachment Manager and specify an address for quarantining messages, an approved sender policy, and a custom bounce message.

1. Go to Orgs and Users > Orgs and select an organization that contains your users.

- Click the Attachment Manager icon in the Inbound Services or Outbound Services section. The View page then displays your filters and settings:

Filter Type	Disposition	Settings
Message Size 200 MB	Bounce	Status On Quarantine Redirect Account - none specified - Approved Senders Off Bounce Message <div style="background-color: #cccccc; padding: 2px; text-align: center;">ERROR 582</div> The file attached violates our email policy
Scanning Options Inside Compressed Binary Scanning	On Off	
Custom File Types ppt - none specified - - none specified - - none specified - - none specified -	Approve Bounce User Quarantine Quarantine Redirect BCC-Quarantine	
System Threats Executables Compressed Files Encrypted Unencrypted	Bounce Ignore Ignore	
Productivity Office Documents Multimedia Music and Sound Images	Ignore Ignore Ignore Ignore	

- Click Edit link in the gray bar and configure the Attachment Manager settings (listed below).
- After you've enabled Attachment Manager, click the Filters link to add or edit filters. See "Create / Edit Attachment Manager Filters" on page 409 for more information.

- Configure notifications for messages that trigger Attachment Manager filters. By default, notifications are sent to the administrator only, but can be sent to the user or both the user and administrator. See “Configuring Notifications for an Organization” on page 273 for information on setting up notifications, and “Default Notifications with Tokens” on page 654 for information on customizing the Attachment Manager Notification message.

Note: Configure Attachment Manager Notifications in the Notifications page. For more information, see “Configuring Notifications for an Organization” on page 273.

Inbound Attachment Manager - test QA IM customer4 Users View Edit Filters

Specify settings for all Inbound Attachment Manager filters. Your settings apply to this organization and new sub-orgs you add. You can copy settings to existing sub-orgs.

Filter Status Turn all filters off/on at once (e.g., to disable filters without having to reconfigure them).
 ▼

Quarantine Redirect Address Enter quarantine account for messages that are filtered with a Quarantine Redirect or BCC-Quarantine disposition.
 (primary email address - no aliases)

[Approved Senders](#) Allow all email from Approved Senders to bypass Inbound Attachment Manager filters.

Bounce Message ERROR 582:

 Apply these settings and filter settings to existing sub-orgs.

Attachment Manager Settings:

Field	Value
Filter Status	<p>Values: On or Off.</p> <p>For all but the message size filters to apply, Filter Status must be On. When Filter Status is off, the message size filter defaults to 200MB.</p> <p>To temporarily disable attachment filters but retain filter settings, set status to Off. Setting it back to On then re-enables all your filters.</p>
Quarantine Redirect Address	<p>Specify an administrator’s Quarantine for quarantining attachment filters with a Quarantine Redirect or BCC-Quarantine disposition. This can be the address of any user who has been added to the message security service.</p> <p>Note: You can also quarantine messages caught by Inbound Attachment Manager filters in individual user quarantines.</p> <p>This is also the address to which Attachment Manager Notifications will be sent.</p>

Field	Value
Approved Senders (for Inbound Attachment Manager only)	You can choose to have inbound messages from senders on the organization's approved senders list bypass the Attachment Manager filters. Click the Approved Senders link to see the current list. (An individual user's approved senders list has no affect on the Attachment Manager filtering.)
Bounce Message	<p>Enter a custom message to return to senders whose messages trigger an attachment filter with a Bounce disposition. This message applies only for file type filters, not the message size filter. Enter ASCII text up to 200 characters long, for example, "This message violates our email policy".</p> <p>When a file-type filter with a Bounce disposition is triggered, the offending message is returned to the sender along with the error code and message text supplied here.</p> <p>Messages bounced for exceeding the message size filter instead return the message: "552 Message too large - psmtip", which can't be customized.</p>
Apply these settings and filter settings to existing sub-orgs	<p>This propagates Attachment Manager settings to all sub-orgs.</p> <p>Values: Check box to turn on feature. The default is off.</p>

Create / Edit Attachment Manager Filters

You create attachment filters on the Attachment Manager Filters page:

1. Go to Orgs and Users > Orgs and select an organization that contains your users.
2. Click the Attachment Manager icon in the Inbound Services or Outbound Services section of the page. The Filter Status must be On for the filters to be active (with the exception of the attachment size filter described below). See "Configure Attachment Manager" on page 406 for steps to enable.
3. Click the Filters link in the gray bar to create your filters. Review these sections to help you configure the filtering strategy that meets your needs:
 - "Attachment Filter Order" on page 410, which describe how the filters are evaluated.
 - "Attachment Filter Dispositions" on page 410, which describes how filtered messages can be processed (for example, bounced or quarantined)
4. Set the maximum message size for file attachments. See "Message Size Filter" on page 412 for details.

5. Enter file types in the Custom File filters. These filter are most useful if you're filtering only a few types of files. See "Custom File Types Filter" on page 413 for details.
6. Set up filters for broad categories of files using the System Threats and Productivity filters. See "System Threats and Productivity Filters" on page 413 for details.
7. Optional: Configure binary scanning as the method to identify file types. See "Troubleshoot Attachment Manager" on page 414 for details.
8. If you haven't done so already, configure notifications for messages that trigger Attachment Manager filters. By default, notifications are automatically sent to the administrator only, but can be sent to the user or both the user and administrator. See "Configuring Notifications for an Organization" on page 273 for information on setting up notifications.

Tip: You can allow Approved Senders for an organization to bypass all Attachment Manager filters by clicking the Approved Senders check box on the Attachment Manager configuration page. See "Configure Attachment Manager" on page 406 for more information.

Attachment Filter Order

In Attachment Manager, filters are evaluated in the following order. The disposition of the first filter triggered is performed:

1. **Message Size:** First, attachments are evaluated for size. If a message triggers this filter, the message is bounced, regardless of whether the attachment is approved by any subsequent attachment filter.
2. **Custom File Types:** These are any file types you've specified to approve, bounce, or quarantine, as exceptions to subsequent filters. These filters are applied before other file type filters. So if you approve .gifs here, but quarantine image files using the Productivity filter, .gifs are approved, while other images are quarantined.
3. **System Threats:** Next, this filter approves, bounces, or quarantines a collection of compressed and executable file formats, including .exe, .zip, .tar, and many others, as well as attachments with multiple file extensions, such as .tar.gz.
4. **Productivity:** Lastly, this filter approves, bounces, or quarantines a collection of common document, image, multimedia, and spreadsheet file types.

Attachment Filter Dispositions

Each attachment filter can have a different disposition, depending on your particular policies (except the message size filter, which always bounces offending messages). You might want to bounce dangerous executables, for example, but merely quarantine images or sound files.

When creating the filter, select a disposition, as follows:

Disposition	Action
Bounce	<p>Rejects the messages and returns the sender an error message.</p> <p>For attachments that exceed the maximum size, the error returned is “552 Message too large - psmtip.”</p> <p>The error message for other filter types defaults to, “582 The file attached violates our email policy.” but can be customized on Attachment Manager’s Edit page (see “Configure Attachment Manager” on page 406).</p>
User Quarantine	<p>Places message in user’s Message Center, and labels the reason for quarantine as Attachment Manager.</p> <p>Also can place the message in the users’ Quarantine Summary. Be sure to turn ON the Quarantine Summary notification for your users if you are concerned that valid attachments may be quarantined (see “Configuring the Quarantine Summary” on page 284).</p>
Quarantine Redirect	<p>Sends the message to Attachment Manager’s designated quarantine. The message is not delivered to the user.</p>
Approve	<p>Skips all remaining Attachment Manager filters, allowing a message with any file type you enter here to bypass Attachment Manager filters.</p>
Ignore	<p>Performs no filtering. Sends the message to the next Attachment Manager filter, if any.</p>
BCC-Quarantine	<p>(Blind Carbon Copy) Copies the message to Attachment Manager’s designated quarantine. Also continues processing the message through remaining filters, delivering it to the intended recipient if it makes it through the filters.</p> <p>You can use this disposition to review what types of attachments users are receiving, without preventing people from receiving them.</p>

If a message triggers more than one filter, the disposition of the first filter triggered is performed. For example, if you’re quarantining executables, and you receive an .exe attachment that is also over the size limit, it will trigger the size filter and bounce, before reaching the Executables filter and being quarantined.

Scanning Options

Binary scanning is an optional method for identifying file attachments; it identifies an attachment by checking its binary content instead of the file extension. You can enable binary scanning from the Attachment Manager Filters page. When you enable binary scanning, Attachment Manager will then use binary scanning to identify file types for all of your filters (Custom File Types, System Threats, and Productivity filters).

See “Attachment Identification Methods” on page 404 for more information. (Note that binary scanning now identifies Microsoft Office 2007 file types.)

The “Scan inside compressed file types” check box is selected by default, and we recommend that you leave this feature ON.

Note: For “Encrypted” compressed file scanning to work correctly (under System Threats), you must turn ON “Scan inside compressed file types.” If you clear this check box, the disposition settings for Encrypted file types will be grayed out.

Scanning Options	<input checked="" type="checkbox"/> Scan inside compressed file types
	<input type="checkbox"/> Enable binary scanning

Message Size Filter

<small>Order</small>	<small>Type</small>	
1	Message Size	Bounce messages larger than the specified size, which includes both the attachment and the body/header.
	Bounce	<input type="text" value="200"/> MB (1-300)

Enter a value from 1 to 300 MB. Leaving the field blank defaults to 200 MB. When an attachment exceeds the size limit, the message is bounced, and the sender receives the SMTP error message, 552 Message too large - psmtpt.

The Message Size filter is always on, even when Attachment Manager’s Filter Status is Off. This policy applies to all traffic, including mail which is not filtered for spam and viruses. When Attachment Manager Filter Status is set to Off, the default value of 200 MB is used. (Note that if a different size limit has been set and Filter Status is set to Off, then the set Message Size limit will apply.)

Custom File Types Filter

Enter Custom File Types to filter only a few file types (rather than the collection included in System Threats and Productivity filters), or as exceptions to subsequent file type filters.

2 **Custom File Types** Enter file types to filter as exceptions to subsequent filters, or that aren't handled by those filters. Do not precede file types with a period. Separate multiple entries with comma and space. For example: vcf, txt, gif

Approve	<input type="text"/>
Bounce	<input type="text"/>
User Quarantine	<input type="text" value="doc"/>
Quarantine Redirect	<input type="text"/>
BCC-Quarantine	<input type="text"/>

For each disposition, enter one or more file extensions, without the period and separated by commas (for example, vcf, txf, gif). See “Attachment Filter Dispositions” on page 410 for a description of each disposition.

It is also possible to filter for files with multiple file extensions. Enter “two-ext” to filter attachments with two file extensions. Enter “three-ext” to filter all attachments with three or more file extensions.

WARNING: Any file with periods in the file name will be considered a multiple extension file. For instance, “Letter From Mr. Jones.doc” would be considered a two-ext file. Using “two-ext” and “three-ext” file types may lead to false positive results.

System Threats and Productivity Filters

Use System Threats and Productivity filters to filter entire categories of file types. System Threats include common executables as well as encrypted and unencrypted compressed file types (virus blocking will already have caught most malicious attachments, but these filters provide extra security).

Using System Threat filters, you can quarantine or bounce executables as well as password-protected compressed files. This feature enables organizations to meet compliance requirements for blocking or processing encrypted message content.

Productivity Filters check for office documents such as Microsoft Word or Excel, or media files such as images and sound files.

3 System Threats	Filter file types that threaten security (click links to see included types). Selecting Ignore passes messages to the next filter. Selecting User Quarantine allows users to deliver filtered messages from their quarantines.
Executables	Bounce
Compressed Files	
Encrypted	Quarantine Redirect
Unencrypted	User Quarantine
4 Productivity	Filter file types to enforce corporate email policies (click links to see included types). Selecting Ignore delivers messages with no filtering. Selecting User Quarantine allows users to deliver filtered messages from their quarantines.
Office Documents	User Quarantine
Multimedia	Ignore
Music and Sound	Ignore
Images	Ignore

1. Click a link (for example, Executables or Compressed Files) to see the file types are included in each filter.

WARNING: To filter just a few file types, don't use System Threats or Productivity filters (leave them on Ignore.) Instead, enter specific file extensions in the Custom File Types filter.

2. Choose how to process messages containing the file types: Bounce, User Quarantine (Inbound only), Quarantine Redirect, Approve, or BCC-Quarantine (Ignore provides no filtering). See "Attachment Filter Dispositions" on page 410.

Unlike Custom File Types, System Threats and Productivity file types are not verified against MIME type, but are filtered based on the file-extension name only.

Troubleshoot Attachment Manager

Here are answers to common questions. If you have more questions, contact support for more information.

What if I don't want messages from certain senders to be filtered?

You can allow Approved Senders for an organization to bypass Attachment Manager filters by clicking the Approved Senders check box on the Attachment Manager configuration page. See "Configure Attachment Manager" on page 406 for more information.

How do you block just one type of file, like an MP3 file or .exe file?

Add the file extension to the Custom File Types filter as described in "Custom File Types Filter" on page 413.

How do you limit file size of attachments?

Set the maximum attachment size using the Message Size filter as described in “Message Size Filter” on page 412.

Does Attachment Manager filter viruses?

No, messages and attachments are scanned for viruses *before* they pass through the Attachment Manager filter. Any messages with viruses are disposed of before reaching attachment filters.

Why is a message in an user’s quarantine when it should have been sent to the admin’s quarantine (Quarantine Redirect) or blocked by Attachment Manager?

The email message contained a virus, and your virus disposition is set to User Quarantine. Because virus scanning takes precedence over other filters, messages with viruses are disposed of according to your virus disposition.

Why are large attachments being bounced, even when Attachment Manager is turned off?

The Message Size filter is always in effect, even if Attachment Manager is off.

What happens if a message has more than one attachment, but only one triggers an attachment filter?

If only one attachment triggers a filter, Attachment Manager performs the disposition of that filter on the entire message, including all other attachments.

What happens if a each attachment triggers a conflicting disposition?

If two or more attachments in the same message trigger a separate filter with different dispositions (except Ignore), Attachment Manager places the message in the designated quarantine for the Quarantine Redirect disposition. That way, the administrator can review the message and decide what to do with it.

Health Check: Update Settings for Executable Attachments

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration.

Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust. Use the instructions below to make any adjustments if necessary to Attachment Manager.

Approved Executable Attachments

Attachment Manager allows admins to set rules around blocking or forwarding messages with executable attachments. When approving messages of a certain type, all spam filtering on the message is skipped.

Health Check will display any executable file types that are specified in the approved list.

To configure Attachment Manager:

1. Go to **Orgs and Users > Orgs** and select an organization that contains your users.
2. Click the Attachment Manager icon in the Inbound Services or Outbound Services section.
3. Click the **Filters** link in the gray bar.
4. Under System Threats, select **Bounce** or **User Quarantine** from the drop-down lists for Executables and Compressed Files.
5. Under Custom File Types, delete any custom executable file types specified in the Approve field, and copy them to Bounce or User Quarantine.
6. Click **Save**.

For more information, see also “Configure Attachment Manager” on page 406.

Related Topics

- **Health Check: Update User Settings**
- **Health Check: Approved Senders List Cleanup**
- **Health Check: Update Virus Settings**

Chapter 17

Industry Heuristics

About Industry Heuristics

Industry Heuristics is an optional feature. For more information on the features included in your service package, contact your account manager or vendor.

Industry Heuristics can help reduce falsely quarantined messages for users and groups that receive large numbers legal- or finance-related messages, which can contain content that appears to be spam. With Industry Heuristics turned on for a user organization, legitimate legal and financial is identified, and then filtered less rigorously to assure that these messages reach users. Messages may pass through spam filters, but are still subject to filtering by the Attachment Manager, Content Manager, Approved/Blocked Senders lists, and Virus Blocking.

Industry Heuristics is comprised of two functions, Content Heuristics and Transport Heuristics.

- *Content Heuristics* recognize content patterns and characteristics unique to a particular market segment, and considers that in the spam score. Content Heuristics can apply to spam in two ways:
 - Consider in Spam Filters: Makes it less likely that content fitting the heuristics is quarantined.
 - Allow: Automatically approves of all content fitting the Content Heuristics category.
- *Transport Heuristics* recognize and authenticate source IP addresses of legitimate senders within an industry segment to create a “trusted network” of senders who represent a significant portion of email traffic in that community. Transport Heuristics compare messages originating from specific domains is against the list of known IPs for that domain.

Different filtering standards are applied to communications among these trusted networks, for example, messages between law firms, courts, bar associations and other government agencies. A message coming from an authenticated SMTP source in the segment has a higher threshold to be considered spam. (The list of organizations in the trusted network is not editable).

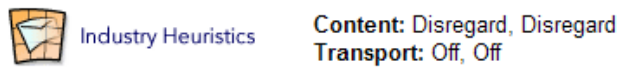
Note: Sales organizations may also find legal industry heuristics helpful, as sales emails often contain contracts and other legal language.

When Industry Heuristics are turned on, additional information is included in the `x-postn` headers. For more information these headers, see “Industry Heuristics Header Fields” on page 643.

Configuring Industry Heuristics

You may wish to create a separate organization for your legal, sales, or finance departments and enable Industry Heuristics only for that organization. By default, Industry Heuristics are turned off for an organization.

1. In the Administration Console, go the Orgs and Users > Orgs.
2. Choose the organization from the Choose Org pull-down list.
3. Click the Industry Heuristics icon in the Inbound Services section of the Org page.



4. Configure Content Heuristics for the financial and legal industries.

Content Heuristics Allow legal or financial content, or filter it less rigorously as spam.

Disregard treats the message normally, based on applicable spam filters.
Consider increases the required score for a message to be considered spam.
Allow delivers the message, bypassing spam filters.

Note: if a message is not triggered as spam, it is still subject to the other applications that may perform alternate dispositions, such as Attachment Manager or Content Manager.

	Disregard	Consider in Spam Filters			Allow
		Low	Moderate	High	
Financial	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Legal	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Transport Heuristics When On, messages from authenticated SMTP sources within the following industries are allowed:

Financial Off E.g., realtors, accounting firms, and lenders

Legal Off E.g., law firms, courts, bar associations, and government agencies

Apply settings and filters to existing sub-orgs.

5. The options are:
 - **Disregard:** Completely disregard the Content Heuristics. Messages are processed normally.
 - **Consider in Spam Filters:** Click Low, Moderate, or High to specify how much Content Heuristics will influence the spam score. The spam category filters act as multipliers to boost the spam probability score. For example, if you click High, legal or financial content messages are more likely to pass to your inbox.
 - **Allow:** Allow legitimate content to bypass the spam filter completely.

6. Set Transport Heuristics to On or Off.
7. Click the propagation checkbox to apply settings and filters to existing sub-orgs.
8. Click Save.

Chapter 18

Configuring Inbound Servers

About Inbound Servers

Every org structure which processes mail includes an *email server configuration*, also called an *email config*. An *email server configuration* holds settings for delivering messages to your mail server. You configure your email config for inbound email flow and security, delivery and disaster recovery features. The Inbound Servers tab manages email configs.

The Inbound Servers Tab

The following sections are included in the Inbound Servers tab:

- RPF: For instructions on managing your TLS, SPF, and IP Lock settings, see “RPF: Tools to Help Prevent Spoofing” on page 498. (available with *Google Message Security* only)
- SPF: For instructions on configuring the SPF Check feature, see “Enabling SPF Check” on page 503. See also “RPF: Tools to Help Prevent Spoofing” on page 498. (available with *Google Message Security* only)
- TLS: Transport-Layer Security settings. See “Transport Layer Security for Inbound Mail” on page 428. See also “RPF: Tools to Help Prevent Spoofing” on page 498.
- Connection Manager: For attack and IP blocking. See “Connection Manager” on page 453.
- Delivery Manager: For server IP/hostname configuration, load balancing, and fail-over. See “Delivery Manager” on page 465.
- Spool Manager: Optional, provides disaster recovery. See “Spool Manager” on page 481.
- Alerts: For proactive notification of events. See “Setting Up Alerts” on page 489 for details.

How Inbound Servers Work

In the organization hierarchy, an email config is usually a sub-org of the Account organization. Each email config has one or more associated sub-orgs that contain users and domains. Settings for an email config affect traffic for all users and domains in its sub-orgs. An address that isn't registered in the email protection service uses the email config for the domain.

Mail traffic is delivered to the receiving mail server through the Internet via any proxy server, router, or firewall you may be using, and is routed by external IP addresses.

When to Configure Inbound Servers

Create a new email config and configure its Inbound Server whenever you build distinct mail flow routing for a group of domains and users. For example, when you create a new mail server that is not part of an existing cluster, you also need to create a new email config.

Make Inbound Server configuration changes whenever you reconfigure Connection Manager, Delivery Manager, or Spooling Manager integration with your mail server. This includes all DNS and IP changes.

Say, for example, you want to route traffic for a group of your users to a new server, while the rest of your users route to the old server. In this case, create a new email config and change your organization structure so that the appropriate domains and users are in sub-orgs of the new email config.

To route mail traffic to deliver to both an old and new server, configure the Delivery Manager to balance load and route to both servers.

Creating an Email Config

To add a new mail server, you need to create a new email config organization and configure it, then create a sub-organization, add the domain and users, and change your MX records.

1. Go to the Orgs & Users > Orgs page (click the Orgs and Users tab immediately after logging in). Select the parent for your new email config from the Choose Org pull-down. Usually, this is your Account organization, but you can select any organization that isn't already under an email config.
2. If the organization is an Account organization, you can use a shortcut to add an email config. Select "Create Email Config" in the Orgs & Users > Orgs page. On the Org Settings page, under New Org, enter a name for your Email Config, usually "Email Config for [Domain]," then click Add. You can then skip to step 4.

Otherwise, select the parent organization. Under New Org, enter a name for your email config, usually “Email Config for [Domain],” then click Add.

3. Click the General Settings icon. Set the Email Config Org Type setting to Yes, and click Save.
4. Enter delivery information for your mail server by entering your mail server’s domain name or IP address in the Delivery Manager > Edit page. See “Setting up Delivery Manager” on page 475 for more information.
5. Add a sub-organization to the new email config. See “Create an Organization” on page 91 for more information.
6. Add domains and users to this new sub-organization. See “Add a Domain for Filtering” on page 236 and “Add / Delete / Move Users” on page 120 for more information.
7. Check the following configuration steps, detailed in other chapters:
 - a. Protect the mail server by configuring the Connection Manager. See “Automatically Blocking Attacks” on page 453 for more information.
 - b. If you have spooling available in your service package: Prepare for disaster recovery by setting up mail spool using the Spool Manager. See “Allocating Spool” on page 483 for details on spool allocation and “Configuring the Spool Manager” on page 484 for details on setting spooling to `Automatic`.
 - c. Configure Alerts to receive pages or emails for important server events. See “Setting Up Alerts” on page 489 for more information.
 - d. Configure your firewall to prevent spammers from bypassing the email protection service. See “Setting Up Secure Mail Delivery” on page 495 for more information.
 - e. Turn on TLS (Transport Layer Security) support if required, and your mail server is configured for TLS. See “Prepare Your Mail Server for TLS” on page 434 for more information.
8. Change DNS MX entries to route your mail traffic to the email protection service for a domain. See “Edit a Domain” on page 243 for more information.

Events

The Delivery Manager, Connection Manager, and Spool Manager all have traffic patterns that trigger *events*. An event is the time and date associated with a significant service reaction to mail server or traffic conditions (ranging from servers being unavailable to network-based attacks).

Events can trigger proactive responses that include sending out alerts, blocking attacks, enabling a failover server, or engaging spooling. See “ Administrator Alerts” on page 489 for more information on configuring alerts.

Event Tracking

Event	
EID	313023718
Event Type	Spam Attack
Begin Time	06/21 12:20:55
End Time	06/21 12:22:26
IP Address	131.161.233.150
Messages	66

Actions Taken	
Time	Action
06/21 12:20:55	alert spam attack Alert not sent, No specified recipients
06/21 12:20:55	IP block inserted ERROR 550 mailbox unavailable

Event Definitions

What are the different events and what do they mean? Following is the list of events, the components they are associated with, and the actions to take for each event. For more information on the events, see the chapters on Connection Manager, Delivery Manager, and Spool Manager.

Administrators can receive alerts (through email, text message, or pager) when these events occur. We strongly recommend that you set alerts for critical Delivery Manager events. See “Setting Up Alerts” on page 489 for more information. Here are definitions of all Event types:

Directory Harvest Attack	<p>A Directory Harvest Attack is a series of delivery attempts by one IP that results in 550 errors. Your email server responds to each request, issuing potentially thousands of 550 errors.</p> <p>Component: Connection Manager (“ Connection Manager” on page 453)</p> <p>Action: Connection Manager can temporarily block the source IP. Alerts can be sent. No action is required.</p>
---------------------------------	--

Spam Attack	<p>A Spam Attack is a barrage of spam messages from one IP address detected by users with spam filtering enabled.</p> <p>Component: Connection Manager (“ Connection Manager” on page 453)</p> <p>Action: Connection Manager can temporarily block the source IP. Alerts can be sent. No action is required.</p>
Virus Outbreak	<p>A Virus Outbreak is a large quantity of virus-laden messages from one IP address detected by users with virus filtering enabled.</p> <p>Component: Connection Manager (“ Connection Manager” on page 453)</p> <p>Action: Connection Manager can temporarily block the source IP. Alerts can be sent. No action is required.</p>
Mailbomb	<p>A mail bomb is a denial of service attack where many 500kb+ messages are sent from a single IP to your server(s)</p> <p>Component: Connection Manager (“ Connection Manager” on page 453)</p> <p>Action: Connection Manager can temporarily block the source IP. Alerts can be sent. No action is required.</p>
Email Host Down	<p>One mail server is unreachable or not responding. Other primary or failover servers are responding.</p> <p>Component: Delivery Manager</p> <p>Action: Delivery Manager attempts delivery for each new connection. If the connection fails, connections are attempted to other primary servers and then to failover servers. Alerts can be sent. You should investigate this issue; see the Delivery Manager troubleshooting section for details.</p>
Org Down	<p>All mail servers associated with an email config are down.</p> <p>Component: Delivery Manager (“ Delivery Manager” on page 465)</p> <p>Action: Spool Manager delay timer starts. If prolonged, spooling triggers. Alerts can be sent. You should investigate the issue; see the Delivery Manager troubleshooting section for details.</p>
Spooling	<p>Spool initiated.</p> <p>Component: Spool Manager (“ Spool Manager” on page 481)</p> <p>Action: No new connections are attempted to servers until spool is full or until you have suspended spooling. Alerts can be sent. You should investigate and unspool as appropriate.</p>

Viewing Event Details

Email administrators who take advantage of automated Connection Manager interventions and other Inbound Servers events require insight into the intervention and effectiveness of the actions taken by the email protection service.

Event Tracking

Search -All Events - > 0 msgs 1 - 5 of 5

Active EMS Events				13:41:42 PT
Event #	Date	Event Type	Msg Count	Source IP
36825	04/19 11:39:55	Spam Attack	122	0.0.0.5
36825	04/19 11:39:55	Dictionary Attack	842	0.0.0.4
36823	04/19 11:39:55	Dictionary Attack	13,222	0.0.0.2
36824	04/19 11:39:55	Spam Attack	521	0.0.0.3
36822	04/19 11:39:55	Spam Attack	78	0.0.0.1

1. Go to Orgs and Users > Orgs and select an email config from the Choose Org menu.
2. Click the Inbound Servers tab.
3. Select the Manager associated with the event (Connection Manager, Delivery Manager or Spool Manager) or click the Events link for access to all types of events.
4. The list of events can even be sorted by type, date, source IP or impact. Click any of the column headers to sort the list by that category. To sort or search for events that had the greatest impact, select messages Over 100, 500, or 1000 and search. This eliminates all the “low-impact” events and leaves only the ones over the value that you selected.

Note: It is not uncommon for an organization, especially an Internet Service Provider, to receive a high number of Directory Harvest Attacks—thousands a day. Up to 500 events are displayed, and searches and sorts are run against the entire population of events.

5. Click the Event ID number to see the Event details.

Event Fields

Events are composed of the following fields:

EID

Unique ID number for the Event.

The EID is the easiest way to differentiate different events when there are multiples of the same type, or that apply to the same IP within the same Event time period.

Event Type	<p>The type of event, which can be Spam Attack, Virus Outbreak, Directory Harvest Attack, Mailbomb, Mail Server Down, Org Down.</p> <p>See the chapters on Connection Manager, Delivery Manager, and Spool Manager for details on the different Events associated</p>
Begin Time	The time that the event started.
End Time	<p>The time the event ended.</p> <p>This is listed only after the event has ended <i>and</i> is verified. For example, in the case where there is an Org Down Event and the email protection service is spooling, Spooling stores incoming traffic in a spool file and does not attempt server delivery. Since the email protection service does not mark the event complete until after a successful delivery to the server, it does not complete until after the spool is full or has been otherwise disabled.</p>
IP Address	<p>For attacks, this is the IP address of the offending attacker. For an Email Host Down event, the associated IP is the down mail server.</p> <p>There is no IP associated with Org Down events.</p>
Messages	<p>For an attack, the number of messages blocked by the automatic attack block.</p> <p>The block prevents new connections from the attacker from being established. Since this happens before receiving details about specific messages, this statistic is generally very low; it only applies to messages within the connection that triggered the attack response.</p>
Actions Taken	<p>The actions taken by the email protection service when the event was detected.</p> <p>The possible actions include emailing alerts to administrators, triggering an automatic attack block, and enabling spooling.</p>

Troubleshooting: Inbound Servers

Why is there no Add Email Config link next to the org where I want to create an email config?

There is only an Add Email Config link next to Account organizations. Typically (over 90% of the time), email configs are sub-orgs of your Account org.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that encrypts and delivers mail securely. Transport Layer Security is an industry-wide best-effort standard based on Secure Sockets Layer (SSL) technology.

Transport Layer Security is an optional feature. For more information on the features included in your service package, contact your account manager or vendor.

The message security service includes several TLS and encryption options.

- **Inbound TLS.** Encryption of mail from outside senders to your server. The first step of mail (from the sender to the message security service) is always encrypted if possible. Mail in the next step (from the message security service to you) is encrypted according to your settings.
- **Outbound TLS.** Encryption of mail from your server to outside servers. Using this option requires that you set up your outbound mail to route through the message security service, which requires additional configuration. See “Configuring Outbound Servers” on page 507 for more information on Outbound Services.
- **Policy Enforced TLS.** Domain-Specific Setting for Inbound TLS. This is an optional feature and is not included with all product bundles. Policy Enforced TLS is configured on the same page as other TLS settings, if it is available. For more information, see “About Policy Enforced TLS” on page 438 and “Set Up Policy Enforced TLS” on page 442.
- **Message Encryption.** Part of Encryption Services. Using this option requires that you set up your outbound mail to route through the message security service, which requires additional configuration. This feature is configured in the Encryption Settings page. For more information, see the *Encryption Services Administration Guide*.

Transport Layer Security for Inbound Mail

Depending on the level of protection you have purchased, you may be able to enable Transport Layer Security (TLS), a protocol that encrypts and delivers mail securely. TLS connections are available for both inbound and outbound mail traffic.

For information on how to set up TLS with inbound mail, see “Setting Up Inbound TLS” on page 434

This section provides a technical overview of how TLS works on your inbound mail delivery and describes how to configure TLS in the Administration Console.

Transport Layer Security (TLS), a protocol that encrypts and delivers mail securely, helps prevent eavesdropping and spoofing (message forgery) between mail servers. TLS is a standards-based protocol based on Secure Sockets Layer (SSL). TLS is rapidly being adopted as the standard for secure email.

The protocol uses cryptography to provide endpoint authentication and communications privacy over the Internet. TLS is the email equivalent of HTTPS for web communications and has similar strengths and weaknesses.

The key features of TLS are:

- **Encrypted messages:**
TLS uses Public Key Infrastructure (PKI) to encrypt messages from mail server to mail server. This encryption makes it more difficult for hackers to intercept and read messages.
- **Authentication:**
TLS supports the use of digital certificates to authenticate the receiving servers. Authentication of sending servers is optional. This process verifies that the receivers (or senders) are who they say they are, which helps to prevent spoofing.

Expanded encryption options are available if you require further security. For more information about these products, see the *Encryption Manager Administration Guide*.

How Inbound TLS Works

Note: In descriptions of connections, this document uses the term *TLS* to refer to the full technical definition: secure SMTP over Transport Layer Security.

For inbound mail traffic, the email protection service acts as a proxy between the sending server and your mail server. Inbound messages are received through two separate SMTP connections. The first connection is from the sending server to the email protection service. The second connection is from the email protection service to your mail server.



This diagram shows the flow of TLS messages between servers:



- Stage 1: The sending server sends a message via TLS to the email protection service, which always accepts TLS messages and process them according to the TLS protocol. The message is encrypted from the sending server to the email protection service.
- Stage 2: You can choose whether the connection from the email protection service to your mail server connection uses TLS.

If a mail server sends a TLS-encrypted message and your mail server has TLS enabled, you receive a TLS-encrypted message.

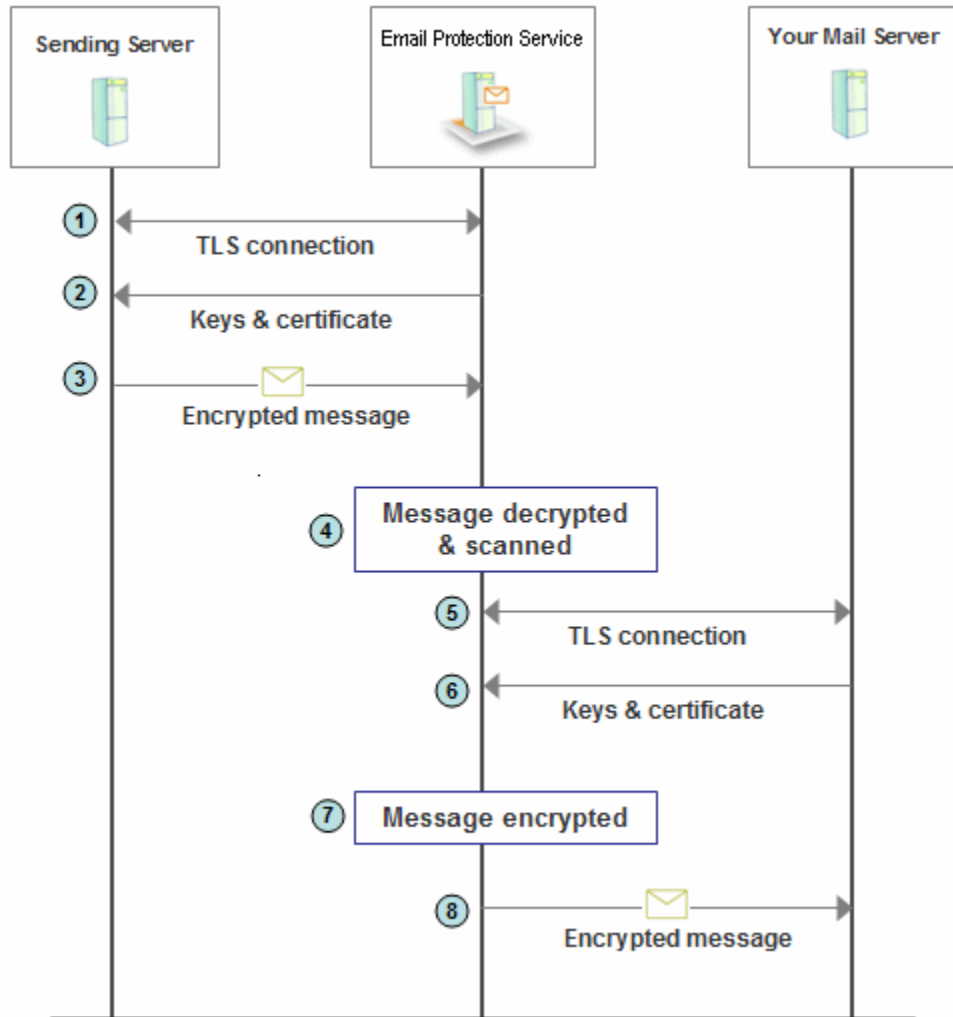


You may choose not to use TLS if your mail server is not TLS enabled. You receive the message from the email protection service unencrypted via SMTP. No TLS-initiated messages are lost or bounced.



Message Processing and Encryption

The following describes message flow, encryption, and message filtering for incoming TLS connections. (Note, this is a high-level overview; please see the TLS specification, RFC 2246, or other technical reference for the complete data flow.)



1. The sending server initiates a TLS connection with the email protection service. (TLS handshake with the email protection service using the ESMTP `STARTTLS` command.)
2. If the sending server attempts a TLS connection, the email protection service sends the certificate information, public key, and encryption specifications to the sending server.

3. While keeping the connection open with the sender, the email protection service establishes a TLS connection with your mail server. Your mail server must be TLS enabled.

Note: If your mail server is not TLS enabled, an SMTP connection can be established and the message is delivered unencrypted. This is based on your TLS settings. You can also set the email protection service to defer all messages if a TLS connection fails.

4. Your mail server sends your certificate information (including the public key for encryption) to the email protection service.
5. The sending server encrypts and delivers the message to the email protection service.
6. The message is decrypted, processed for viruses, and filtered based on junk mail settings and email policies (such as message attachments and content type). Other than the initial decryption, filtering is identical to normal filtering.
7. The message is encrypted again and delivered to your server via TLS.

As noted above, messages are decrypted in memory for virus and junk mail processing. In some instances, mail delivered via TLS is stored unencrypted:

- **Spooled messages.** In the case of disaster recovery, spool messages are stored unencrypted in our secure network, and then encrypted when delivered from spool to your mail servers.
- **Quarantined messages.** Quarantined messages are stored unencrypted in our secure network, and then delivered encrypted to your mail server when delivered from the Message Center. Both the quarantine summary message links and the Message Center allow users to display the messages in a browser via HTTP (not secure).

As part of your security policy, you may wish to disable the message links in the quarantine summary and Message Center. This ensures end-to-end secure delivery, requiring users to deliver messages from quarantine summary or Message Center to their inboxes. However, since the risk of falsely quarantining valid email is small, you may choose to retain the convenience of viewing messages through the quarantine summary or Message Center.

If you enable TLS in the administrative console, and your mail server is TLS-enabled, all notifications and alerts are delivered via TLS.

Authentication and Certificates

You need a digital certificate that includes public and private keys so that your mail server can establish TLS connections and encrypt/decrypt messages. This certificate can be an authority-signed certificate or a self-signed certificate. Your certificate is used only to negotiate encryption between the mail servers, and not to perform any disposition based the information in the certificate.

Your users do not need to configure any certificates on their mail clients to support TLS.

Following is a description of certificate processing in incoming TLS mail transactions.



1. TLS traffic is delivered to the email protection service using authority-signed certificates.

When the email protection service processes your incoming messages, the sending mail server receives a Google certificate that references a wild card server (*.psmtp.com) which represents the email protection service servers.

It is possible to employ encryption up to the 256-bit level (the highest level commercially available).

2. TLS traffic delivered from the email protection service to your server is encrypted using your certificate.

For TLS connections between the email protection service and your server, you may use either self-signed or authority-signed certificates. The type of certificate doesn't affect delivery—the email protection service uses your certificate to negotiate the encryption between the two servers, and does not perform any disposition based on the information in the certificate.

TLS-encrypted messages or messages sent from an authority-signed certificate only imply that the senders are who they say they are. Messages sent via TLS are not necessarily less likely to contain viruses or be junk mail.

Authentication Restrictions

The majority of current TLS implementations provide encrypted transactions, but do not enforce validation of authentication. Mail servers can be configured to process messages based on certificate type (authority-signed vs. self-signed), status (for example, expired or revoked), or other certificate information. With TLS, mail servers can only stop or deny messages based on certificate status or information, and most servers do not impose these restrictions.

If the sending domain restricts TLS traffic based on the receiving server's certificate (for example, deferring mail traffic if the domain in the certificate does not match the recipient's domain), you need to inform the sender that your mail traffic presents a security certificate from the email protection service. This should prevent mail from being held if the sending server expects a certificate referencing your domain or organization.

Other Forms of Email Encryption

In addition to TLS, earlier forms of SSL-based email security are also supported. When TLS is enabled, the email protection service attempts to connect with TLS first, but if this is not available, earlier versions of SSL email security are used, including SSL2 and SSL3.

Mail Server Performance with TLS

If you choose to enable TLS on your mail server, you may experience a performance decrease. Your server must establish an encrypted session for each TLS connection, which takes a few more processing cycles than establishing an unencrypted session. In addition, network bandwidth may be affected because of the additional data in the TLS handshake. The performance impact could be approximately 10-15 milliseconds per message; actual performance depends on your server configuration and the amount of incoming messages. In most cases, this difference won't be noticeable to your users. If there are performance issues, you may adjust the TLS settings through the Administration Console (see "Configure TLS for Inbound Servers" on page 436).

Setting Up Inbound TLS

Setting up inbound TLS involves these steps

- Prepare your mail server for TLS
- Test Your Mail Server's TLS Configuration
- Configure TLS for inbound servers in the Administration Console

Each step is described in detail below.

On the same page as inbound TLS, you can also configure inbound Policy Enforced TLS. For more information about Policy Enforced TLS, see "About Policy Enforced TLS" on page 438.

Follow these steps to set up inbound TLS on each mail server you want to configure.

Prepare Your Mail Server for TLS

Enabling TLS delivery requires enabling TLS on your mail server. Following are the steps required:

1. **Turn on TLS for Outbound service in the email protection service. See "Setting Up Outbound TLS" on page 522 for configuration steps.**

You only need to turn on TLS for Outbound if your outgoing mail is delivered through the Outbound service.

WARNING: You must turn on TLS for Outbound service in the Administration Console before enabling TLS on your mail server.

Some mail servers, specifically Microsoft Exchange 2000/2003, defer your outgoing mail if TLS is enabled *first*. If you find that messages are queued, be sure that TLS is disabled on your mail server, then turn on TLS in the Administration Console, and enable TLS on your mail server.

Similarly, to turn off TLS for outbound service, you must disable TLS on Exchange *before* making changes to the Outbound TLS settings in the Administration Console.

2. Obtain a certificate from a commercial certificate authority, or create a self-signed certificate for encryption purposes.

To obtain or create a certificate, contact an appropriate security vendor as the email protection service does not provide tools for obtaining or creating a certificate. More information on this may be available through support.

3. Install the certificate and enable TLS on your mail server.

Important: TLS support requires that you install your certificate and configure TLS on your mail server. This procedure may require some research and technical configuration upon your part. Please consult your mail server documentation for information on enabling TLS.

Further information for configuring the most common mail servers may be available through support. For further information, consult documentation and support for your mail server.

Test Your Mail Server's TLS Configuration

You can check if your mail server will accept TLS connections by using telnet from your mail server to the server software itself (you type the commands in `bold` text):

```
> telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.domain.com
Wed, 08 Feb 2007 08:05:03 -0700 (PDT)
> ehlo localhost
250-mail.domain.com Hello localhost [127.0.0.1],
pleased to meet you
250-STARTTLS
> starttls
220 2.0.0 Ready to start TLS
```

If you have other ESMTP options enabled, you will see more lines that start with 250-OPTIONNAME, and not only 250-STARTTLS. Once you receive a 200-series response to your `starttls` command, this confirms that your mail server will accept TLS connections.

For details verifying whether a message was transmitted via TLS, see “Received Header Field” on page 638.

You can also view a report of TLS activity with your service. See “TLS Reports” on page 580 for more information.

Configure TLS for Inbound Servers

Following is the procedure to enable TLS connections for inbound email. TLS connections are configured on each email config.

By default, TLS inbound support is turned off.

1. In the Administration Console, click Inbound Servers > TLS.



2. In the Inbound TLS page, choose an email server config from the Choose Org pull-down list.
3. Choose a setting for TLS delivery from the email protection service to your mail server.

Inbound TLS settings for delivery to email server config - test web Outbound Email Config

TLS Delivery

Choose the TLS encryption setting for email flow between the email protection service and your mail server.

Important: Your email server must be configured for TLS to receive messages via TLS.

- Send only SMTP
No TLS encryption, all messages delivered via SMTP.
- Send by SMTP or TLS
Messages sent via TLS are delivered via TLS to the recipient. Recipient servers that do not support TLS will receive their mail delivered via SMTP. All other messages are delivered via SMTP. (Recommended)
- Send by TLS if possible
Deliver all messages by TLS when possible. Recipient servers that do not support TLS will receive their mail via SMTP. (This may impact your mail server performance)
- Send by TLS Only
Send all messages by TLS. Mail sent to recipient servers that do not support TLS will be deferred. (This may impact your mail server performance.)



Following are descriptions of each delivery option:

- **Send only SMTP**

No TLS connections from the email protection service to your server. In other words, this is the “off” setting. If a message is sent via TLS, it is received by the email protection service in encrypted form, but delivered to your server unencrypted via SMTP.



- **Send by SMTP or TLS**

If a message is sent via TLS, the email protection service delivers the message via TLS to your server if possible, but otherwise delivers by SMTP. If the message is sent via SMTP, the email protection service delivers the message via SMTP to your server, so the message is delivered to match the sender’s preference if possible. This is the recommended setting. It ensures end-to-end TLS connections, and the impact to your server performance is relatively low.



- **Send by TLS if possible**

All messages are delivered from the email protection service to your mail server using TLS if possible. Recipient servers that do not support TLS receive their mail via SMTP. Messages, whether sent via SMTP or TLS are encrypted and sent via TLS from the email protection service.

This setting is not recommended because of the possibility of high load on your server. Because the TLS protocol uses encryption, your mail server must communicate to set up the encryption and decrypt every packet received from each SMTP connection. This impacts server performance.



- **Send by TLS Only**

Send all messages by TLS. Mail sent to recipient servers that do not support TLS will be deferred. This impacts server performance.



4. Click Save. Repeat the process for any additional email configs.

About Policy Enforced TLS

The message security service includes Transport Layer Security (TLS) functionality which can be applied to all mail traffic. Policy Enforced TLS expands this functionality, by allowing domain-based control of TLS. You can use Policy Enforced TLS to set up a custom encryption policy to send and receive for specific domains. For instance, you could configure Policy Enforced TLS so that all mail sent to a partner will be encrypted with TLS, and will bounce if the partner's TLS encryption stops working.

When you specify encryption for a specific sender or recipient, you can be sure that these connections are always encrypted. If Policy Enforced TLS cannot establish a TLS connection to the other server, the message will be deferred and no mail will be sent.

Features and Benefits

Policy Enforced TLS provides the following benefits:

- Support for Transport-Layer Security (TLS) encryption of email. Mail is encrypted before delivery, based on your TLS settings. You can set Policy Enforced TLS to bounce messages which cannot be encrypted, or to allow non-secure mail transmission.
- Ability to configure security settings separately for specific domains. You can name specific domains which will receive additional security. Domain-based TLS is set for each mail server separately.
- TLS configuration for inbound and outbound mail. Policy Enforced TLS can be configured for inbound mail and outbound mail separately.
- Ability to verify certificates to prevent malformed certificates or domain spoofing.
- Ability to send alert emails to administrators when Policy Enforced TLS bounces a message.

Requirements

Policy Enforced TLS is set up separately for inbound and outbound mail.

To set up Policy Enforced TLS for inbound or outbound mail requires the following:

- Support on your mail server for Transport Layer Security (TLS).
- Administration Console read and write permissions for Inbound Transport Security on the email config level.

To set up Policy Enforced TLS for outbound mail requires the following

- Support on your mail server for Transport Layer Security (TLS).
- Administration Console read and write permissions for Outbound Transport Security and Outbound Server Management on the email config level.
- Support on your server for Outbound Services.

Setting up TLS on your server ensures that your confidential email is secure throughout transmission. For information on implementing TLS on your mail server, check your mail server documentation. If you are using multiple servers, enable TLS on each server that routes mail to the email protection service.

For more information about Transport Layer Security in the Administration Console, see “Transport Layer Security (TLS)” on page 428.

For more information about other Encryption Services, see *Encryption Services Administration Guide*.

For instructions on how to route your outbound mail through Outbound Services, see the *Outbound Services Configuration Guide*.

How Policy Enforced TLS Works

Following is an overview of the data flow of Policy Enforced TLS. Policy Enforced TLS handles inbound and outbound mail flow separately.

Inbound Policy Enforced TLS Mail Flow

If you have Policy Enforced TLS enabled for inbound mail, specify a list of sending domains. Mail from these domains will be encrypted, while other domains use your normal TLS rules.

For inbound mail traffic, the email protection service acts as a proxy between the sending server and your mail server. Inbound messages are received through two separate SMTP connections. The first connection is from the sending server to the email protection service. The second connection is from the email protection service to your mail server.

This diagram shows the flow of TLS messages between servers:



- Stage 1: The sending server sends a message via TLS to the email protection service, which will always accept TLS messages and process them according to the TLS protocol. The message is encrypted from the sending server to the email protection service.
- Stage 2: A TLS connection is attempted between the email protection service and your receiving mail server. If a TLS connection is not possible, the email protection service will either defer the message, or send the message unencrypted, depending on your settings.

Without Policy Enforced TLS, you can set the email protection service to defer all messages if TLS is not possible, or to deliver them.

With Policy Enforced TLS, you can name specific sender domains which must be encrypted. If a message from one of these domains cannot be encrypted with TLS, it will always be deferred.

The deferral message for inbound messages is:

```
451 STARTTLS is required for this sender - psmtip
```

The deferral is handled by the sending server. Most sending servers will continue to attempt to send the message for up to five days.

As noted above, messages are decrypted in memory for virus and junk mail processing, then encrypted again when sent to you. In some instances, mail delivered via TLS is stored unencrypted:

- Spooled mail. In the case of disaster recovery, spool messages are stored unencrypted in our secure network, and then encrypted when delivered from spool to your mail servers.
- Quarantined messages. Quarantined messages are stored unencrypted in our secure network, and then delivered encrypted to your mail server when delivered from the Message Center. Both the quarantine summary message links and the Message Center allow users to display the messages in a browser via HTTP (not secure).

As part of your security policy, you may wish to disable the message links in the quarantine summary and Message Center. This will ensure end-to-end secure delivery, requiring users to deliver messages from quarantine summary or Message Center to their inboxes. However, since the risk of falsely quarantining valid email is small, you may choose to retain the convenience of viewing messages through the quarantine summary or Message Center.

Outbound Policy Enforced TLS Mail Flow

If you have Policy Enforced TLS enabled for outbound mail, you can specify a list of sending domains. Mail to these domains will always be encrypted. For outbound mail traffic, the email protection service acts as a proxy between the your mail server and the receiving server.

This diagram shows the flow of TLS messages between servers:



- Stage 1: The first connection is from your mail server to the email protection service. You can choose whether this connection uses TLS.
- Stage 2: The second connection is from the email protection service to the receiving mail server. If the exact recipient domain is in your list of domains for Outbound TLS by Recipient Domain, the outbound security service will connect via TLS to the receiving mail server.

If the recipient domain is set up for Policy Enforced TLS and TLS is not available, the following deferral message for outbound messages is sent:

```
451 Recipient does not support STARTTLS - psmtp
```

The deferral is handled by your server. Most sending servers will continue to attempt to send the message for up to five days.

Outbound mail sent to a domain that exactly matches one on the outbound sender list will always be sent via TLS in the second step. The Policy Enforced TLS settings override standard TLS setting for that email config organization for these domains.

If you have set up Certificate Validation, Policy Enforced TLS will drop the second connection and send an error if the recipient's certificate does not meet your validation requirements. See "Certificate Validation" on page 445 for more information.

Mail Between Message Security Service Customers

If two domains both use the message security service, Policy-Enforced TLS will enforce TLS on both hops of the journey, including those hops where TLS settings would not normally apply.

If either party has Policy-Enforced TLS for the other domain, the message security service will defer messages if the other domain uses an SMTP session instead of TLS.

This added protection applies only to domains using the message security service. It does not apply to distant hops of other mail relay servers.

Set Up Policy Enforced TLS

Set up Inbound TLS by Sender Domain

1. In the Administration Console, click the Inbound Servers tab. Select your email config organization, and click the TLS link.
2. If TLS is set to "Send only SMTP", change it to allow TLS. The recommended setting is "SMTP or TLS." See "Transport Layer Security (TLS)" on page 428 for more information on TLS settings.

3. Scroll to the Inbound TLS by Sender Domain section, at the bottom of the page. If you do not see this section, you do not have Policy Enforced TLS enabled. Contact your account representative for information.

Domain-Specific Setting for Inbound TLS

Require TLS to be used when receiving mail from specific domains. Note that the sender's domain is taken from the sender envelope, not the email header.

To add domains to the active lists, enter the domain name (for example: domain.com), and click the Add Domain button.

Domain Name:

<input type="checkbox"/>	Domain Name	Last Modified
<input type="checkbox"/>	domain.com	Wednesday, August 1, 2007 10:52:17 AM PDT

4. Enter the domain name you wish to set as TLS-only. Type the exact domain name; wildcards and subdomains are not supported.
5. Click Add. The change takes effect immediately.
6. Recommended: Enable TLS Alerts so you will be notified if a problem occurs. See “TLS Alerts” on page 448 for more information.

To remove one or more domains, check the domains you wish to delete and click Delete Selected. The changes take effect immediately.

Set up Outbound TLS by Recipient Domain

Before you can use Outbound TLS by Recipient Domain, set your mail server to route outbound mail through the email protection service, and enable TLS on your mail server. See “About Policy Enforced TLS” on page 438 for more information about requirements.

1. In the Administration Console, click the Outbound Servers tab. Select your email config organization, and click the TLS link.
2. If TLS is set to “Accept only SMTP” or “Send only SMTP”, change your settings to allow TLS. The recommended setting is “SMTP or TLS.” See “Transport Layer Security for Outbound Mail” on page 521 for more information on outbound TLS settings.

3. Scroll to the Outbound TLS by Sender Domain section, at the bottom of the page. If you do not see this section, you do not have Policy Enforced TLS enabled. Contact your account representative for information.

Domain-Specific Setting for Outbound TLS

Require TLS to be used when sending mail to specific domains. The domain-specific settings override the default settings.

To add domains to the active lists, select the appropriate TLS Certification Validation option, enter the domain name (for example: domain.com), and click the Add Domain button.

To change the domain-specific settings, select the checkbox next to the modified Domain Names.

Domain Name:

TLS Certificate Validation:

<input type="checkbox"/>	Domain Name	TLS Certification	Last Modified
<input type="checkbox"/>	example.com	Verify Cert	Wednesday, August 1, 2007 10:58:55 AM PDT
<input type="checkbox"/>	jumboinc.com	Encrypt Only	Wednesday, August 1, 2007 10:58:06 AM PDT
<input type="checkbox"/>	medical.jumboinc.com	Check Trust	Wednesday, August 1, 2007 10:58:55 AM PDT

4. Enter the domain name you wish to set as TLS-only. Type the exact domain name. Wildcards and subdomains are not supported; each subdomain must be added separately.
5. Click Add. The change takes effect immediately.
6. Optional: Set Certificate Validation. The default setting, Encryption Only, should be sufficient for most domains, but you can validate the recipient's certificate by changing this setting to Verify Certificate, Trust Check, or Domain Check. For more information, see "Certificate Validation" on page 445.
7. Recommended: Enable TLS Alerts so you will be notified if a problem occurs. See "TLS Alerts" on page 448 for more information.

To remove a domain, select the domain you wish to delete and click Remove. The change takes effect immediately.

Policy Enforced TLS with Multiple Email Config Organizations

If you have multiple Email Config organizations for different mail servers, consider using the same TLS and Policy Enforced TLS settings for mail server as a best practice. Otherwise, you may see surprising deferral messages.

Policy-Enforced TLS for outbound messages is based on the sender's email address, not the sender's server. If you have multiple mail servers that share users in the same domain, those users will have different TLS policies, which may cause unexpected deferrals.

Certificate Validation

Certificate Validation is an advanced feature for administrators who need to verify TLS certificates to avoid malformed or spoofed certificates. When outbound mail is sent to a domain that is configured for Certificate Validation, Policy Enforced TLS verifies the format, source, and domain of the certificate. You can specify different validation settings for each domain.

Set up Certificate Validation for each domain on the Outbound TLS settings page, under the heading “Domain-Specific Setting for Outbound TLS.”

Domain-Specific Setting for Outbound TLS

Require TLS to be used when sending mail to specific domains. The domain-specific settings override the default settings.

To add domains to the active lists, select the appropriate TLS Certification Validation option, enter the domain name (for example: domain.com), and click the Add Domain button.

To change the domain-specific settings, select the checkbox next to the modified Domain Names.

Domain Name:

TLS Certificate Validation:

<input type="checkbox"/>	Domain Name	TLS Certification	Last Modified
<input type="checkbox"/>	example.com	Verify Cert	Wednesday, August 1, 2007 10:58:55 AM PDT
<input type="checkbox"/>	jumboinc.com	Encrypt Only	Wednesday, August 1, 2007 10:58:06 AM PDT
<input type="checkbox"/>	medical.jumboinc.com	Check Trust	Wednesday, August 1, 2007 10:58:55 AM PDT

To set up Certificate Validation:

1. Go to Outbound TLS settings in the Administration Console.
2. If the domain is not already listed in Policy Enforced TLS, add the recipient domain to Policy Enforced TLS.
3. Under “Domain-Specific Setting for Outbound TLS,” set TLS Certification to the appropriate setting and click Save Selected.

Scope of Certificate Validation

Certificate Validation examines SSL certificates to verify a recipient’s identity. The standard that defines TLS, RFC 2487, states clearly that the possibility of multiple hops during email delivery makes TLS certificates unsuitable for authenticating a sender’s identity (inbound messages).

To comply with the standard, Certificate Validation authenticates the recipient’s identity for only outbound Policy Enforced TLS. Certificate Validation is not used for inbound mail because the RFC standards do not support this use.

Certificate Validation Settings

Certificate Verification is a powerful tool to protect your secure connection from spoofing and invalid certificates. However, it also will interrupt mail flow if the recipient's certificate is not set up correctly. If protection from spoofing and invalid certificates is not a major concern, use Encrypt Only. Use Certificate Verification if you wish to set up regular, ongoing secure connections with a specific partner for extremely sensitive information.

Note: If you set up Certificate Validation, be sure to set up TLS Alerts as well, so you will know if a problem occurs. For more information, see "TLS Alerts" on page 448.

Certificate Validation settings are described below.

TLS Certification	Description
Encrypt Only	<p>Behavior: Policy Enforced TLS obtains the keys from the Server Certificate, extracts the keys, completes the TLS handshake, and begins the encrypted session. No further verification takes place. Errors that prevent key extract will result in a bounced connection, but any other certificate-related errors are ignored.</p> <p>Recommendations: This setting provides the most reliable delivery of encrypted mail, and is recommended in most cases. Use if you wish to allow a TLS connection even with malformed or out-of-date certificates. This setting allows encrypted communication even if the recipient's certificate is invalid, as long as the certificate is functional.</p>
Verify Cert	<p>Behavior: Confirm that the certificate has proper form and syntax. Ensures that certificates are valid, but provides no protection against spoofing. Policy Enforced TLS ends the session if any certificate errors occur, but allows an out of date certificate, self-signed certificate, or certificate from an unknown trust.</p> <p>Recommendations: This setting can be used to detect any problems with the TLS certificate. If you wish to block malformed certificates, and detect any certificate problems, use this setting. This setting provides increased verification, but may stop some outbound mail.</p>

TLS Certification	Description
<p>Check Trust</p>	<p>Behavior: In addition to the certificate tests in Verify Cert, also verifies that the certificate is from a known valid Certificate Authority. Does not allow a self-signed certificate or certificate from an unknown trust. Requires a complete certificate chain. Will also block any certificate linked to an IP address instead of a hostname. Ends the mail session if the trust check fails.</p> <p>Recommendations: This is a very stringent setting and can cause problems with outbound mail flow to the recipient if the recipient's certificate is not properly prepared. Contact your recipient before you use this setting, and send at least a few trial messages to test that mail flow is not interrupted. This setting provides secure delivery and protection against spoofing, but may interrupt delivery if the certificate is not signed properly.</p>
<p>Check Domain</p>	<p>Behavior: In addition to the certificate tests in Verify Cert and Check Trust, also confirms that the domain in the certificate matches the domain of the server host. If there is a wildcard in the domain certificate, the recipient's domain must match the wildcard. Will also block any certificate linked to an IP address instead of a hostname. Ends the session if the domain check fails.</p> <p>Recommendations: This is the most stringent setting and will cause outbound mail to fail if the domain in the certificate does not match the domain of the recipient's mail server. Contact your recipient before you use this setting, and send at least a few trial messages to test that mail flow is not interrupted. Be aware that mislabeled domains in TLS certificates are not uncommon; if your recipient is using a different domain name in certificates, mail flow will be interrupted. This setting provides the most secure delivery and protection against spoofing, but has a high risk of mail flow interruption.</p>

Change the Default Certificate Validation Setting

You can change the default setting as well. When you add a new domain to Policy Enforced TLS, it will use this Certificate Validation setting.

To change the default Certificate Validation setting

Go to Outbound TLS settings in the Administration Console.

1. Under TLS Certificate Validation, select the default setting you wish to use.

2. Click Save as Default.

TLS Alerts

Policy Enforced TLS is intended for secured business partners who intend to encrypt all email communication between two parties. To prevent secure messages from being transmitted in the open, Policy Enforced TLS will refuse messages that come from specified domains when TLS sessions fail.

TLS Alerts inform your administrators when Policy Enforced TLS rejects a message. If a TLS connection fails, this may indicate a problem which requires immediate administrator action. With TLS Alerts, your administrators can detect and correct security problems immediately.

TLS Alerts apply to both inbound and outbound messages.

WARNING: TLS Alerts are not enabled by default. You must set up them up.

Configure TLS Alerts

Set up, modify or disable TLS Alerts in the Administration Console using batch commands.

Enable, Modify or Disable TLS Alerts

1. Log in to the Administration Console.
2. Go to the Batch page in the Orgs & Users tab.
3. Enter the following command into Step 2.5 and click “Submit job”:

```
modifyorg <orgname>, tls_notify_admin=<admin>,  
tls_notify_on=<interval>
```

`orgname` is the name of your email config organization. TLS Alerts are set on the email config level, not the user or account level.

`admin` is the email address (or alias) of an administrator account. You can use your own address or another address in any domain, as long as it is the address or alias of an administrator for any organization.

`interval` shows how often an alert can be sent, in seconds. The minimum is 1 (no more than one message per second), and the maximum is 86400 (no more than one message per day.) After a Policy Enforced TLS problem causes an alert, no more alerts will be sent for the time period specified. In most cases, a 600 second default is recommended. To turn off TLS Alerts, set the interval to 0.

4. Confirm the values by entering the following command into Step 2.5 and clicking “Submit job”:

```
displayorg <orgname>
```

`orgname` is the name of your email config organization.

Modify or Disable TLS Alerts

1. Log in to the Administration Console.
2. Go to the Batch page in the Orgs & Users tab.
3. Enter the following command into Step 2.5 and click “Submit job”:

```
modifyorg <orgname>, tls_notify_admin=<admin>,  
tls_notify_on=<interval>
```

`orgname` is the name of your email config organization. TLS Alerts are set on the email config level, not the user or account level.

`admin` is the email address (or alias) of a new admin address to use. You can use your own address or another address in any domain, as long as it is the address or alias of an administrator for any organization.

`interval` shows how often an alert can be sent, in seconds. Set to 0 to disable TLS Alerts.

4. Confirm the values by entering the following command into Step 2.5 and clicking “Submit job”:

```
displayorg <orgname>
```

`orgname` is the name of your email config organization.

Alerts Description

The sender of TLS Alerts is:

```
"<yourcompany> Support" support@<domain>
```

`yourcompany` is the name of your company, listed in the Administration Console Organization General Settings. `domain` is the name of the domain affected.

When Policy Enforced TLS blocks an inbound message, your administrator will see the following alert:

This message is an automated alert from your email protection service.

Your email protection service was unable to accept messages from the following domain, because the domain's mail server cannot use TLS:

<sender domain>

Your Inbound TLS by Domain encryption policy requires this domain to send messages using TLS. Your email protection service returns messages from this domain if the domain's mail server cannot establish a TLS connection with the service.

Recommended action: Contact the email administrator for domain <sender domain>.

When Policy Enforced TLS blocks an outbound message, your administrator will see the following alert:

This message is an automated alert from your email protection service.

Your email protection service was unable to send messages to the following domain, because the domain's mail server cannot use TLS:

<recipient domain>

Your Outbound TLS by Domain encryption policy requires this domain to receive messages using TLS. Your email protection service returns messages sent to this domain if the domain's mail server cannot establish a TLS connection with the service.

Recommended action: Contact the email administrator for domain <recipient domain>.

Alerts for messages blocked in a distant hop

When Policy Enforced TLS blocks an inbound message because of a TLS failure on a distant hop (a message send outbound through the email protection service by a sender unable to establish a TLS connection), your administrator will see the following alert:

This message is an automated alert from your email security service.

The email security service was unable to accept messages from the following domain, because the domain's mail server did not establish a TLS connection:

<sender domain>

Your Inbound TLS by Domain encryption policy requires messages from this domain be sent using TLS. Your email security service defers messages if the domain's mail server does not establish a TLS connection with the service.

Recommended action: Contact the email administrator for the domain <sender domain>.

If the problem cannot be resolved, you can use the email security service's Administration Console to delete the encryption policy. This will allow email from this domain to be received, but without encryption.

When Policy Enforced TLS blocks an outbound message because of a TLS failure on a distant hop (a message sent to a recipient who also uses the email protection service who could not establish a TLS connection), your administrator will see the following alert:

This message is an automated alert from your email security service.

Your email security service was unable to send messages to the following domain, because the domain's mail server would not accept a TLS connection.

<recipient domain>

Your Outbound TLS by Domain encryption policy requires this domain to receive your messages using TLS. Your email security service defers the messages if the service cannot establish a TLS connection with the domain's mail server.

Recommended action: Contact the email administrator for the domain <recipient domain>.

If the problem cannot be resolved, you can use the email security service's Administration Console to delete the encryption policy. This will allow email from this domain to be delivered, but without encryption.

Chapter 19

Connection Manager

About Connection Manager

Connection Manager groups and analyzes message content by connection and by the IP address of the sender. Based on the experience with attacks, Connection Manager recognizes different attacks, and can automatically protect your mail server and alert you when attacks are detected. You can also configure the Connection Manager to block all connections from a specific IP address, or to let a particular IP address connect, even when its behavior would normally trigger an attack.

Connection Manager has three pages: View, Edit and Events:

- View provides visibility into your mail flow and server health.
- Edit allows you to enable or disable automatic attack blocking.
- Events allows you to examine individual attacks.

Note: Connection Manager settings vary based on your purchased features. For some versions of the message security service, Connection Manager blocks are always in place and cannot be disabled. For other versions, it is an optional feature

The Connection Manager automatically blocks and prevents attacks and provides an interface to block IP ranges using a selectable SMTP error code. It also allows you to configure trusted servers which should not be blocked as attackers.

Automatically Blocking Attacks

The Connection Manager can be configured to automatically block attacks using the Edit page.

In order for Connection Manager to stop an attack, an administrator must, in advance, activate the settings, select a sensitivity level for determining the condition, and choose an appropriate 500-class error response.

Threat Response		
Attack Type	Sensitivity	500 Error Returned
<p>Email Bomb Detects the malicious delivery of messages meant to deny or disrupt normal services.</p>	<input type="checkbox"/> Normal	550 mailbox unavailable
<p>Directory Harvest Attack Prevents spammers from harvesting valid email addresses off of your server.</p>	<input type="checkbox"/> Normal	550 mailbox unavailable
<p>Virus OutBreak Identifies a sudden spike in the volume of virus-laden messages relative to total inbound messages.</p>	<input type="checkbox"/> Normal	550 mailbox unavailable
<p>Spam Attack Identifies a sudden spike in the volume of spam relative to total inbound messages.</p>	<input type="checkbox"/> Normal	550 mailbox unavailable

Types of Attacks

Based on billions of messages processed each month, profiles were developed for the following four different types of malicious mail server attacks.

Directory Harvest Attack (DHA)	DHA refers to an attack where the attacker sends many SMTP “rcpt to” commands to a server in an attempt to check common user names by brute force. Although its aim is to retrieve a list of user addresses, it can act as a Denial of Service (DoS) attack by making the receiving mail server overloaded by replying to “rcpt to” commands instead of processing mail traffic.
Email Bomb	An email bomb is a DoS attack where a large volume of emails with a large mean message size are sent from a particular IP, overwhelming the receiving mail server.
Spam Attack	A spam attack is DoS attack whereby a statistically significant quantity of spam relative to non-spam traffic is sent from one server.
Virus Outbreak	A virus outbreak is a DoS attack whereby a statistically significant amount of virus traffic relative to valid email traffic is received from a particular sending server over a time period.

Sensitivity to Attacks

Connection Manager settings provide flexibility when responding to email attacks. The sensitivity setting provides a simple lever to adjust the attention the Connection Manager pays to attackers. The default setting for each attack is “Normal”. Normal is the recommended setting, which will identify most attacks with no chance of misdiagnosing an attack.

To understand just how the other sensitivities relate to Normal, consider that each email attack has a numerical formula, and each sensitivity setting has a multiplier which adjusts the scale of the attack. This table lists the multipliers used for each sensitivity setting:

Sensitivity	Multiplier	Description
Very Low	0.25	Blocks relatively few attacks.
Low	0.5	Blocks fewer.
Normal	1	Default. Identifies most attacks without error.
High	2	Blocks more attacks
Very High	4	Very aggressive in blocking attacks. Increases possibility of error.

Note: The Sensitivity settings also affect alerts since sensitivity determines when the event is initiated.

Enabling Automatic Attack Blocking

Automatic attack blocking should be configured as soon as you create a new inbound email config. Connection Manager’s automatic attack blocking provides protection so your server bandwidth is used for processing legitimate traffic than junk messages. See

If you have any trusted relay servers passing mail to your primary mail servers, then they will pass significantly more traffic than other servers. As such, it is likely that these servers will trigger automatic blocks. If you have any relay servers you do not want to be blocked by the Connection Manager’s automatic blocks, then follow the steps in “Pass Throughs: Preventing Attack Blocking” on page 459.

Note: Some customers always have Directory Harvest Attack, Spam Attack, and Virus Outbreak attack blocking enabled. This is based on your service plan. Settings can be adjusted, but the attack blocking cannot be disabled.

1. Go to Orgs and Users > Orgs and select the mail server you want to protect from the Choose Org pull-down list.
2. Click the Inbound Servers tab. The Connection Mgr page appears.
3. Click the Edit link in the dark gray bar.

4. Select the check boxes for any automatic blocks you want to enable, and set your desired Sensitivity and 500-series error message and submit the form. See “Types of Attacks” on page 454 for descriptions on sensitivity settings.
5. Click Submit to save the changes.

Handling “Unknown User” Bounces

WARNING: Email servers such as Microsoft Exchange and gmail accept all inbound messages, even for invalid recipients, then perform a directory lookup to validate the recipient and send a bounce message, if needed, by separate email. This process, *asynchronous bouncing*, suppresses the real-time DHA prevention that Connection Manager can provide. To allow Connection Manager to handle this, activate Asynchronous Bouncing control. When activating this service, it is important to keep your user list up to date to avoid DHA false positives.

Handling "Unknown User" Bounces

Email servers that issue "unknown user" bounce messages asynchronously require added protection.

Email servers like **Microsoft Exchange** and **gmail** will accept all inbound messages, even for invalid recipients, then perform a directory lookup to validate the recipient. If the recipient is not listed in the directory, a new message is generated and placed in the outbound queue to be delivered to the sender. This process suppresses the real-time DHA prevention that the email protection service can provide.

By activating this feature, the email protection service will compare directory information with incoming recipients to measure erroneous delivery attempts. When activating this service, it is imperative that you keep our directory up to date.

Activate **Check the box if your email server issues an asynchronous bounce for unknown users.** This setting tracks invalid delivery attempts and prevents Directory Harvest Attacks.

[Full Definitions](#)

Submit Cancel

To activate this feature:

1. Go to Orgs and Users > Orgs and select the mail server you want to protect from the Choose Org pull-down list.
2. Click the Inbound Servers tab. The Connection Mgr page appears.
3. Click the Edit link in the dark gray bar.
4. Check “Activate” at the bottom of the page.
5. Click Submit to save the changes.

What activating this feature means

Activating the checkbox under Handling “Unknown User” Bounces is only useful if you are using a server that initially accepts mail for invalid users, such as Microsoft Exchange or qmail.

This feature provides additional protection against directory harvest attacks, and can dramatically reduce load on your server. If you are using a Microsoft Exchange mail server, you will benefit tremendously from this protection.

WARNING: You should not enable this feature until you have most of your users added. This feature checks incoming mail against your user list in the message security service. Therefore, it may block good mail if you enable the feature before adding the majority of your users.

Manual IP Block Configuration

The Connection Manager prevents malicious email attacks. If you do not have it available to you, or if you wish to block a specific IP address (or range of addresses) for a set amount of time, use the Manual IP Blocking feature.

Manual IP Blocking can also be used for administrators who choose to only receive alerts when they are under attack, and then use the manual IP block to stop the attack. If the IP address is not known, you can go to the “View Sender-specific Data” page to identify the Top 50 IP addresses connecting to your email server at that time.

Note: If you have multiple rules acting on the same IP address or range, (e.g. one automated Connection Manager block and one manual Pass Through) the Connection Manager will act on the rule with the longest duration.

Following are two examples of when you would configure manual IP blocking:

- Case 1: A list service sends you content you never want to allow to your users. In this case, set up a manual block for the IP ranges that make up the list server cluster.
- Case 2: A business partner sends regular newsletters which are sometimes picked up as spam, causing the IP address to be blocked. In this case, set up a manual pass through for the IP ranges that make up the list server cluster. This will insure that all traffic is individually processed by the filters. For more information about Pass Through, see “Pass Throughs: Preventing Attack Blocking” on page 459.

Manual IP Blocking

Manual IP Blocking allows you to define a specific IP address or range to block or bounce

Rule Name

IP Address

 Example: 255.137.52.4
 End IP Address, if range

Action To Take

Return SMTP Error:

Blackhole (email is deleted without delivery)

Pass Through (process as normal)

Expiration

Days Hours Mins

Notes

Blocking an IP Range

Set up a manual block whenever you would use your firewall/router to block all traffic from an IP or IP range.

1. Go to Orgs and Users > Orgs, and choose the email config you want to protect from Choose Org pull-down list.
2. Click the Inbound Servers tab. The Connection Mgr page appears.
3. Click the Block an IP link.
4. Name your manual blocking rule and fill in the IP address or range of the servers to block.

WARNING: Be careful not to block a large range. There is no automated caution or limit preventing you from blocking thousands of IPs with one rule.

5. Select the desired action.

Blackhole: Connection Manager acknowledges receipt of the message and then discards it without possibility of retrieval.

500 Error: There are several 500-class errors to choose from, though email servers treat all 500 errors the same. Connection Manager generates these errors so your server does not need to (see “Attack Blocking Details” on page 460).

Pass Through: When blocking a range of IP addresses, the pass through option will allow email to be delivered from an IP address within a range of blocked addresses. Pass Through messages will not bypass the junk email or virus filters. They are still subject to filters and quarantining.

6. Set the desired Expiration time.
7. Type in any Notes and click Submit.

Pass Throughs: Preventing Attack Blocking

A pass through is a manual block set with Pass Through as the action. See “Manual IP Block Configuration” on page 457.

Configure a manual pass through whenever you have a trusted relay server which sends you unfiltered traffic, the volume of mail will be enough to trigger an attack. However, in order for an attack rule to trigger, the majority of email from the source needs to fit the content profile of a DHA (little or no message content), email bomb (large messages), spam attack (spam messages), or virus outbreak (virus-laden messages). Once the second criteria is met, then an attack block will be triggered. Since the server is trusted, you know that it is not initiating the attack, so you should set a pass through to prevent automatic attack blocking from preventing all traffic from the server.

If you do not trust that the server sends you valid traffic, it would be unwise to set up a pass through.

Note: A pass through will not cause the mail traffic from the server to bypass filters, so this does not create email security holes.

Attack Blocking Details

When enabled, the Connection Manager automatically detects and blocks attacks as follows:

1. All input from connections from the offending IP address receives your SMTP error response and all connections to your mail server due to the attack are closed. Following is the list of SMTP error codes:

550 mailbox unavailable - psmtpp	This is the standard response a mail server will return when the attempted address is invalid.
552 storage allocation exceeded - psmtpp	This is the standard response a server will return when the recipient's mailbox is out of disk space.
553 mailbox name not allowed - psmtpp	This error indicates a syntax problem.
554 transaction failed - psmtpp	This error indicates too many errors processing the message.
571 spam source blocked - psmtpp	This error indicates that the sender was detected as a spammer.

You can configure an SMTP error which best fits how you want Connection Manager to respond to a type of attack. You can use vague errors which indicate user, server, or transmission problems, or you can use an error which indicates that the content was simply blocked as an attack.

2. Connection Manager logs an event containing attack details. (See "Connection Manager Events" on page 462 for more details on events.)
3. The Connection Manager sends alerts to specified email addresses. (See "Administrator Alerts" on page 489 for more information.)
4. No new connections are allowed from the offending IP address for a period of time.

Network Effect Protection

Network Effect Protection is a powerful feature in Connection Manager that protects your server from attacks. Network Effect Protection identifies IP addresses that are a source of multiple attacks, and temporarily drops connections from those IP addresses. This level of security applies across the message security service, and does not require any special configuration.

If a sending mail server is detected as a source of a spam or other malicious email attacks, Network Effect Protection temporarily marks the IP as a dangerous source. During an attack, Connection Manager tracks and logs the source IP address and activity level of the sender. Connection Manager stops the attack as well as prevents the sender from subsequently attacking any other customers of the message security service.

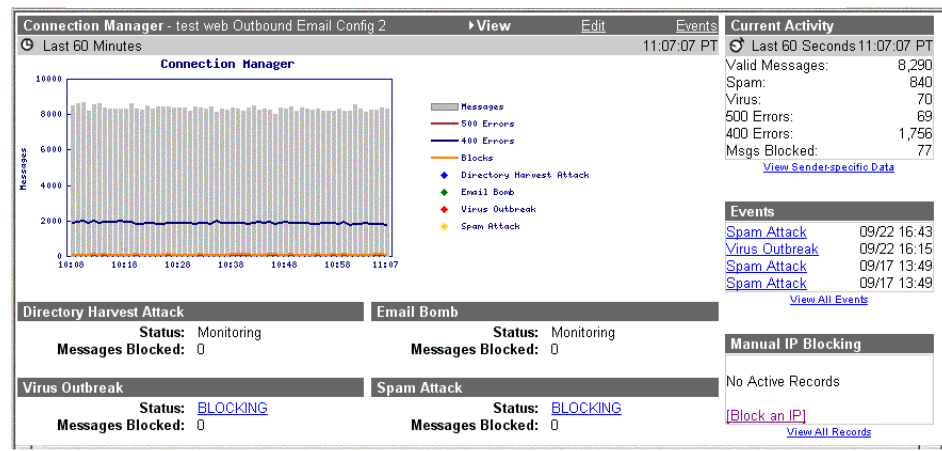
While an IP address is identified as a source of an SMTP attack, connections from the server are dropped without an error for one hour. Most legitimate servers detect dropped connection as a network error and attempt a new connection. However, most malicious sending servers, which send mail in bulk, will not attempt to send another message. Because of this, Network Effect Protection protects your mail server from attacks, with very little risk of false positives.

After every hour of refused connections, Connection Manager evaluates the behavior of the offending IP address to determine whether to remove the IP blocks, and return the traffic profile to normal conditions.

You can bypass Network Effect Protection for a particular sending IP address by adding a manual pass through. For more information about how to do this, see “Pass Throughs: Preventing Attack Blocking” on page 459.

Interpreting the Connection Manager View Page

The Connection Manager View page is a static page which gives you insight into your mail server health. Since the data behind the page is constantly changing, use your browser to reload the page to load new data.



The Connection Manager View page is made up of the following sections:

Last 60 Minutes Graph	<p>Graph showing details on messages processed per minute including 500-series errors, 400-series errors, attacks blocked and the number of messages blocked.</p> <p>The graph is updated once per minute.</p>
Current Activity	<p>Similar to the data displayed on the Overview page but includes vital 400 and 500-series SMTP error information.</p> <p>This perspective of Connection Manager effectiveness contains the last 60 seconds of statistics on your inbound message traffic. This information is updated every few seconds. The timestamp shows the hour, minute, and seconds of the traffic sampling in Pacific Time.</p>
Component Status	<p>An administrator can quickly view the status for each Connection Manager attack type.</p> <ul style="list-style-type: none">• Inactive: Not enabled.• Monitoring: Enabled, but no such attack is being blocked.• Blocking: Enabled and blocking an attack. <p>Status information is updated every second.</p>
Connection Manager Events	<p>The most recent Connection Manager-related events</p> <p>For further investigation or analysis on the event and related actions, click the event name to view the Event Record.</p> <p>A log of all Connection Manager events within the last 48 hours can be accessed by clicking on the View All Events link. This list can be searched and sorted for ease of navigation.</p> <p>This list is updated as new events are logged.</p>
Manual IP Blocking	<p>Shows five Manual IP Blocks by expiration date. See “Manual IP Block Configuration” on page 457 for more information.</p> <p>This list is updated as new manual blocks are configured.</p>

Connection Manager Events

The Connection Manager Events page is accessed by either clicking the Events link in the dark gray bar or click View All Events on the Connection Manager View page.

The Connection Manager Events page provides:

- A list of all events associated with the Connection Manager
- Interface to display up to 500 events of any type from the past 48 hours
- The ability to select an event to view its details

Since there is a Connection Manager Events for each attack detected, the event details include the following information:

EID	Unique Event ID Number for the Attack Detected
Event Name	Type of attack blocked (DHA, Email Bomb, Spam Attack, or Virus Outbreak)
Begin Time	Date and time the attack was detected
End Time	End date and time for the connections responsible for the attack. Note: If attack blocking is enabled, then the attack is blocked immediately at the time of detection.
Messages	Number of messages blocked by the attack block
Actions Taken	Time-stamped details on when the IP block response to the attack was inserted and details on what alerts were sent out

Troubleshooting: Connection Manager

How do you locate the IP address of a server that has opened a long time-duration TCP/IP connection to your mail server?

1. From the Administration Console go to the Organization pull-down list or the Show Hierarchy window, to select the appropriate email server config for the server that is being probed.
2. Click the Inbound Servers tab. The Connection Manager page appears.
3. Click the View Sender-Specific Data link near the top right corner of the page. The IP you are looking for will have an extremely long Avg. Duration time and possible Msg. Size of 0.

Health Check: Update Connection Manager Settings

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration.

Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust.

To configure Connection Manager for Health Check:

1. Set the "Virus Outbreak" sensitivity to VERY HIGH.

Note: A virus outbreak is a DoS attack whereby a statistically significant amount of virus traffic relative to valid email traffic is received from a particular sending server over a time period. This setting identifies a sudden spike in the volume of virus-laden messages relative to total inbound messages.

2. In the Administration Console, go to **Orgs and Users > Orgs**, then select an organization that contains the users for whom you want to configure Connection Manager.
3. Click **Inbound Servers**, and select **Connection Mgr** on the tab bar.
4. Click **Edit**.
5. In the Sensitivity drop-down list for Virus Outbreak, select **Very High**.
6. Click **Submit**.

For more information about Connection Manager and setting Virus Outbreak sensitivity level, see "Connection Manager" on page 453.

Related Topics

- **Health Check: Update Virus Settings**
- **Health Check: Approved Senders List Cleanup**
- **Health Check: Update Settings for Executable Attachments**
- **Health Check: Firewall Test**
- **Health Check: Update User Settings**

Chapter 20

Delivery Manager

About Delivery Manager

Delivery Manager allows you to:

- Balance the load of message traffic across multiple email servers.
- Set up fail over.
- Identify server outages and alert the administrator.

Delivery Manager balances inbound message load across multiple email hosts, regardless of the email server's geographic location or operating system. The Delivery Manager works independently of such limitations because the message security service architecture relies on the SMTP email standard.

You can assign multiple email servers to one email config from the Delivery Manager page. This will work as long as the user groups under that particular email config can share the same email servers.

See "Configuring Inbound Servers" on page 421 for information about creating email server configs.

How Delivery Manager Works

After messages are filtered, valid email messages are delivered to the customer's mail server. Below is the process that Delivery Manager uses when connecting to a customer.

1. When a new connection is opened to the message security service for a domain, the connection is assigned to an email server config, and in turn, a delivery server at the customer site.

The primary email servers are evaluated first (fail over servers are ignored at this point). If there is more than one primary server, Delivery Manager takes into account the percentages for each server and decides upon a delivery order. If there is more than one primary server specified and the customer has not specified percentages, Delivery Manager assigns each an equal weight and randomly assigns a delivery order.

2. A connection attempt is made. If the connection attempt immediately fails, times out, or the server's connection limit has been reached, then Delivery Manager connects to the next primary server in the delivery order.
3. Step 2 is repeated as necessary through the rest of the primary servers. This continues until either a successful connection is made or until all primary servers have been tried.
4. If all primary servers fail, then steps 1-3 occur using the bank of fail over servers.

It will try the fail over servers unless any one of the primary servers had connection limiting in effect and was at its limit. In other words, the system will not roll to the fail over when it feels that the only reason it could not connect to a customer's primary server was that they were at their maximum number of desired connections.

5. If a connection is successfully made, Delivery Manager passes the email message to the customer server. Consistent with the pass-through architecture of the message security service, the system relays responses to SMTP commands back to the sending server.
6. If all primary and fail over server connections fail, or the sending connection approaches the 5 minute connection timeout, then the SMTP error, `451 Can't connect to domain.com - psmtip` is returned to the sender.

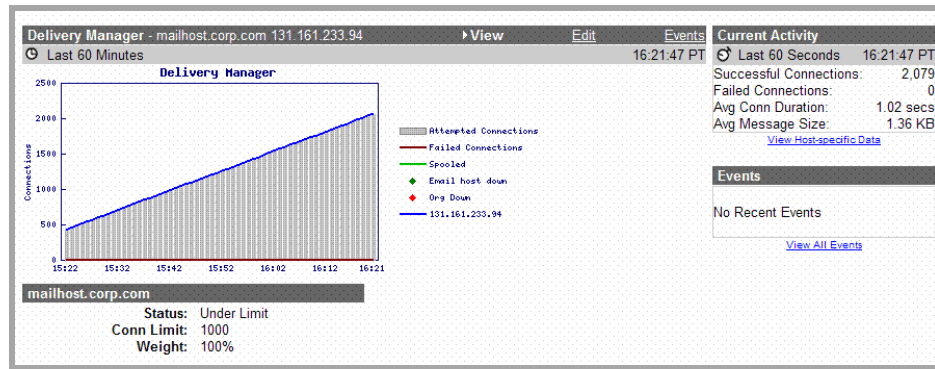
Interpreting the Delivery Manager View

The Delivery Manager View page gives you a summary of connection and event activity for an email server config over the past 60 minutes and 60 seconds.

View the Delivery Manager View Page

1. Click the Inbound Servers tab and choose an email server config from the pull-down list.

2. Click the Delivery Manager link to show the overview page.



The data is displayed on this page updated every few seconds but the page does not automatically refresh itself. Refresh the browser window to refresh the data.

The format of time stamps is the hour, minute, and second in Pacific Time.

The Delivery Manager graph shows activity over the last 60 minutes, including how many connection attempts, both successful and failed, there have been for the email server config. Events such as mail spooling, email host down, and org down events are also shown (if any have occurred).

Status	Displays the status of the mail server. Typically, the status will be “under limit” which means the number of connections is less than the set limit. Under more extreme cases, it may also display “Host Down” when a connection cannot be made.
Connection Limit and Weight	Shows the connection limit and traffic percentage allocated to an email server. These parameters may be changed from the Delivery Manager - Edit page.
Current Activity Box	Displays the vital statistics relating to your email system over the last 60 seconds.
View Host-specific Data link	Clicking the View Host-specific Data link lists your email servers (by IP address) and provides more in-depth data.
Events	Displays any recent Delivery Manager events, such as a mail host or org down event. Click the event or the View All Events link to see more information about a specific event. WARNING: We strongly recommend that you configure alerts for these events so that you will automatically receive notification of an event. See “ Administrator Alerts” on page 489 for more information on configuring alerts.

Dual Delivery

Dual Delivery is a setting in Delivery Manager that sends approved mail to the same user on multiple mail servers. When you set up Dual Delivery, the message security service will send approved mail to your primary mail server plus a second mail server that you specify.

Requirements

To use Dual Delivery, you must meet the following requirements:

- **Primary Server.** A primary mail server accessible from the Internet with a valid DNS record. Your domain and users must be set up to receive mail on your primary server.
- **Dual Delivery Server.** A dual delivery mail server accessible from the Internet with a valid DNS record. Your domain and users must be set up to receive mail on your dual delivery server as well.

Note: The Primary Server and Dual Delivery Server mail servers can be any Internet-compatible mail server, including any version of Google Apps Gmail that supports your domain. Note that while Gmail is supported, the Message Security & Discovery feature available with Google Apps Premier Edition includes separate integration between Gmail and the message security service, and does not support dual delivery. To use dual delivery, update to the standalone version of the message security service.

- **Registered users.** Set up all users in the message security service. Mail sent to users not registered in the message security service, including mail sent to a catchall address, will not be delivered to the dual delivery mail server. Mail sent to a domain alias or subdomain (with subdomain stripping enabled) will be redirected to the same address in the primary domain.
- **Tag and Deliver Off.** You must have the Junk Mail Tag and Deliver feature disabled for your users. If the Tag and Deliver feature is enabled, you will not be able to configure Dual Delivery

How Dual Delivery Works

After successful delivery of mail to the primary mail server, dual delivery sends another copy of the same mail message to your dual delivery server.

Note: Dual Delivery is available for inbound mail only. Outbound mail is never sent to a dual delivery server.

Dual Delivery is different from Spool Manager, which spools mail in the case of a mail flow failure and delivers mail once mail flow is restored. Dual Delivery will only send mail to the dual delivery server if the message is successfully delivered to the primary mail server, and does not store messages in the message security service like Spool Manager. You can use Dual Delivery with Spool Manager; messages that are spooled are also sent to the dual delivery server.

Headers

When the message security service attempts to send a message with Dual Delivery, the message security service will mark all mail, including both the message sent to the primary mail server and the message sent to the dual delivery server with an extension header field indicating that Dual Delivery was attempted. The extension mail header is:

```
X-pstn-continuity: dualDelivered=true
```

Data Flow

The following describes the data flow of dual delivery.

Primary Mail Server Connection. The message security service receives an incoming connection from the sending server and opens a connection with the recipient mail server, as usual. If the connection fails, the message security service will attempt to connect to a failover server that you specify in Delivery Manager.

Send Message to Primary Mail Server. The message security service sends the first copy of the message to the primary mail server, or a failover server if the primary server is down.

Report Success and Close Connection with Sender. After the recipient successfully receives the message, the message security service sends a 250 Ok SMTP message to the sending server and closes the connection with the sending server.

Open Connection with Dual Delivery Server. If dual delivery is enabled and the message is an appropriate message for dual delivery, the message security service opens a new connection with the dual delivery server.

Send Message to Dual Delivery Server. The message security service sends the second copy of the message, then closes the connection with the dual delivery server.

Send Alert if Needed. If delivery to the dual delivery mail server fails, the original sender does not receive any alert or notice, since the message was already successfully delivery. However, if you set up alerts for dual delivery, the message security service will send an Alert to an address you specify, advising that a problem occurred with dual delivery.

What data is sent to dual delivery

The following table describes what messages are sent to the dual delivery server.

If the message is...	Dual Delivery will...
sent successfully to a registered user	send the message to the dual delivery server.
sent successfully to a non-registered user	not send the message to the dual delivery server.

If the message is...	Dual Delivery will...
sent successfully to a non-registered user (with catchall enabled)	not send the message to the dual delivery server.
sent successfully to an alias	send the message to the alias, unless the dual delivery server is Gmail, in which case the message is sent to the primary user instead.
sent successfully to a mailing list (which is set up in the message security service as an alias)	send the message to the alias, unless the dual delivery server is Gmail, in which case the message is sent to the primary user instead, like any other alias.
delivered from Quarantine	send the message to the dual delivery server, but without dual delivery mail header extensions.
delivered from an Archive.	not send the message to the dual delivery server.
sent successfully to an address in a domain alias.	send the message to the dual delivery server, unless sending to Gmail, in which case the message is sent to the same username in the primary domain instead.
sent successfully to a subdomain (with domain substripping enabled)	send the message to the dual delivery server, unless sending to Gmail, in which case the message is sent to the same username in the primary domain instead.
not sent successfully to the primary mail server	not send the message to the dual delivery server.
not sent successfully to the primary mail server, but spooled in Spool Manager	send the message to the dual delivery server.
delivered from Spool Manager	not send the message to the dual delivery server, since the message was already sent during spooling.

Alerts

When you enable dual delivery, be sure to set up Alerts so that you will know if any problems happen with dual delivery.

Important: Alerts are strongly recommended. If you do not use Alerts, you will not have any automated way to detect failed attempts to connect to the dual delivery server.

If a message is not successfully sent to the dual delivery server, neither the sender nor the recipient will receive any error message or resend the message, so an Alert message is vital so that you can detect and address any problem that happens with dual delivery.

To set up an Alert for Dual Delivery, use the following batch command:

```
modifyorg [orgname], dd_notify_on=[value], dd_notify_admin=[admin]
```

where [orgname] is the name of your email config organization, [value] is 0 to disable alerts or an integer that indicates the minimum number of seconds between alerts (to prevent excessive alerts during an incident), and [admin] is the address of a valid administrator in the email security service.

For example, if your domain is `jumboinc.com`, and your email config org is “JumboInc Email Config” then use the following command to enable alerts to an admin address that can occur as often as every five minutes:

```
modifyorg JumboInc Email Config, dd_notify_on=300,  
dd_notify_admin=admin@jumboinc.com
```

Using Dual Delivery with Gmail

You can set Dual Delivery to send mail to Gmail as a dual delivery server. You must still set up your domain and users in Gmail as well as the message security service and your primary domain.

To deliver mail to Gmail as a dual delivery server, choose “Send a copy to Google Apps Gmail” under Dual Delivery.

Note that while Gmail is supported, including any version of Google Apps Gmail that supports your domain, the Message Security & Discovery feature available with Google Apps Premier Edition (called “Postini Services” in the Google Apps dashboard) includes separate integration between Gmail and the message security service, and does not support dual delivery. To use dual delivery, update to the standalone version of the message security service.

When your dual delivery server is Gmail, the message security service makes a few special steps for increased compatibility:

- All messages sent to an alias are redirected to the primary address.
- All messages sent to a domain alias are redirected to the same user name in the primary domain.
- All messages sent to a subdomain (with domain substripping enabled) are redirected to the same user name in the primary domain.

For more information, see “Use Google Apps Gmail” on page 473.

Sample Uses

Some sample scenarios of ways to use Dual Delivery:

Pilot and Migration of Google Apps

In this scenario, an administrator is moving from an in-house mail server to Google Apps Gmail, but is beginning with a pilot program and slowly transitioning users to Gmail.

Initially, set the primary mail server as your mail server, and the dual delivery mail server as Gmail. Enable mail accounts for users and let the users try Gmail functions.

To continue the transition, switch the primary mail server to Gmail and the dual delivery mail server to the in-house mail server.

Note that if users connect to the dual delivery server, any outbound messages or replies will be sent from that server, so they will not be archived or stored on the primary server.

Using a Dual Delivery for Backup

In this scenario, an administrator has a primary mail server that handles all mail, but wants to have a backup server where users can access their mail in case of any kind of system failure on the mail server. This could also be used to provide remote web access to email for users away from the office.

The dual delivery server might be a Google Apps Gmail account set up to use the domain, or could be another off-site mail server configured to accept mail for the same domain and user list as the primary mail server.

Set up the primary mail server as usual, then add dual delivery to deliver mail to the dual delivery server.

Note that if users connect to the dual delivery server, any outbound messages or replies will be sent from that server, so they will not be archived or stored on the primary server.

Servers in Separate Locations

In this scenario, an administrator has mail servers in two locations that are geographically very distant, all on the same domain, and wants users to be able to connect to whichever mail server is closer to them.

In this scenario, set one mail server as the primary mail server, and the other as the dual delivery mail server.

It may also be possible to set up more complex scenarios, with different email config organizations and separate dual delivery server settings for each email config. be sure to plan this kind of scenario out carefully before changing any Delivery Manager settings.

Dual Delivery and Split Delivery

If you're using multiple mail servers, it may be important to note the distinction between *dual delivery* and *split delivery*.

In *dual delivery*, a copy of every message is sent to two separate servers. On a successful dual delivery, both mail servers receive a copy of a message. You can implement dual delivery in Delivery Manager using these instructions.

In *split delivery*, incoming mail is routed to one of two servers, based on your user settings. On a successful split delivery, only one mail server receives the message. Which server receives the message is based on the address of the recipient. Set up split delivery by creating multiple email config organizations, setting Delivery Manager for each email config to route to the appropriate server, and adding appropriate users to the user orgs under these email configs. Split delivery is not covered by this document; for information about split delivery, contact support.

You can use dual delivery and split delivery together, but plan your delivery settings carefully. For instance, you could set up two separate email configs to use split delivery, and then set up Dual Delivery on each email config, in order to deliver a copy of the message to Gmail. These configurations can become very complex, and are not covered by this guide. Be sure to set Delivery Manager settings for each email config appropriately.

Use Google Apps Gmail

You can set Google Apps Gmail as your primary server. You must still set up your domain and users in Gmail as well as the message security service.

To deliver mail to Gmail as a dual delivery server, choose "Use Google Apps Gmail" under Delivery Manager.

Note that while Gmail is supported, including any version of Google Apps Gmail that supports your domain, the Message Security & Discovery feature available with Google Apps Premier Edition (called "Postini Services" in the Google Apps dashboard) includes separate integration between Gmail and the message security service, and does not support dual delivery.

Use Cases

Use Google Apps Gmail has several common use cases:

- **Piloting Google Apps Premier and Education Edition:** You can use the feature to route email for a portion of your users to pilot Google Apps Gmail or as you migrate groups of users to Google Apps Gmail. To set up a split delivery pilot, create a new email config organization that uses Google Apps Gmail, then move pilot users to a user org under your new email config.

- **Optimizing delivery to Google Apps:** If you've already configured your email delivery to Google Apps Gmail, you can keep your current settings or use the new routing feature. With the new routing feature, Postini Delivery Manager automatically synchronizes with the Gmail servers and shares spam information for Gmail processing.

System Requirements

To use the Google Apps Gmail feature, you will need the following:

- Access to an Email Config organization.
- Any edition of Google Apps for your domain. You must set up your domain beforehand in Google Apps.
- If you want Postini to process outbound mail as well, this option is available only with Google Apps Premier or Education Edition and is configured in the Google Apps Control Panel.

Setup

Set up the new Gmail routing feature in the Administration Console, and then configure outbound and other settings (such as SPF and IP Whitelisting) in Google Apps control panel.

For a complete set up:

1. Set up your domain and users in Google Apps Control Panel.
2. Set up inbound mail with Use Google Apps Gmail in the Administration Console, under Delivery Manager > Edit.
3. Set up outbound mail in the Google Apps Control Panel if desired.
4. Set up other Google Apps mail settings, such as SPF and Whitelisting, if desired.

To use the new inbound Gmail routing feature, go to Delivery Manager > Edit in the Administration Console.



Mail flow will route to Gmail immediately after you save your changes, and you can change back just as quickly.

Note: If you activated the Postini for Google Apps service through the Google Apps control panel, this feature do not apply -- no action is required. The Postini service automatically takes care of routing to Google Apps in the background.

Setting up Delivery Manager

Authorized administrators can configure/edit Delivery Manager. Exercise caution whenever making changes, as errors may impact your mail flow.

The Delivery Manager Edit page is shown below. Changes made to this page take effect with the next new mail server connection to the message security service.

The screenshot shows the 'Delivery Manager - email-to-go Email Config' page. The 'Email Servers and Load Balancing' section is active, with the option 'Use my own email server (configured below)' selected. Below this is a table for configuring email servers:

Email Servers	% Conn.	Conn. Limit	Open Conn.
extestom5.postini.com	50		n/a
extestom2.postini.com	50		n/a

The 'Fail Over' section is also visible, with a table for alternate email servers:

Email Servers	% Conn.	Conn. Limit	Open Conn.

The 'Overflow' section has a checkbox for 'Allows fail over email servers to accept excess messages beyond primary connection limits. (This does not apply if you are using Google Apps Gmail as your mail server.)' which is currently unchecked.

The 'Dual Delivery Server' section has a checkbox for 'Enable Dual Delivery: Send a copy of all incoming messages to another mail server. Users must be registered on both mail servers. Recommended. Set up delivery alerts by batch commands. [Learn more...](#)' which is unchecked. Below it, the option 'Send a copy to this email server:' is selected, with an empty text input field.

Edit Delivery Manager

To navigate to the Delivery Manager edit screen, follow the steps below:

1. Click the Inbound Servers tab.
2. Select an email server config from the pull-down list.
3. Click the Delivery Manager link.
4. In the Overview page, click the Edit link in the gray bar.
5. In the Edit page, fill out the fields using the information from the table described in the next section.

6. Click Save.

Email Servers and Load Balancing

Following are descriptions of the fields for Delivery Manager:

Field Name	Value
Use Google Apps Gmail	<p>Send mail to Google Apps Gmail. This will send mail directly to Google Apps. Set up your domain in users in Google Apps as well as the message security server.</p> <p>For more information, see “Use Google Apps Gmail” on page 473.</p>
Email Servers	<p>List your email server(s). Use either the mail host names (i.e. mail.sample.com) or the IP addresses (255.255.255.255). Either are acceptable formats.</p> <p>If more fields are required, enter the first two and click Submit. After returning to the page, you will find additional fields. Repeat as necessary until all email hosts are listed.</p> <p>Once you enter the mail host name or IP address and click Submit, the change occurs <i>immediately!</i> A faulty entry will prevent email from being delivered to your servers, thus stopping email from coming into your organization.</p> <p>Important: You should test the email server after making any changes. You can test by validating that your email server is indeed receiving email from the message security service. Please contact support if you experience difficulty.</p> <p>We recommend listing the email servers in descending order, with the most robust email server listed first. This will make it easier for calculating the distribution percentages for each email server.</p>
% Conn.	<p>Once all mail hosts are listed and connection limits are set, you can apply a weighted distribution of traffic across the servers. Enter the percentage allocation for each email server. For example, if you have three email servers and you want the first email server listed to receive 50% of the inbound email traffic, enter 50 in the % Connections field. Leaving the remaining fields empty will distribute the inbound messages equally among the remaining servers. Assigning a distribution percentage for each email server is fine as long as it totals 100. You will receive an error if you assign a load distribution that totals more than 100 percent. Also, only whole percentages may be used.</p>

Field Name	Value
Conn. Limit	<p>If you know how many simultaneous connections your email server can accommodate, set that value in the designated field. Submit the page and return. You will find that the number of open connections will be displayed in bold- this is the real time number of open connections. This is useful to validate that you haven't set your Connection Limit too low. When an email server is experiencing an enormous amount of traffic, and the email server attempts to open enough connections to keep up with the requests, it can dramatically increase the likelihood of a server outage. Setting the Connection Limit in Delivery Manager will let the message security service act as an "edge server", preventing your server from being overwhelmed and possibly brought down.</p> <p>If you don't know your mail server connection limitations, we suggest you go to the "Host-specific data" available from the Delivery Manager-View page. If you configured your mail host properly, this will show the number of real time connections. Refresh the page several times over a few minutes to see how the number of connections fluctuates. Once you have an idea of the numerical range for open connections, set a limit that won't be too low to inhibit traffic, but isn't too high to allow your server to be disabled by excessive traffic. The email server software manual may also provide this information.</p> <p>Connection limits are instituted starting with the first new connection created after the limit is set. The limit is not imposed on existing connection when the configuration is made. So connections will slowly settle down to the limit as existing connections to the server complete.</p>
Open Conn.	Displays the number of currently open connections.

Fail over

Following are descriptions of field names for the fail over configuration.

Field Name	Value
Email Servers	<p>A fail over email server is one that is kept out of regular rotation for inbound email traffic. The fail over server is designated to enter the email rotation if ALL of the primary email hosts fails. Like the primary email server, it too can be set with a connection limit and even receive a percentage of email traffic. When all primary email servers fail and there isn't a designated fail over server, the email will either be spooled by the message security service (if you have Spool Manager available) or the messages will be deferred.</p> <p>Enter the host name or IP addresses of the mail servers that will be used in all primary email servers fail. See "Email Servers and Load Balancing" on page 476 for more information.</p> <p>The fail over configuration is one load-balanced set of servers, and not three full fail overs which fail over for each other in sequence.</p>
% Conn.	See previous table.
Conn. Limit	See previous table.
Open Conn.	See previous table.

Overflow

Click the check box if you wish to allow fail over email servers to accept excess messages beyond primary connection limits.

Dual Delivery Server

Following are descriptions of field names for the Dual Delivery configuration.

Field Name	Value
Enable Dual Delivery	<p>Check to enable dual delivery. If checked, a message will be delivered to a dual delivery server if the message was successfully delivered to a registered user.</p> <p>For more information, see "Dual Delivery" on page 468.</p>
Send a copy to Google Apps Gmail	Sets your dual delivery server as Google Apps Gmail.

Field Name	Value
Send copy to this email server	<p>Sets your dual delivery server as the MX record or IP address that you specify.</p> <p>Note that dual delivery servers do not support a failover server.</p>

Verifying Email Flow

With access to Delivery Manager Message Traffic Graphs, it is easy to determine what traffic is flowing through the message security service:

In the Administration Console, select the appropriate email server from the pull-down list or the Show Hierarchy window.

Click the Inbound Servers tab, then the Delivery Manager link. View the Message Traffic Graph:

- Gray Bars = Total attempted connections.
- Dark Red Lines = Failed connections.
- Light Green Lines = Spooled connections.
- Any other color lines = Delivered connections. See the legend on the graph for details about which line refers to which IP.

The graph will show whether or not traffic is flowing through the message security service. Each gray bar represents one minute.

The Current Activity box in the upper right-hand corner of the Delivery Manager overview page also shows statistics for the current email server config.

Delivery Manager Events

WARNING: Events relating to the Delivery Manager are usually mission-critical. If the Delivery Manager loses a connection with your email server, or the number of connections has been exceeded, it requires the attention of an email administrator. For this reason, we *STRONGLY URGE* you to configure your Delivery Manager alerts to be delivered to your mobile phone or pager.

Do not send alerts to your email account on your company email server. Standard mobile phones can receive text messages. Contact your wireless carrier to activate text messaging and to obtain the email address for your phone or wireless-enabled PDA.

Because of their critical nature, Delivery Manager events appear at the top of the "Events" list on the Overview page and are marked with a red flag.

It is common for the Delivery Manager events list to be empty because the message security service keeps Event records for two days. If no events have occurred during the past 2 days, the list will be empty.

The list of events can be sorted by type, date, source IP or impact. Clicking on any of the column headers will sort the list by that category. To sort or search for events that had the greatest impact, select messages over 100, 500, or 1000 and search. This will eliminate all low impact events and leave only the events over the value that was selected.

Delivery Manager Alerts and Event Types

Email Host Down

If there are 3 failed connections (with no successes) to one of your email servers within a 1-minute interval (checked every 15 seconds), an alert will be sent. If the email server is unreachable for an extended period of time, you will receive the initial alert, but no additional alerts are sent, assuming the initial alert hasn't ended yet (it's been continuous). One alert per event is sent out.

Organization Email Host Down

Same as Email Host Down, except that Organization Email Host Down means that all your email servers that have email filtered by the message security service are unreachable. A server may be unreachable because it is down or because there is a network outage between your server and the message security service.

Troubleshooting: Delivery Manager

What does it mean if Open Conn. = n/a when a Conn. Limit is set through the Inbound Server > Delivery Manager page?

This means that the process which lists the number of simultaneous connections died. Please contact Support to request that this be reset.

If no Conn. Limit is set, then the number of Open Conn. will not be listed.

My mail server has been brought down in the past due to too much incoming mail. Can the message security service be used to limit connections to my mail server, to prevent excessive connections from bringing it down?

Yes, you can use Delivery Manager to impose connection limits.

Chapter 21

Spool Manager

About Spool Manager

When your mail server becomes unavailable (for example, due to a crashed server or network connectivity problems), the Spool Manager stores or *spools* your mail for later release when your server is ready.

The Spool Manager is an optional feature available with some service configurations. Spool Manager is not available with Google Message Filtering. Contact your vendor or account manager for details.

Spool is allocated by total size of data, not by time. While some agreements or invoices include an estimation of the amount of time mail will be spooled, this is only an estimate. Spool Manager always operates on the data size of the spool, not duration of spooling events.

Note: You must set Spool Manager to “Automatic” if you want spooling to occur automatically when your mail server is unavailable. You should also configure alerts.

How Spool Manager Works

This section describes the spooling process, and how messages are spooled. Following is an overview the Spool Manager processes.

Spooling Set Up

You are allocated spooling space with Enterprise Edition. You may purchase additional spooling from your account manager.

Do the following when you add or delete an email config or purchase additional spool.

1. Allocate the total amount of spool across your email configs. Spool is allocated by total size of data, not by time.
2. Set up alerts for each email config.

3. Set the unspooling connection rate and delay interval, and turn on Spool Manager by setting the Spooling Mechanism and Unspooling Control to “Automatic” for each email config.

When a Connection Failure Occurs

When there is a connection failure that lasts longer than the spool delay interval, the Spool Manager sends an alert (if alerts have been configured), and begins to spool your mail (if you have set up automatic spooling).

Alternately, you can manually start spooling mail if the event is a planned outage such as a software or hardware upgrade.

Spool Manager continues to spool messages until the spool allocation is reached.

When a Connection Failure Ends

If Spool Manager was started manually:

1. Spooling must *be manually suspended* (stopped).
2. Unspool your mail using the Spool Manager, which delivers the stored messages to your email server.
3. After your traffic is unspooled, if you wish spooling to trigger automatically, then you need to set the Spooling Mechanism to “Automatic” for each email config.

If Spool Manager was started automatically:

1. Unspooling automatically triggers three minutes after the failure ends.
2. If the server becomes unavailable again, then unspooling stops and waits until three minutes after the server becomes available.
3. When unspooling completes, the Spool Manager is ready for the next connection failure.

When and How Messages are Spooled

The Spool Manager monitors connections to your mail servers and decides when to start spooling mail based on connectivity failures and the *spool delay* you configure. If there is sufficient mailflow through the system (about one connection every 15 seconds), and three connections fail within a 60 second window, the spool delay countdown begins. During this period, if the message security service receives sufficient mail flow, and every subsequent delivery attempt fails, spooling begins.

When mail is spooling, messages are accepted and stored for your use. The senders do not see any errors.

During spooling, messages are processed according to these guidelines:

- Messages that successfully passed through mail policies, junk mail filters, and virus scanning are spooled.
- Junk mail and virus-infected messages are not spooled—they are quarantined according to the normal filtering mechanism. Quarantined messages are accessible even if your mail server is down.
- The Blatant Spam Blocking filter rejects blatant spam messages as usual.

If your spooling space runs out, spooling stops, and incoming messages are deferred with the error: `451 Can't connect to domain.com - psmtip`. Most sending servers keep trying to send messages for 5 days.

Allocating Spool

You can allocate your total spool storage across all or some of your email configs. When you add or delete an email config, or purchase additional spool, you must adjust the allocation of the spool.

The spooling allocation can be changed at any time, even during spooling. The minimum increase in spool allocation is 0.1 MB (100 KB).

Spooling is allocated by disk space, not time. A large amount of data causes the spool to fill up more quickly.

To allocate spool, follow these steps. You must have permission to access to the Account level of the hierarchy.

1. You must first select the Account. You have two options:
 - In Orgs and Users tab, choose your account from the Choose Org pulldown list.
 - Click the **Show Hierarchy** link in the orange menu bar, and click the link to your account.
2. Go to Inbound Servers > Spooling. Your total amount of spool is displayed at the top of the page.

Note: If you do not see the Spool Allocation page, you may not have your account selected. See step 1 for details.

Spool Allocation - Jumbo Inc. Corporate Account			
View Edit			
Spool Allocation			
Total Allocation		0	
Unallocated		-100 MB	
Email Configurations	% of Allocation*	Size	Used
New York Email Config	0	100 MB	0
Chicago	0	0	0
TOTALS	0.0%	100 MB	0
<small>*percent values are approximate</small>			

3. Click the **Edit** link gray bar. Distribute the total amount of spool across your email configs. Spool allocation can be specified in whole megabytes or in decimals, such as 0.2 MB.
4. Click **Submit**.

Configuring the Spool Manager

You typically configure or change the Spool Manager settings when you first set up spooling, add or delete an email config, or purchase more spool storage. You also use the Spool Manager Edit page to manually start and stop spooling, and to unspool your messages.

Two situations require immediate attention:

- You must suspend spooling when your mail server begins to function normally again. Otherwise, Spool Manager continues to spool messages until the spool allocation is reached.
- After you suspend spooling, you must have already configured Spool Manager for automatic unspooling, or you must manually initiate unspooling to receive your spooled messages. Otherwise, messages remain in the spool, even when your mail server has returned to normal and is accepting messages.

To Manage the Spool Manager Settings:

1. If you have not already done so, allocate spool to your email configs. See "Allocating Spool" on page 483 for details.
2. Select an email config from the Choose Org menu located in the upper-left corner of any page.

3. Click the **Spool Mgr** link in the Inbound Servers menu bar, then click the **Edit** link. The Edit fields are described below.
4. Click **Submit** to save your changes.

Spooling Mechanism

Spool initiation can be in one of three states: Automatic, Start Manually, and Suspend.

Automatic	<p>The Spool Manager starts spooling automatically when there is an outage. See “Spool Delay” below for more information.</p> <p>Note: You must set Spool Manager to automatic if you want spooling to occur automatically. This is not the default.</p>
Start Manually	<p>You may start spooling messages while upgrading server software, hardware, network, or during any other process that might interrupt delivery of email messages. Spooling begins once you click the Submit button, and continues until you select set the Spooling Mechanism to Suspend. (Spool Manager doesn't issue alerts for manually initiated spooling.)</p> <p>Manual Spooling must be suspended before you can unspool.</p>
Suspend	<p>Spooling is turned off. Spooling will not occur even if your email server is down.</p>
Spool Delay	<p>The spool delay, in conjunction with connection failures, determines when spooling starts. See “How Spool Manager Works” on page 481 for more information on when spooling starts. The spool delay choices are 15, 30, or 60 minutes.</p> <p>In order to prevent spooling from occurring during normal network fluctuations, the minimum spool delay is 15 minutes (a setting of less than 15 minutes may unnecessarily trigger spooling when network is temporarily busy or slow).</p> <p>When there's a failed connection during the spool delay (before spooling starts) mail is deferred with an SMTP error 451 Can't connect to <i>domain.com</i> - psmtpt. According to SMTP protocol, mail defers for 5 days before bouncing back to sender.</p>

Unspooling Control

Unspooling is the process of delivering the spooled messages. Unspooling can be controlled either automatically or manually.

Automatic	<p>While you have mail spooled, Spool Manager polls your server one time per minute until it has been available for 3 subsequent minutes. Then, it automatically stops spooling and unspools your mail.</p> <p>If, while automatically unspooling, your mail server becomes unavailable for 5 minutes, then automatic unspooling stops, and starts polling for server availability again.</p> <p>Note: If automatic spooling is enabled, it triggers normally when unspooling is interrupted.</p>
Manual	<p>While you have mail spooled, you can manually start and stop unspooling using the following two settings:</p> <p>Start Unspooling: Manually starts unspooling</p> <p>Stop Unspooling: Manually stops unspooling</p> <p>The Start and Stop settings are available only when Manual Spooling is configured and you have spooled mail.</p>

Unspooling Connection Rate

The Set Rate is the number of connections dedicated to unspooling stored messages. The Set Rate should deliver messages at a volume that your mail servers can safely manage. We recommend allocating no more than 100 connections, or a maximum of 15% of the sum of your connection limits, whichever is lower. A higher number of connections may result in a greater burden on your mail server, and risk causing a mail server outage.

Interpreting the Spool Manager View

The Spool Manager View page shows your spooling status and activity.

Displaying the Spool Manager View

1. Go to the Inbound Servers page and select an email config from the Choose Org menu.
2. Click the **Spool Mgr** link in Inbound Manager menu bar.

The View page also displays Spool Manager settings. All the settings are editable from the Spool Manager - Edit page (other than Allocation, which must be altered by amending your contract).

Spool Remaining	Remaining space available for spooling for this email config.
Duration	The amount of time since spooling was last activated.
Spool Status	<ul style="list-style-type: none"> • Not Provisioned: Customers have not purchased spooling services. • Suspended: Spooling is disabled and will not engage even if there's a server or network outage. • Standing By: Spooling is activated and monitoring the number of failed connections. • Spooling: Spooling process is in progress. • Unspooling: Spool Manager is in the process of delivering messages from spool storage. Once unspooling is complete, the status returns to Standing By.
Spooling Delay	See "Spool Delay" on page 485.
Allocated Spool	See "Allocating Spool" on page 483
Unspooling Rate	"Unspooling Connection Rate" on page 486.

Alerts and Events for Spool Manager

Alerts

We **highly recommend** you set up alerts to notify you of spooling activity. You can set up alerts for the following Spool Manager actions:

- Spool Initiated
- Spool Quota Thresholds (50%, 75%, 90%, 95%, 99% of full)
- Spool Full
- Unspool Initiated
- Unspool Complete

See for "Setting Up Alerts" on page 489 for information on configuring alerts.

Any events relating to the Spool Manager are always mission critical. For this reason, you should configure Spool Manager alerts to be directed to your mobile phone or pager.

WARNING: Be sure your alerts are configured to send the notification to an account on your wireless device and not your email account (as all messages to this account could be spooled).

Events

Spool Manager has one event, Organization Email Host Down, which indicates that all of your email servers that have email filtered by the message security service are unreachable. For more information on this event, see “Connection Manager Events” on page 462.

Troubleshooting: Spool Manager

My mail server connection is now working and I still have spooled mail. Why hasn't my mail automatically unspooled?

If your Unspooling Control is configured to manual, the unspooling process must be manually initiated (even after your mail servers are reestablished). See “Unspooling Control” on page 486 for more information.

If your Unspooling Control is configured to automatic, your server has not been available for three successive minutes.

Why is my email is being spooled even though my mail server is running?

You have an intermittent or slow network connection. That is interpreted by the Spool Manager as a failed mail connection. Increase your spool delay period; see “Spool Delay” on page 485 for more information.

Chapter 22

Administrator Alerts

About Alerts

The message security service can send you an alert whenever an Inbound Servers event is triggered.

Alerts are a key tool in tracking the health and status of your email flow. Every time the Connection Manager automatically blocks an attack, the Delivery Manager detects your email server is down, and with each Spool Manager action, an event is triggered.

Alerts are designed for flexibility; you can send urgent notifications to text-enabled wireless devices, and non-urgent notifications such as Spam Attacks or Directory Harvest Attacks to an email account for reference.

Each alert is brief enough for delivery to a mobile device, but contains useful information about the event.

For instance, a Directory Harvest Attack alert will look like this:

```
SUBJECT:
DIRECTORY HARVEST ATTACK: name of the affected email config
BODY:
2002/04/10 23:10:33 GMT
from 109.219.82.126
block '550 mailbox unavailable - psmtip'
```

Remember to configure the alerts for each email config. Delivery Manager and Spool Manager alerts should be configured to send notifications to a wireless device or an external address, since you cannot receive Alerts to your main address when the server is down.

Setting Up Alerts

You can configure multiple recipients to receive alerts. This gives you the flexibility of spreading responsibilities across your staff, and to send alerts to different email accounts.

WARNING: When your service is activated, alerts are not configured. *It is vital that you set up alerts for each email config so that you will receive proactive notification when urgent server events occur.*

Set up Alerts

3. In the Administration Console, choose an email config from the Choose Org pull-down list.
4. Click Inbound Servers > Alerts.

Alerts - New York Email Config			
	Click here to Configure	Click here to Configure	Config More >>
Connection Manager			
Email Bomb	<input type="checkbox"/>	<input type="checkbox"/>	
Directory Harvest Attack	<input type="checkbox"/>	<input type="checkbox"/>	
Virus Outbreak	<input type="checkbox"/>	<input type="checkbox"/>	
Spam Attack	<input type="checkbox"/>	<input type="checkbox"/>	
Delivery Manager			
Organization Email Host Down	<input type="checkbox"/>	<input type="checkbox"/>	
Email Host Down	<input type="checkbox"/>	<input type="checkbox"/>	
Spool Manager			
Spool Initiated	<input type="checkbox"/>	<input type="checkbox"/>	
Spool Quota Thresholds (50%, 75%, 90%, 95%, 99% of full)	<input type="checkbox"/>	<input type="checkbox"/>	
Spool Full	<input type="checkbox"/>	<input type="checkbox"/>	
Unspool Initiated	<input type="checkbox"/>	<input type="checkbox"/>	
Unspool Complete	<input type="checkbox"/>	<input type="checkbox"/>	

5. Click the “Click Here to Configure” link to configure a recipient.

Enter the name and address of the recipient. Mobile devices such as pagers, mobile phones, and wireless PDAs can receive email, and should be used as the address for your recipients.

Alert Destination - Acme Email Config	
An alert can be delivered to any email address including any wireless device that is text-enabled.	
<p>Name Give this destination a name.</p>	<input type="text" value="Admin email/device"/> <small>(example: Mark's pager)</small>
<p>Address Enter an email address where alerts will be sent. It's HIGHLY RECOMMENDED that Delivery Manager and Spool Manager alerts go to a mobile device. Check with your phone carrier to validate the email address, and test the device.</p>	<input type="text"/> <small>(example: 6505551212@sprintpcs.com)</small>

6. Enter the mobile device's email address in the destination field as you would for the primary email address. For example, a mobile address might be *cell_phone_number@your_carrier.com*.
 - a. Send a regular text message to your device to test that you have the correct address and that your device is text-enabled.
 - b. If your device does not have text-messaging enabled or if you do not know your address, contact your wireless provider.
7. Click the “Configure More” link to add more recipients. There is no limit to the number of recipients.
8. Click the Submit button to return to the Alerts page.
9. Check the alerts that you want that recipient to receive. See “Alert Descriptions” on page 491 for details on events, or click the Alert Descriptions link at the bottom of the page.

Important: We strongly recommend, at a minimum, you set up alerts for the Delivery Manager “Organization Email Host Down” event, and the Spool Manager events (if your service package includes Spool Manager).

10. Click the Submit button.

Repeat this procedure for each email config.

Alert Descriptions

This section describes the alert for Connection Manager, Delivery Manager, and Spool Manager. One alert is sent for each event is triggered.

Connection Manager Alerts

Configuring Connection Manager with the most sensitive setting means that more blocks will be put in place. The more sensitive the setting, the less traffic is necessary to trigger a Connection Manager event, and therefore, an alert. See (“ Connection Manager” on page 453) for more information.

There’s no action you need to take in response to a Connection Manager event. These types of events are very common, and may generate a large number of alerts. You may decide not to set up alerts for Connection Manager events unless specifically conducting analysis on attacking IP or collecting other statistical data.

Email Bomb

Email bombs are denial of service attacks where a volume of large, identical messages are sent. Connection Manager will identify spikes in message volume that violate standard variance in message traffic. Conditions where like messages are sent repeatedly, messages are of particular size characteristics, and the ratio of suspect to valid email is high will result in the classification of an email bomb.

Directory Harvest Attack	A Directory Harvest Attack is a series of delivery attempts that result in 550 errors. Your email server will respond to each request, issuing potentially thousands of 550 errors. If the spammer happens to reach a valid address, a spam message may be delivered, and the address is logged as valid. Sensitivity allows a variance in the ratio of valid to invalid messages per session or per source IP. Very low sensitivity will <i>not block</i> the IP if there is a single valid address in the session. Very high sensitivity ranges up to a ratio of 1:5 valid addresses.
Virus Outbreak	Virus filtering must be turned on in order for Connection Manager to identify a virus attack. A virus attack is tracked by monitoring both the ratio of virus infected messages to valid email, as well as the total volume of virus infected messages from the IP during a specific interval. If the ratio changes in a statistically significant manner, the IP will be blocked temporarily.
Spam Attack	Spam filtering must be turned on in order for Connection Manager to identify a spam attack. A spam attack is tracked by monitoring both the ratio of spam to valid email, as well as the total volume of spam from the IP during a specific interval. If the ratio changes in a statistically significant manner, the IP will be blocked until the attack stops. For each Connection Manager event, an alert is sent out. This means for a Spam Attack, for each IP detected and/or block, an alert is sent.

Delivery Manager Alerts

Following are the Delivery Manager events which trigger alerts. See “ Delivery Manager” on page 465 for more information.

Email Host Down	If there are 3 failed connections (with no successes) within a 1-minute interval (checked every 15 seconds), an alert will be issued. If the email server is unreachable for an extended period of time, you will receive the initial alert, but then you wouldn't receive an additional alert, assuming the initial alert hasn't ended yet (it's been continuous). One alert per event is sent out.
Organization Email Host Down	Similar to Email Host Down, Organization Email Host Down means that all your email servers in the email config are unreachable. A server may be unreachable because it is down, or because of temporary network issues between the message security service.

Spool Manager Alerts

Following are the Spool Manager events which trigger alerts. For information on see, “ Spool Manager” on page 481. Spool Manager is an optional feature. Please contact your account manager for information on your service package.

Spool Initiated	Spooling has initiated automatically for incoming mail.
Spool Quota Thresholds	Spool has reached a threshold for alerts. You can set the alerts threshold to 50%, 75%, 90%, 95%, and 99% of the allocated spool.
Spool Full	The allocated spool size has been reached and email is being deferred. No email is lost or bounced. The sending server will continue attempt message delivery.
Unspool Initiated	Once your email servers are functioning correctly, you must have already configured Spool Manager for automatic unspooling, or you must manually unspool messages in the Spool Manager. This alert is triggered when stored messages in the spool have begun to be delivered to your email hosts.
Unspool Complete	The stored messages in the spool have been completely delivered to your email hosts.

Chapter 23

IP Ranges and Security

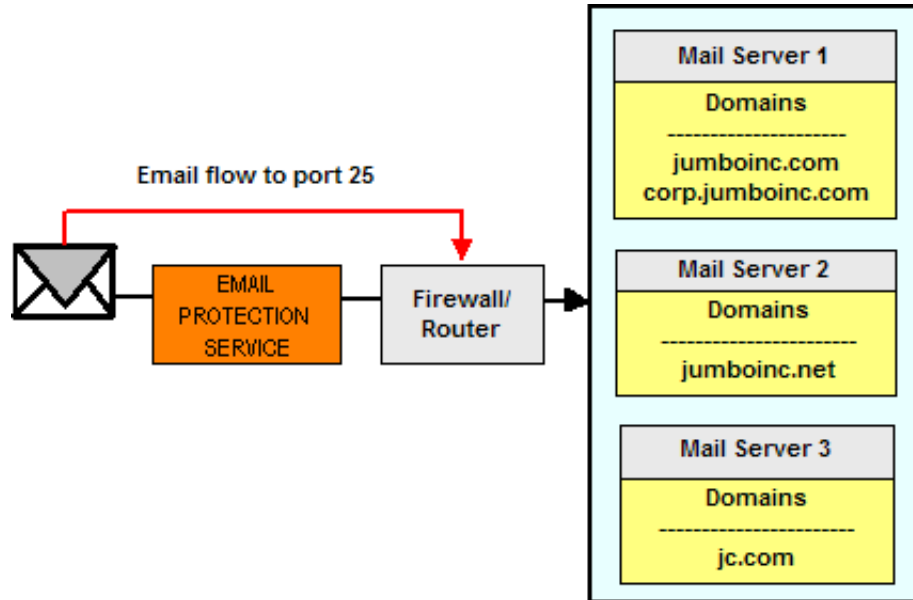
About IP Ranges and Security

This chapter contains detailed information about secure mail delivery, including network and IP information for protecting your mail servers. Unexpected spam is sometimes the result of direct connections to your mail server. If a malicious sender is able to find your mail server and connect directly, your users may receive junk email. This chapter also includes information on protecting your servers from spoofing using the RPF page (see “RPF: Tools to Help Prevent Spoofing” on page 498).

Setting Up Secure Mail Delivery

Some senders of virus and spam do not follow DNS standards for selecting MX records. They send an email to the highest numbered server, or randomly pick a server. Sometimes spammers specifically target mail servers using low-priority DNS MX records or by directly looking up a server using a common naming scheme, `mail.yourdomain.com`.

This diagram shows email flow through the message security service, and email flow circumvented by spammers.



Configuring for All Domains

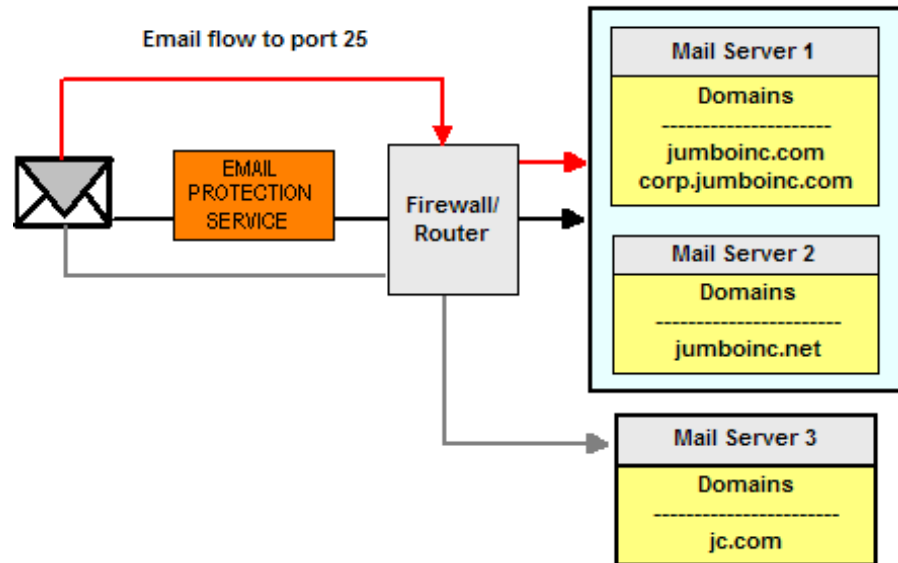
If all of your domains are registered in and routing through the message security service, we strongly recommend the following: Configure your email server or firewall to refuse port 25 traffic *except* for the IP ranges of the message security service, and portable address range. See "IP Range" on page 498 for this information.

This configuration actively prevents actual traffic from bypassing the message security service instead of simply making the mail server harder to find. In the unlikely event that server processing is impaired, sending email servers will queue up their messages until processing resumes (no email is lost). During this time, you may wait until the message security service is processing properly, or you can temporarily reconfigure your mail server to accept email from any sending server. If you reconfigure your system, however, email that includes potential spam and viruses will be delivered to your users.

Configuring for Partial Domains

Configuring your email server or firewall to accept email traffic from only IP ranges for the message security service is suitable *only* for environments where all domains are registered. If not all of your domains are registered in and routing through the message security service, this solution will not work.

For example, in the diagram below, the domain `jc.com` is not configured for email flow through the message security service. If you configure your email server or firewall to accept email traffic from only the appropriate IP ranges, all email for the domain `jc.com`, which is not routed through the message security service, would bounce.



In this case, the recommendation is:

- Remove the DNS MX records—only for the domains routing to the message security service—that point directly to your email server. In the event that servers are down, sending email servers will queue up messages for later delivery.
- Pick another name for your mail server besides `mail.yourdomain.com`, since spammers will sometimes guess that your mail server is named `mail.yourdomain.com` and use this to avoid filtering.

WARNING: These recommended steps only obfuscate your mail server. They do **not fully protect it**. To protect your mail server, add all domains to your hierarchy and then use the suggestions above in “Configuring for All Domains” on page 496.

IP Range

The following are the IP ranges for the email protection service systems. Note, for system 20 customers, both sets of IP ranges are applicable.

System	IP Range	CIDR Range	IP/Subnet Mask Pair
5, 6, 7, 8, 20	64.18.0.0 - 64.18.15.255	64.18.0.0/20	64.18.0.0 mask 255.255.240.0
9	74.125.148.0 - 74.125.151.255	74.125.148.0/22	74.125.148.0 mask 255.255.252.0
10	74.125.244.0 - 74.125.247.255	74.125.244.0/22	74.125.244.0 mask 255.255.252.0
11, 20, 200, 201	207.126.144.0 - 207.126.159.255	207.126.144.0/20	207.126.144.0 mask 255.255.240.0

To determine the system for your account:

Your system number is shown the URL when you log in to the Administration Console or Message Center. The system number is prefaced by “ac-s” or “mc-s”, for example:

URL displayed for an account on System 8 when logged in to the Administration Console:

```
https://ac-s8.postini.com/exec/adminstart?
```

URL displayed for an account on System 200 when logged in to the Message Center:

```
https://mc-s200.postini.com/app/msgctr/junk_quarantine
```

RPF: Tools to Help Prevent Spoofing

Note: The RPF feature is available for *Google Message Security* customers only. If you are not a Google Message Security customer and want to set up IP Lock, see “Setting Up IP Lock with Batch Commands” on page 505.

The RPF page enables you to manage *Receiver Policy Framework* settings. From this page, you can specify whether incoming mail from a specific domain must be sent via end-to-end TLS, and you can prevent or allow spoofing by checking the SPF records or IP address of a domain, and you can set up DKIM policies.

The RPF page gives you the advantage of setting up your security settings with more granularity. This means you can select individual domains for SPF check rather than set up SPF check for **all** of your all inbound mail. You can do this with the *Inbound sender-specific security* settings on the RPF page.

Note that *Inbound default security* settings enable you to set up security settings globally for all of our your incoming mail, while *Inbound sender-specific security* settings enable you to specify individual domains for these security settings.

Important: Only registered users are eligible for RPF protection with SPF, IP Lock, and DKIM settings, so these RPF filters will ignore unregistered recipients. However, End-to-End TLS requirements are still applied for unregistered recipients.

For instructions, see “Managing Settings for RPF” on page 500.

About Spoofing

Spammers can easily spoof the sender address to deceive recipients into believing a message was sent from a specific domain. Most junk messages sent in this way will be easily caught by spam filtering. However, you can configure the message security service to accept messages within your domain from only a specific server or group of servers. This prevents other servers from spoofing the sender domain.

You may not always want to stop spoofing. Many legitimate, desirable messages are spoofed. Travel web sites, news forwarding by email, automated system alerts, greeting cards and many other online services often use spoofing as a way to send mail which seems to come from another sender.

However, when junk email messages are reaching your users because the sender is falsifying a domain name in your Approved Senders list, you can configure the Administration Console to protect against this in the following ways:

- **Remove the Approved Sender.** You may have a domain on your approved senders list which leaves you vulnerable to spoofed junk email. If you do not need the approved sender, it is often easiest just to remove that entry from the approved senders list. See “Approved and Blocked Sender Lists” on page 387.
- **Require TLS.** You can use the *Inbound sender-specific security* page to specify that incoming mail from a domain must be sent via end-to-end TLS. See “Managing Settings for RPF” on page 500. Note that your email server must be configured for TLS to receive messages via TLS.
- **Check the SPF records of a domain.** The *SPF Check* setting helps protect against domain spoofing of incoming emails (for your registered users only). With this feature turned on, the message security service checks the SPF record to determine whether a message comes from an authorized mail server for that domain. Messages are accepted or rejected based on the policy that you specify in the SPF configuration for the domain. You can set up SPF Check globally for all of your incoming mail, but to help avoid false positives we recommend that you set up SPF Check using the *Inbound sender-specific security* page, which enables you to specify individual domains when configuring this security feature. See “Managing Settings for RPF” on page 500.
- **Set up IP Lock.** If a domain is vital to your business and cannot be removed from the approved senders list, you can use the *Inbound sender-specific security* page to set up IP Lock (for your registered users only). For instructions, see “Managing Settings for RPF” on page 500. See also “Setting Up IP Lock with Batch Commands” on page 505.
- **Configure DKIM policies.** Spammers can forge the From address on mail messages so that the spam appears to come from a user in your domain. To help prevent this type of abuse, a digital “signature” can be added to the header of outgoing mail messages. Recipient domains can then check the domain signature to verify that the message really comes from that domain and that it has not been changed along the way. The DKIM policies for an org decide what to do with inbound mail (for registered recipients only) in each of three unsuccessful cases -- an invalid DKIM signature, a missing DKIM signature, and “temporary validation failures” (for example, DNS lookup failures).

Managing Settings for RPF

Note: This feature is available for *Google Message Security* customers only.

The RPF page enables you to manage the following settings:

Inbound default security - This provides links to *global* settings for SPF, TLS, and DKIM settings. These settings apply to all of your inbound mail, regardless of the sender domain.

Inbound sender-specific security - This enables you to configure TLS, SPF, IP Lock, and DKIM settings for the individual domains that you specify.

To configure *Inbound sender-specific security* for a domain, follow these steps:

1. Log in to the Administration Console, and select an Email Config organization.
2. Click the **Inbound Servers** tab.
3. Click **RPF** in the blue bar at the top.

This opens the Inbound RPF page:



4. Click **Add domain**.

This opens the *Inbound sender-specific security* page, where you can specify individual domains when setting up security features.

5. In the Domain field, type the domain name -- for example, *solarmora.com*.
6. To complete your configuration, see "Guidelines for Configuring Inbound Sender-Specific Security" on page 502.
7. Click **Save**.

Guidelines for Configuring Inbound Sender-Specific Security

The *Inbound sender-specific security* page includes the following settings:

- **TLS** - If you select the TLS check box, all messages from this domain must be sent via end-to-end TLS. The recommended setting on the TLS page is *Send by SMTP or TLS*.
- **SPF** - (*Google Message Security* customers only) Depending on whether the SPF response type is Fail or SoftFail, you can set the disposition to Reject, Quarantine, Disable Approved Sender List, Perform IP Lock test, or Pass - Skip IP Lock test. For instructions on setting up SPF, see “Enabling SPF Check” on page 503. Note that this setting protects your registered users only.
- **IP Lock** - (*Google Message Security* customers only) If you select the IP Lock check box, select an IP address for both the Start Range and End Range, and optionally include a description. Note that you can add as many ranges as needed. Choose a disposition -- for example, *Pass IP Lock test* if an IP is within the specified range, or *Reject* if an IP is not within the specified range. See also “Setting Up IP Lock with Batch Commands” on page 505. Note that this setting protects your registered users only.
- **DKIM** - If you select the DKIM check box, you can choose a disposition of *ignore*, *blackhole*, *quarantine*, or *reject* for inbound mail in each of three unsuccessful cases -- an invalid DKIM signature, a missing DKIM signature, and “temporary validation failures” (for example, DNS lookup failures). Note that this setting protects your registered users only.

Follow these guidelines for Inbound sender-specific settings:

- The TLS setting takes precedence over the SPF, IP Lock, and DKIM settings. If you select the TLS check box, all messages from this domain must be sent via end-to-end TLS, regardless of the configuration you choose for SPF, IP Lock or DKIM.
- If there's a published SPF record for a specific domain, the SPF Check feature enables you to take advantage of this. It helps you prevent spoofed emails for that domain from reaching your users' inboxes.
- Many domains do not set up SPF records. If you want more granularity and control to account for this, we recommend that you set up the SPF Check feature using the *Inbound sender-specific security* page. This page enables you to set up the feature by specific domain rather than as a global (default) setting for all of your inbound mail.
- With SPF Check, there's a risk of false positives, which may cause legitimate messages to be bounced (depending on the disposition selected for SoftFail). This is partly because SPF Check depends on the settings within the sender's SPF record. For example, if the sending company has a contract with a third party to send a survey on behalf of the company, and the company's IT department fails to update the SPF record, then legitimately spoofed messages may be rejected.
- For the SPF Check SoftFail response type, we recommend that you use the default disposition of Disable Approved Sender List. If you change this setting to Quarantine, your users may be required to check their Quarantine much more often.
- SPF Check takes precedence over the IP Lock and DKIM features, and Connection Manager takes precedence over SPF Check. For example, before SPF Check has an effect on a message's disposition, Connection Manager checks for potential malicious IP addresses and domains, as well as for SMTP attacks. For more details, see "Connection Manager" on page 453.
- If junk emails are reaching your users because a sender is falsifying a domain name in your Approved Senders list, and if this spoofed domain is vital to your business and can't be removed from the approved senders list, we recommend that you set up an IP lock on this domain.
- More follow-up maintenance may be needed if you use IP Lock. For example, to keep the list of IP addresses up-to-date, you may need regular email exchanges with trusted partners, as well as with colleagues within your organization. Also, if you are using the IP lock list to prevent a sender from spoofing a domain in your Approved Senders list, determine if this domain is still vital to your business. If it is no longer a vital business domain, consider removing it from the IP lock list.

Enabling SPF Check

Note: This feature is available for *Google Message Security* customers only.

Some organizations publish Sender Policy Framework (SPF) records to help reduce email spoofing of their domains. SPF records include a range of IP addresses that are authorized to send mail on a domain's behalf. To help reduce the chance that your users will receive spoofed emails, you can enable the SPF Check feature at the Email Config level in the Administration Console. By default, this feature is turned off.

Important: Note that *Inbound default security* settings enable you to set up SPF Check globally for all of our your incoming mail, while *Inbound sender-specific security* settings on the RPF page enable you to specify individual domains for these security settings. If you want more granularity and control, we recommend that you set up SPF Check **by domain** using the *Inbound sender-specific security* settings. See "Managing Settings for RPF" on page 500.

The SPF Check feature displays four possible response types and a disposition for each response:

- **Fail** - This response type means the domain owner believes the message is unauthorized -- in other words, spoofed or forged. The default disposition for this response is Reject. (The disposition for this response type is not configurable).
- **SoftFail** - This means the domain owner believes the message is unauthorized, but the owner is not completely sure and doesn't want messages rejected on this basis alone. The default disposition for this response type is Disable Approved Sender List. This disposition means all messages in SoftFail will be filtered for spam, even those that are on the approved senders list. Other possible dispositions include Reject, Quarantine, and Ignore, but the recommended setting is Disable Approved Sender List.
- **Pass** - This means the SPF Check passed successfully. The default disposition for this response type is Ignore.
- **None/Neutral** - This means no SPF record was found during the SPF Check. The disposition is No policy - Ignore.

To enable SPF Check, follow these steps:

1. Log in to the Administration Console, and select an Email Config organization.
2. Click the Inbound Servers tab.
3. Click **SPF** to open the *Inbound SPF* page.
4. Select the **Enable SPF Check** check box.

Important: This is a global setting that will check SPF records for all incoming mail. If you want more granularity and control, we recommend that you set up the SPF Check feature **by domain** using the *Inbound sender-specific security* settings on the RPF page. See "Managing Settings for RPF" on page 500.

5. Choose a disposition for the Fail response type; for example, **Reject** or **Quarantine**.
6. For the SoftFail response type, select **Disable Approved Sender List** (recommended).
7. Click **Submit**.

Setting Up IP Lock with Batch Commands

Allowed IP configurations (IP Lock) can be set up using Batch commands.

Note: If you are a *Google Message Security* customer, you can also use the RPF page to set up your IP Lock configuration.

IMPORTANT: When adding an IP range using the *iplock add_range* command, new ranges are not enabled by default (the default mode is off). To turn the IP Lock rule on, you must set the command for *mode=on*. See the instructions below.

Run the following command to enable your IP range:

```
iplock modify org=<orgtag>, domain=<domain>, mode=on
```

For instructions and details on submitting batch commands for IP Lock, see the following sections in the *Batch Reference Guide*:

- `iplock add_range`
- `iplock delete`
- `iplock delete_range`
- `iplock display`
- `iplock set_disposition`

You can also set up IP Lock via the RPF page. See “Guidelines for Configuring Inbound Sender-Specific Security” on page 502.

Chapter 24

Configuring Outbound Servers

About Outbound Services

When Outbound Services is enabled and configured, mail from users is routed to the message security service for filtering before it reaches external contacts. You can use outbound mail processing to protect your customers and partners from virus-infected messages, enforce your corporate email policies and compliance standards, and collect information about your outgoing mail traffic.

Outbound mail processing is an optional feature. For more information about your service package and options, contact your account manager or vendor.

Outbound mail filtering is very similar to inbound mail filtering. Filters include:

- Virus Blocking (see “Virus Blocking” on page 311)
- Attachment Manager (see “About Attachment Manager” on page 403)
- Content Manager (see “Content Manager” on page 329)
- Legal Compliance Footer

Outbound Services requires special setup. For full information about how to set up Outbound Services, see the *Outbound Services Configuration Guide*.

Outbound Concepts

With Outbound mail processing, you will redirect your mail to be filtered through the message security service. All outgoing messages will be forwarded to the message security service, which then filters the message and connects separately to each recipient of the mail.



Mail is not stored in the message security service. When your mail server sends mail to outbound services, the message security service makes an immediate connection to each recipient, and does not send back a success to your sending mail server until all recipients have received or rejected the message.

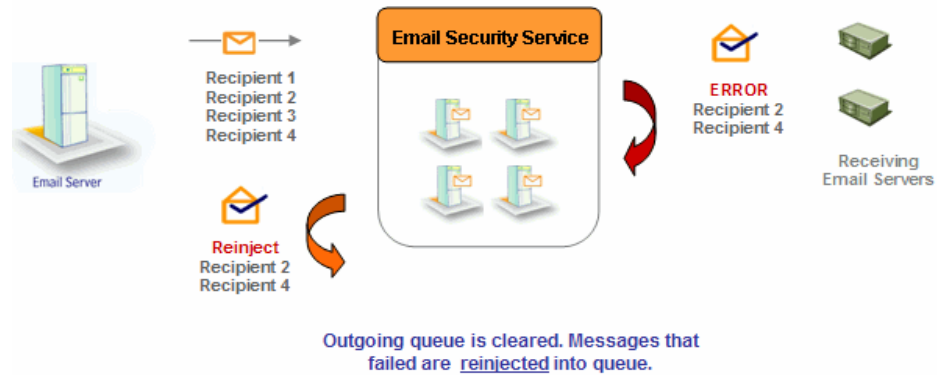
In rare cases, Outbound mail processing may need to send mail back to your server, then sent back to the message security service. This is called *reinjection*. You'll need to set your mail server to accept mail from the message security service and send it out again. You'll need to enable reinjection before you can set up Outbound mail flow. Reinjection is explained in further detail below.

There are four steps to configure outbound mail service. First, you'll configure reinjection. Then, optionally, you'll adjust your sending server's SMTP timeout to 15 minutes. Then, list your server's IP address in the Administration console. Once these steps are complete, redirect your mail flow by setting up a *smarthost* on your mail server to route mail through the message security service.

Setting up outbound is different for each mail server. For instructions specific to your mail server, see the *Outbound Services Configuration Guide*.

About Rejection

Reinjection is the process of relaying a message back to the customer's server when it cannot be delivered due to conflicting SMTP errors after DATA. The reinjection host is often the same server as the outbound server, but this is not required.



The reinjection host must be configured to allow the message security service IP addresses to relay for external recipients. You may have already set up your mail server and firewall to accept messages from the message security service, but reinjection requires further access. Your reinjection server must accept mail from the message security service and send it out again. This is called a *private relay*.

WARNING: Be careful when you set up a private relay. If you allow all IP addresses to pass mail through your server, your mail server will become an *open relay*. This leaves your mail server vulnerable to hijacking from malicious senders.

Reinjection Scenarios

Because of the way SMTP standards work, a mail relay can only send back a single result for each SMTP command. If you send mail to multiple recipients, the message security service may not be able to send a single accurate response to the DATA command. This occurs if some recipient servers accept the message and others reject the message. Specific examples are given below.

Before the SMTP DATA command, individual recipients can be accepted or rejected. However, after the sender transmits the DATA command, only one response code can be returned to reject or accept the message for all previously accepted recipients. If this happens, the message security service will send a success, then reinject the message again, using only the recipients who were unable to receive mail the first time.

Outbound reinjects the message to the reinjection server at your company, and the reinjection machine resubmits the email message to the message security service for processing. When your server attempts to deliver the reinjected message, Outbound treats the resubmitted message as a new message and scans the message again. Since only failed messages are reinjected, this will usually fail, but it's possible that some messages may need to be reinjected again. Because fewer messages are reinjected every time, this cannot result in an endless loop.

Reinjection happens very rarely. Less than 0.1% of messages are reinjected. A message is reinjected only if:

- Outbound is managing connections to multiple receiving servers.
- Some recipient servers accept the message address (in response to the RCPT TO command) but reject the message contents (in response to the DATA command).
- Different recipients give different types of responses (250, 400 class errors, and 500 class errors).

This type of situation may occur if the receiving server runs out of disk space or crashes after accepting a mail recipient. Reinjection is only necessary if you have successfully gotten to the DATA phase of message transmission.

Message Reinjection Details

The Outbound Service reinjects the original content of the message to prevent duplicate outbound message processing (such as duplicating the compliance footer). The received header is changed to indicate reinjection and prevent the message from being detected as looping through the message security service.

Since reinjected messages will be in the original form — and it is reasonable to assume that some amount of time will pass between the first time we saw a message and when it is reinjected and resent — it is possible that an administrator could change outbound settings during this time.

The outbound server modifies and adds the word “reinjection” to the headers of reinjected messages. The Reinjection header line looks like a Received header line, except that “Received” is replaced with “Reinject”. There are two possible formats for the header.

The reinjection header will look similar to this:

```
Reinject: from [sending IP] (outboundsX.obsmtip.com) by  
reinject.domain.com . . . .
```

The [AAA.BBB.CCC.DDD] represents the IP address of the outbound server that processed the message. X is the number of the system which processes your mail traffic. The exact header strings will vary with the reinjection host, but each Reinject header should refer to a transmission either from or to an server labelled OB.

Reinjection should happen extremely rarely—less than 1% of the time.

Setting Up Outbound Filtering

Steps for setting up outbound filtering are different for each mail server. For instructions specific to your mail server, see the *Outbound Services Configuration Guide*.

There are four steps to activate outbound mail filtering:

1. Configure reinjection on at least one of your mail servers.

Configure your mail server and firewall to accept email only from the message security service. This is called a *private relay*. Your reinjection host needs to accept all email from the message security service's outbound servers. From your server's perspective, the message security service's delivery servers should be considered a trusted server. Allow relaying only from the message security service's IP range and other trusted relay servers.

Important: See "About Reinjection" on page 509 for details on reinjection.

If you have multiple mail servers, specify which server (or servers) will act as the reinjection host, and be sure that server can route mail back to the message security service.

Following are IP ranges:

To determine the system for your account: Your system number is shown the URL when you log in to the Administration Console or Message Center. The system number is prefaced by "ac-s" or "mc-s", for example:

URL displayed for an account on System 8 when logged in to the Administration Console:

```
https://ac-s8.postini.com/exec/adminstart?
```

URL displayed for an account on System 200 when logged in to the Message Center:

```
https://mc-s200.postini.com/app/msgctr/junk_quarantine\
```

Important: For system 20 customers, both sets of IP ranges are applicable.

System	IP Range	CIDR Range	IP/Subnet Mask Pair
5, 6, 7, 8, 20	64.18.0.0 - 64.18.15.255	64.18.0.0/20	64.18.0.0 mask 255.255.240.0
9	74.125.148.0 - 74.125.151.255	74.125.148.0/22	74.125.148.0 mask 255.255.252.0
10	74.125.244.0 - 74.125.247.255	74.125.244.0/22	74.125.244.0 mask 255.255.252.0
11, 20, 200, 201	207.126.144.0 - 207.126.159.255	207.126.144.0/20	207.126.144.0 mask 255.255.240.0

Contact your vendor for support and tips on setting up reinjection for your specific type of server.

Ensure that you are not an Open Relay (a machine that will accept email from anyone) by testing to see if an external IP can send an email through your reinjection host. You should see an error similar to “relaying denied.”

2. Configure your sending server’s SMTP timeout to 15 minutes (recommended).

Extend the timeout on your outbound server for delivering email. We recommend a 15-minute timeout. This provides Outbound with some flexibility to handle slow receiving mail servers.

For step-by-step instructions for configuring timeouts, contact your vendor for support and tips on configuring your specific type of server.

3. Add sending service IP addresses to the Outbound Servers tab.

Log in to the Administration Console. Select your email config and go to the Outbound Servers tab.

Click Add Record and enter the following data.

Accepted IP Ranges	<p>Enter a starting and ending IP for your email services address range. Be sure to use external IP addresses.</p> <p>When you send outbound email to the message security service for filtering, we need to know the external IP address range of your servers that are sending us email so that we can accept those messages. Outbound Services will reject all outbound mail unless the IP address is listed.</p> <p>The address range must be within a single class C address space. The IP range must be sequential. If you have non-sequential IPs, just add multiple records.</p> <p>If you have only one IP address, enter that IP address in both fields.</p> <p>When you save your IP range, Outbound Services will test to be sure that your IP addresses are unique.</p>
---------------------------	--

Reinjection Host	<p>Enter the IP address of your reinjection host.</p> <p>This should be the IP address of a mail server that will accept mail from the message security service and relay that mail back out again.</p> <p>You can enter multiple reinjection hosts, and specify a load balance between them. You can also specify failover servers for reinjection. Normally, this is not necessary and these fields can be left blank.</p> <p>You can also enter a hostname for the reinjection server instead of an IP address. However, you should not do so if the reinjection server has an MX record that routes mail back to the message security service. Use the IP range instead.</p> <p>Note: Enabling a reinjection host usually requires special configuration. For instructions specific to your mail server, see the <i>Outbound Services Configuration Guide</i>.</p> <p>If your mail server has not been set up to allow Outbound Services to act as a private relay, you'll need to configure your mail server before you can proceed.</p>
-------------------------	--

Click the Save button.

Outbound services will test your reinjection host. If your mail server has not been set up to allow Outbound Services to act as a private relay, you'll need to configure your mail server before you can proceed.

If you have more than one outbound server IP range, add additional records.

4. Configure a *smarthost* (or private DNS) on your sending servers.

Once you've set up a reinjection host and added the IP range to the Administration Console, redirect your mail to the message security service by setting up a *smarthost*. *Smarthost* is a common term for a server that accepts outbound mail and passes it on to the recipient.

Before you make changes, be sure to note your old settings in case problems occur. If there are problems with setup, mail flow can be delayed or interrupted.

The hostnames used in smarthost configuration depend on your system in the email protection service. Your system number is shown the URL when you log in to the Administration Console or Message Center. The system number is prefaced by "ac-s" or "mc-s", for example:

URL displayed for an account on System 8 when logged in to the Administration Console:

`https://ac-s8.postini.com/exec/adminstart?`

URL displayed for an account on System 200 when logged in to the Message Center:

`https://mc-s200.postini.com/app/msgctr/junk_quarantine`

Hostnames for smarthosts:

System	Hostname
5	outbounds5.obsmtip.com (previously named: outbound1.obsmtip.com)
6	outbounds6.obsmtip.com (previously named: outbound3.obsmtip.com)
7	outbounds7.obsmtip.com (previously named outbound5.obsmtip.com)
8	outbounds8.obsmtip.com
9	outbounds9.obsmtip.com
10	outbounds10.obsmtip.com
11	outbounds11.obsmtip.com
20	outbounds20.obsmtip.com
200	outbounds200.obsmtip.com
201	outbounds201.obsmtip.com

Setting up a smarthost is different for every server. Contact your vendor for support on steps for setting up a smarthost on your particular mail server.

If you are using a mail server that supports private DNS settings, you can set up Private DNS Service instead of setting a smarthost. For information about private DNS service as an alternative to a smarthost, see the *Outbound Services Configuration Guide*.

5. If applicable for your mail server (for example, if you are using Microsoft Exchange), you can configure Outbound services to quarantine or blackhole undeliverable bounce messages. See “Handling Undeliverable Bounce Messages” on page 515 for step to set up.
6. Configure outbound services, such as outbound virus filtering or a compliance footer. See “Outbound Services” on page 517 for more information.

Deleting an Outbound Servers Entry

If you change IP address ranges, or begin using a new mail server for outbound mail, you may need to remove an entry from Outbound Servers.

To remove an IP range:

1. Log in to the Administration Console.
2. Click the Outbound Servers tab and select the proper email config from the Choose Org pull-down menu.
3. Click the IP range you wish to delete.
4. Clear the IP range for the outbound server, but leave the reinjection server settings untouched.
5. Click Save to remove the IP range.

Handling Undeliverable Bounce Messages

Many mail servers (such as Microsoft Exchange) accept all mail traffic and then later create a new outgoing mail message in the event there is no recipient account. If the sending address is forged or unavailable, undeliverable bounce messages may become caught in your system. Outbound can be configured to quarantine or blackhole these messages at your discretion.

To block Undeliverable Bounce Messages:

1. Click the Outbound Servers tab.
2. Select an email config from the Choose Org pull-down.
3. Click Configure.

Choose Quarantine or Blackhole from the Status field to set the disposition for undeliverable bounce messages. "Off" allows undeliverable bounce messages to defer for up to five days before bouncing. "Blackhole" will accept the messages as if successfully delivered and silently discard.

4. Type in the email address of the administrator in whose quarantine these messages should be quarantined.

Note: This step is necessary even if blackholing the messages.

5. Click Save.

Interpreting the Outbound Overview Page

The Outbound Servers tab helps you to visualize your outgoing mail flow by providing the following functionality:

Processing Overview	<p>Graph of messages over time for the last 60 minutes of traffic, depicting processed, delivered, deferred (400-series errors), bounced (500-series errors), reinjected, and quarantined traffic.</p> <p>This graph helps you to visualize your outgoing mail flow, including details about messages processed and their final disposition for the last 60 minutes. The graphs are updated every minute, but you must reload the page to see a new graph.</p>
Email Activity	<p>Graph of messages over time for the last 60 minutes of traffic depicting inbound and outbound traffic.</p> <p>This graph helps you to visualize inbound versus outbound mail flow. The graphs are updated every minute, but you must reload the page to see a new graph.</p>
Current Activity	<p>Statistics from the last 60 seconds of traffic — Valid Messages, 400 Errors, 500-Errors, Quarantined, Avg. Message Size, Total Bytes.</p>
Log	<p>Link to logs.</p> <p>These logs will display all definitive delivery and failure information. For temporary deferral information, refer to your mail server logs. The log loads immediately, but it is up to 20 minutes behind current outgoing mail flow.</p>

Status	<p>Lists all accepted IP ranges for outgoing mail servers and their associated reinjection host.</p> <p>This information is used to determine which IPs can transmit outgoing mail traffic to the message security service.</p>
Undeliverable Bounces	<p>Configuration to block or blackhole undeliverable bounce messages generated by your mail server.</p> <p>Most mail servers silently discard these messages when they are not deliverable. Since the message security service is acting as a proxy, your sending mail server will not realize it can discard them.</p>

Outbound Services

The Outbound Services are made up of the following components: Virus Blocking, Attachment Manager, Content Manager, and Compliance Footer. These components apply filtering and can insert content into outbound mail.

- For information about outbound Virus Blocking, see “Virus Blocking” on page 311.
- For information about outbound Attachment Manager, see “About Attachment Manager” on page 403.
- For information about outbound Content Manager, see “How Content Manager Works” on page 333.
- For information about Compliance Footers, see “Compliance Footer” on page 518.

Message Association with Organization Settings

All outbound mail is connected with an email configuration organization that has the sending IP listed in Outbound Configuration. If the sending IP is not listed, the message is rejected.

For settings such as Outbound Content Manager, Outbound Attachment Manager, Outbound Virus Filtering, and Compliance Footer, settings are used based on the appropriate organization.

Outbound attempts to use the most relevant organization settings:

- If the sender's **email address is registered** as a user account under that email config, then Outbound uses the settings for the organization that contains that user.
- If the sender's **email address is not registered, but the domain is registered**, then Outbound uses the settings for the organization that contains that domain.
- If the sender's **email address and domain are not registered**, then Outbound uses the settings for the email config organization that contains the sending IP address.

Component Order of Operations

The order of operations for outbound components is:

1. Scan and perform disposition for outbound Virus Blocking.
2. Scan and perform disposition for outbound Content Manager.
3. Perform Outbound Spam Scanning.
4. Scan and perform for outbound Attachment Manager.
5. Insert compliance footer.

Outbound Traffic Reports

Outbound mail processing generates reports of outbound traffic. See "Traffic Reports" on page 555 for detailed information.

Compliance Footer

Outbound messages can be configured with footer text that describes an email policy or legal compliance. This compliance footer is added into the last existing text portion of a message. In the rare event of an empty text portion, the compliance footer is not included. The compliance footer is part of Outbound Services. Compliance footers are configured at the organization level.

Note: The compliance footer currently supports ASCII and English character sets only.

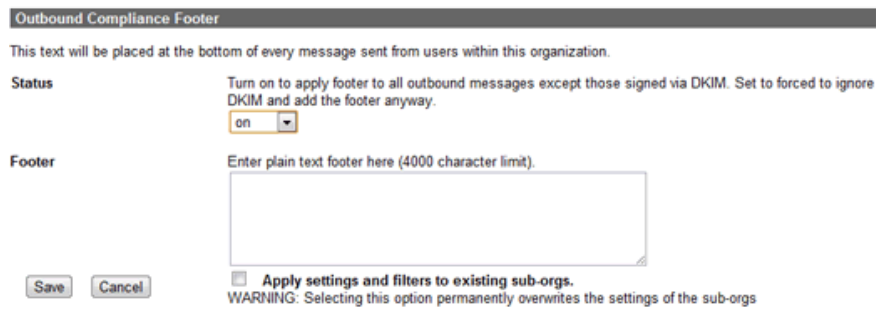
Add a Compliance Footer to an Outgoing Email.

1. In the Administration Console, go to Orgs and Users > Orgs.
2. Choose an organization from the Choose Orgs pull-down list, or click an organization in the organizations list.

3. In the Organization Management page, scroll to the Outbound Services section, and click the Compliance Footer icon.



4. In the Outbound Compliance Footer page:
 - Set the footer Status to **on**, **off**, or **forced** (the *forced* option adds the footer even for DKIM-signed outgoing mail).
 - Add the footer text. We recommend plain-text footers.
 - Choose whether to propagate the footer to sub-orgs.



This text will be placed at the bottom of every message sent from users within this organization.

Status Turn on to apply footer to all outbound messages except those signed via DKIM. Set to forced to ignore DKIM and add the footer anyway.
on

Footer Enter plain text footer here (4000 character limit).

Apply settings and filters to existing sub-orgs.
WARNING: Selecting this option permanently overwrites the settings of the sub-orgs

Save Cancel

5. Click **Save**.

Test the compliance footer

Once you have configured and enabled the compliance footer, you can test it by sending a message to an address outside your domain. In order for a message to include the compliance footer, it must pass through the Postini Outbound Service.

Formatting the Compliance Footer Text

HTML

The Outbound Compliance Footer is designed to be a text-only footer; however, it is possible to add some minimal HTML to the footer. If the Compliance Footer is added to an HTML-formatted message, any HTML in the footer is rendered as expected. If the footer is added to a plain-text or RTF message, the HTML is not rendered and the footer is displayed as plain text including the HTML code.

Line Breaks

If you do not include line breaks in the footer, it is displayed as one long string:

```
Sentence 1, Sentence 2, Sentence 3, Sentence 4....
```

To include line breaks, press `Enter` at each point where you would like a break:

```
Sentence 1[press Enter]
```

```
Sentence 2[press Enter]
```

```
...
```

Processing with Different Message Types

Following are descriptions of how the compliance footer is processed for different types of messages.

Type of Message	Description
HTML Messages	<p>When a compliance footer is configured and enabled, the message security service adds the text of the footer as-is to the bottom of each text part of the message. For HTML text parts, it includes the <code><PRE></code> tag before the footer so that the text of the footer is rendered in HTML mail clients as fixed-width text. Since the text added by the message security service is seen as a part of the HTML, the mail client renders the HTML tags properly.</p> <p>To override the <code><PRE></code> tag, begin the footer with a closing tag: <code></PRE></code>. This allows you to specify your own font tag.</p>
Binary Messages	<p>Messages that do not contain text parts do not include a compliance footer.</p>

Type of Message	Description
Multipart/Alternative Messages	Messages that are created as a text part which contains other embedded objects (including messages or other text parts) include a compliance footer. The footer is added to the end of the last text part of the container — not to any embedded text parts.
Forwarded Messages	<p>If the message has a text part, the footer is added to the last text part of the message.</p> <p>Messages that are forwarded as attachments do not have a compliance footer added within the forwarded message body.</p>
Bounced Messages	Do not include a compliance footer.
Quarantined Messages	Quarantined messages that are delivered from quarantine do not include a compliance footer.
Reinjected Messages	<p>Reinjected messages include single compliance footer. Even if a message is reinjected several times, it will only have one footer inserted.</p> <p>For further details about reinjection, see “Configuring Outbound Servers” on page 507.</p>

Transport Layer Security for Outbound Mail

Note: This section covers TLS for outbound mail. For information about TLS for inbound mail, see “Transport Layer Security for Inbound Mail” on page 428.

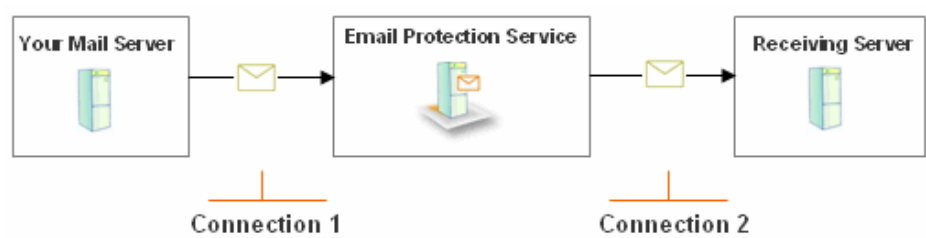
Outbound Service supports Transport Layer Security (TLS), which is a protocol that encrypts and delivers mail securely. If you have the TLS option enabled, you can configure TLS connections for both inbound and outbound mail traffic.

You can send TLS-encrypted messages to a receiving mail server that is TLS-enabled. You must have TLS enabled on your mail server. If the receiving mail server does not support TLS, the message is delivered via SMTP (no messages are lost or bounced) assuming you have selected the “SMTP or TLS” option described in this section.

Expanded encryption options are available if you require further security. This includes the ability to configure TLS settings for specific domains, and the ability to send encrypted mail through a secure portal for recipients who do not have TLS enabled. For more information about these products, see “About Policy Enforced TLS” on page 438 and the *Encryption Manager Administration Guide*.

For outbound mail traffic, the message securityfiltering service acts as a proxy between the your mail server and the receiving server. The first connection is from your mail server to the message securityfiltering service. You can choose whether this connection uses TLS. You may choose not to use TLS if your mail server is not TLS-enabled.

The second connection is from the message securityfiltering service to the receiving mail server. If you chose TLS encryption for the first connection, the message securityfiltering service can connect via TLS to the receiving mail server.



For further details on TLS, please see “Authentication and Certificates” on page 432.

Setting Up Outbound TLS

Setting up outbound TLS involves these steps

- Preparing your mail server for TLS
- Testing Your Mail Server’s TLS Configuration
- Configuring TLS for inbound servers

Each step is described in detail below.

On the same page as inbound TLS, you can also configure inbound Policy Enforced TLS. For more information about Policy Enforced TLS, see “About Policy Enforced TLS” on page 438.

Follow these steps to set up outbound TLS on each mail server you want to configure.

Prepare Your Mail Server for TLS

Enabling TLS delivery requires enabling TLS on your mail server. Following are the steps required:

1. **Turn on TLS for Outbound service in the email protection service. See “Setting Up Outbound TLS” on page 522 for configuration steps.**

You only need to turn on TLS for Outbound if your outgoing mail is delivered through the Outbound service.

WARNING: You must turn on TLS for Outbound service in the Administration Console before enabling TLS on your mail server.

Some mail servers, specifically Microsoft Exchange 2000/2003, defer your outgoing mail if TLS is enabled *first*. If you find that messages are queued, be sure that TLS is disabled on your mail server, then turn on TLS in the Administration Console, and enable TLS on your mail server.

Similarly, to turn off TLS for outbound service, you must disable TLS on Exchange *before* making changes to the Outbound TLS settings in the Administration Console.

2. Obtain a certificate from a commercial certificate authority, or create a self-signed certificate for encryption purposes.

To obtain or create a certificate, contact an appropriate security vendor as the email protection service does not provide tools for obtaining or creating a certificate. More information on this may be available through support.

3. Install the certificate and enable TLS on your mail server.

Important: TLS support requires that you install your certificate and configure TLS on your mail server. This procedure may require some research and technical configuration upon your part. Please consult your mail server documentation for information on enabling TLS.

Further information for configuring the most common mail servers may be available through support. For further information, consult documentation and support for your mail server.

Test Your Mail Server's TLS Configuration

You can check if your mail server will accept TLS connections by using telnet from your mail server to the server software itself (you type the commands in `bold` text):

```
> telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.domain.com
Wed, 08 Feb 2007 08:05:03 -0700 (PDT)
> ehlo localhost
250-mail.domain.com Hello localhost [127.0.0.1],
pleased to meet you
250-STARTTLS
> starttls
220 2.0.0 Ready to start TLS
```

If you have other ESMTP options enabled, you will see more lines that start with 250-OPTIONNAME, and not only 250-STARTTLS. Once you receive a 200-series response to your `starttls` command, this confirms that your mail server will accept TLS connections.

For details verifying whether a message was transmitted via TLS, see “Received Header Field” on page 638.

You can also view a report of TLS activity with your service. See “TLS Reports” on page 580 for more information.

Configure TLS for Outbound Servers

To enable TLS delivery:

1. In the Administration Console, click Outbound Servers > TLS.
2. In the Outbound TLS screen, choose an email server config from the Choose Org pull-down list.
Note: Be sure to pick an email config org that is administering your outbound server.
3. Choose the Outbound TLS settings. To do this, you must select how the message securityfiltering service accepts outbound messages from your mail server, and also how the message securityfiltering service sends your outbound messages to recipient mail servers. These settings are described below.

1. Choose how the email protection service accepts outbound messages from your mail server.

Important: Your mail server, including reinjection hosts, must be configured for TLS to send messages via TLS.

- Accept SMTP and TLS.**
The email protection service accepts messages via either SMTP or TLS from your mail server.
- Accept only TLS**
The email protection service accepts message only via TLS from your mail server.
Caution: All non-TLS encrypted messages are deferred.

The first Outbound TLS setting enables you to choose how the message securityfiltering service accepts outbound messages from your mail server:

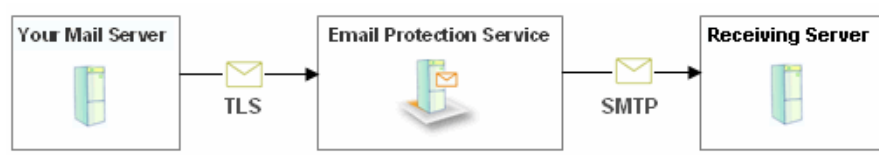
- **Accept SMTP and TLS:** This is the old “on” setting and is recommended. With this selection, the message securityfiltering service accepts messages via either SMTP or TLS from your mail server.
- **Accept only TLS:** With this selection, the message securityfiltering service accepts message only via TLS from your mail server. All non-TLS encrypted messages are deferred.

2. Choose how the email protection service sends your outbound message to recipient mail servers.

- Send only SMTP**
No TLS encryption, all messages delivered via SMTP.
- Send by SMTP or TLS**
Messages sent via TLS are delivered via TLS to the recipient. Recipient servers that do not support TLS will receive their mail delivered via SMTP. All other messages are delivered via SMTP. (Recommended)
- Send and Deliver TLS**
Messages sent via TLS are delivered via TLS to the recipient. If the recipient server does not support TLS, these messages are deferred. All other messages are delivered via SMTP.
- Send by TLS if possible**
Deliver all messages by TLS when possible. Recipient servers that do not support TLS will receive their mail via SMTP.
- Send by TLS Only.**
Send all messages by TLS. Mail sent to recipient servers that do not support TLS will be deferred.

The second outbound TLS setting enables you to choose how the message securityfiltering service sends your outbound messages to recipient mail servers.

- **Send only SMTP:** This is the old “off” setting. No TLS encryption, and all messages are delivered via SMTP.



- **Send by SMTP or TLS:** This is the recommended setting. Messages sent via TLS are delivered via TLS to the recipient. Recipient servers that do not support TLS will receive their mail delivered via SMTP. All other messages are delivered via SMTP.



- **Send by TLS if possible:** This delivers all messages by TLS when possible. Recipient servers that do not support TLS will receive their mail via SMTP.



- **Send only TLS:** Send all messages by TLS. Mail sent to recipient servers that do not support TLS will be deferred.



- **Send and Deliver TLS:** Messages sent via TLS are delivered via TLS to the recipient. If the recipient does not support TLS the message will be deferred. All other messages are delivered via SMTP.



4. Click Save. Repeat the process for any additional email server configs that are administering an outbound server.

Install digital certificates and enable your mail server for TLS. See “Prepare Your Mail Server for TLS” on page 434 for more information.

Configuring Your Mail Server for TLS

1. Turn on TLS for Outbound service in the message securityfiltering service.

See “Setting Up Outbound TLS” on page 522 for configuration steps.

WARNING: You must turn on TLS for Outbound service in the Administration Console before enabling TLS on your mail server.

Some mail servers, specifically Microsoft Exchange 2000/2003, will defer your outgoing mail if TLS is enabled *first*. If you find that messages are queued, be sure that TLS is disabled on your mail server, then turn on TLS in the Administration Console and enable TLS on your mail server.

Similarly, to turn off TLS for outbound service, you must disable TLS on Exchange *before* making changes to the Outbound TLS settings in the Administration Console.

2. Obtain a certificate from a commercial certificate authority, or create a self-signed certificate for encryption purposes.

Contact support for basic information about creating a self-signed certificate on Windows XP or LINUX/UNIX variants.

You will need to work with a certificate authority or self-signing certificate vendor to set up TLS— this service is not provided by the message securityfiltering service.

3. Install the certificate and enable TLS on your mail server.

Important: TLS support requires that you install your certificate and configure TLS on your mail server. This procedure may require some research and technical configuration on your part. Please consult your mail server documentation for information on enabling TLS.

Related Topics

- **Outbound Concepts**
- **Setting Up Outbound Filtering**
- **Handling Undeliverable Bounce Messages**
- **Compliance Footer**
- **Setting Up Outbound TLS**
- **Troubleshooting: Outbound**

Troubleshooting Outbound Spam Scanning

The message security service filters all outbound mail for spam-like content, in order to keep Outbound Services IP addresses from being listed on registered blacklists (RBLs) that would interrupt deliverability.

With Outbound Spam Scanning, messages are evaluated on an individual basis according to content: valid messages are transmitted normally, and offending messages are bounced (with a 500 reply code).

For information about legal policies regarding outbound spam content, see our *Acceptable Use Policy*.

When outbound filters block content for spam, there are three common reasons: an *open relay*, a *botnet infection*, or *junk content*.

- **Open Relay:** If you allow all IP addresses to pass mail through your server, your mail server will become an *open relay*. This security vulnerability leaves your mail server vulnerable to hijacking from malicious senders, who connect to your mail server and use it to send spam out through your mail server. An open relay is the most common cause of outbound spam content; about half of all outbound mail blocked for spam content is caused by an open relay.
- **Botnet Infection:** Malicious senders sometimes spread viruses which hijack your servers and use them to send out junk email to recipients throughout the Internet, as a way to distribute load and avoid IP black lists. This is known as a *botnet infection*.
- **Junk Content:** The outbound spam filter uses content-based heuristics to detect messages with spam-like content. Sometimes, outbound content you intentionally send may be detected as spam by the message security service. This is very rare, since only the most extreme spam messages are stopped, and false positives are very rare. Junk content constitutes only a small portion of mail blocked for spam content.

If messages are blocked as spam, you will see delivery failure messages on your mail server that show 500-series error messages when trying to deliver content. Often, you will see a very large number of delivery failure messages for messages that look like identical commercial messages, not related to your normal business.

If you think your mail may be blocked by outbound spam filtering, check for the most common causes of outbound messages bounced for spam.

Check for open relays

If your mail server is an open relay, a malicious sender will eventually find it and use it to send out spam.

You can check to see if your mail server is acting as an open relay by following these steps:

1. Run an open relay test from outside your network. The easiest way to do this is find a publicly available open relay test on the web. Go to <http://www.google.com> and search for "open relay test" to find an open relay test server.
2. Run the test to check for open relays on your mail server, using your mail server name or the external IP address of your mail server.
3. If the test shows your mail server is an open relay, change it to be a private relay. This is different for each server. For steps on how to set up a private relay for most common servers, see the *Outbound Services Configuration Guide*

Check for botnet attacks.

A botnet attack is a virus running on your mail server or inside your network. You can detect and resolve a botnet attack with up-to-date virus scanning software.

1. If you do not already have virus scanning and protection on your mail server and other machines in your network, purchase and install it.
2. Update your virus scanning and protection with the latest data files.
3. Scan your machines for viruses, and remove any viruses found.

Check for spam-like content

If some of your outbound mail, especially broadcasts, mailing lists and other announcements, are getting bounced with 500 series errors and not delivered, the email security service may be detecting messages as spam.

Check the text of the message failure message.

1. Alter the content of your message so that it will not be rejected as junk mail.
2. If you need to send mail that will not pass through outbound spam filtering, send that mail through a separate mail server that does not route outbound mail through Outbound Services.
3. If you believe the message was captured in error, you can submit it for future revisions of the junk mail filters. For more information on reporting suspected false positives, contact support.

Troubleshooting: Outbound

How can I use one IP range for outbound servers for multiple server configurations?

Break up the IP range into smaller ranges and associate those ranges with the appropriate email config. IP ranges are unique and will associate a mail message with a user or email config for the purposes of outbound configuration.

How do you remove an Outbound IP Range?

When removing an Outbound Email Server by deleting all entries under Accepted IP Range and Reinjection Host, the following error occurs:

```
A reinjection host is required.
```

To eliminate this error, follow the steps below:

1. In the Administration Console, choose the appropriate email config organization and click the Outbound Servers tab.
2. Select the Outbound IP range to be removed by clicking on the IP range under the gray Status bar.

3. Delete the entries under Accepted IP Range.
4. Leave the entries under Reinjection Host.
5. Click the Submit button.

This will successfully remove both the IP range and associated Rejection Host.

What happens if reinjection fails?

If reinjection fails, then the message will be deferred to all recipients. This means that any recipients who did receive the message during the original transmission will receive duplicates of that message. Some mail servers may compensate for these duplicates.

Why does my compliance footer not show up?

The messages were associated with an organization that does not have the compliance footer configured. See “Configuring Outbound Servers” on page 507 for details on how a message is associated with an organization.

Why do I see an error message, “Can’t find account level org above mail host”?

There is a problem with your organization hierarchy. Contact your vendor for support to correct this problem.

Chapter 25

Test Tools & Mail Flow Troubleshooting

About Test Tools & Mail Flow Troubleshooting

From time to time, you'll need to ensure that the message security service is running as desired. The System Tests section of the Administration Console includes several programs for testing and troubleshooting the delivery of email.

If you have a mail delivery emergency (no incoming mail), see "Troubleshoot Incoming Email Delivery" on page 544.

SMTP Message Test

Use the SMTP Message Test to verify whether your email server can receive a message. The test generates an actual message, so you should use an address with both an email account on your mail server and a user account on the message security service. You can also enter a user alias, but not a domain alias.

Note: If your mail server rejects spoofed sender addresses, this may cause the SMTP Message test to fail even though other mail can be sent successfully.

To run the SMTP Message Test:

1. Go to the home page (click the logo at the top of any Administration Console).
2. Click the SMTP Message Test link in the lower left-hand corner of the page.
3. On the SMTP Message Test page, enter the email address of a user to be used as the message recipient.

4. Select an option:
 - **Test mail flow through the data center:** Checks mail connectivity through the message security service to your mail server. It can be used to troubleshoot mail delivery to identify problems with Administration Console settings.
 - **Test an email generated by the data center:** Helps you troubleshoot issues concerning delivery of alerts, quarantine summaries, and quarantined messages.
 - **Test an email from the data center directly to your mail host:** Checks mail connectivity to your mail server. It can be used to troubleshoot mail delivery and find problems on your mail server.
5. Click Test. The results appear at the bottom of the page:

SMTP Message Test Tests delivery to your mail server. This test generates a message, so you must enter an email address that has both an account on your mail server and the email protection service. After running the test, you'll check the inbox to confirm delivery.

Enter a valid email address on your mail server:

Test mail flow to your server
 Sends a test message from the Internet through the data center to your mail server.

Test an email generated by the data center
 The data center generates and sends a test message through our system to your mail server. This most closely simulates delivery from quarantine.

Test that your mail server can receive mail traffic from the data center
 The data center generates and sends a test message directly to your mail server.

To run the SMTP Message Test by batch file:

See the **testmail** command section in the “Commands” chapter of the *Batch Reference Guide* for details on submitting the following command:

```
testmail <user name>, mailtype=0/1
```

<code><user name></code>	Address for the test email recipient
<code>mailtype=0/1</code>	Method for test: 0, if sent through the data center 1, if generated by the data center

Successful Results for SMTP Test

Test mail flow through the data center

A successful SMTP Message Test using this option displays the following test summary:

```
Sending test email to marc@jumboinc.com:
```



```
Establish connection...
Sending HELO
Sending MAIL FROM
Sending RCPT TO
Sending data
End of data dot
Success
```

The email data center can deliver email to this email server from an external email server.

Test an email generated by the data center

When the SMTP Message Test successfully delivers mail to your mail server using this option you will see:

```
Sending test email to mark@jumboinc.com:
```

```
Establish connection...
Sending HELO
Sending MAIL FROM
Sending RCPT TO
Sending data
End of data dot
Success
```

The email data center can deliver email to this email server from an external email server.

Test an email from the data center directly to your mail host

Note: This test setting will always fail if your mail server is set to accept only TLS mail. If your mail server accepts only TLS connections, use one of the other two test settings instead.

When the SMTP Message Test successful delivers mail to your mail server using this option, you will see:

```
Sending test email to marc@jumboinc.com:
Establish connection...
Sending HELO
Sending MAIL FROM
Sending RCPT TO
Sending data
End of data dot
Success
```

The email data center can deliver email to this email server.

In all cases, the recipient `marc@jumboinc.com` will receive the following email:

```
From: Test <test@psmtp.com>
To: mark@jumboinc.com
Subject: Email Flow Test
```

This is a test message.

Error Messages and Next Steps

When the SMTP Message Test fails, you will see a summary similar to the successful test results, however the last line of the summary points out when the transaction failed.

For example:

```
Establish connection...  
Sending HELO  
HELO failed.
```

Phase of Test	Next Steps
SMTP Connection failed.	See “Troubleshoot Incoming Email Delivery” for full steps.
HELO failed.	This usually indicates an issue with your mail server. Look in your mail server logs for the exact SMTP error it returned. This information will help you resolve this issue.
MAIL FROM failed.	This indicates that your mail server will not accept the sender (<code>test@psmtp.com</code>) or timed out during this phase of the test. Look in your mail server logs for the exact SMTP error it returned. This information will help you resolve this issue.
RCPT TO failed.	This usually indicates that your mail server rejected the recipient or timed out during this phase of the test. Does the recipient have an email box on the server? Look in your mail server logs for the exact SMTP error it returned. This information will help you resolve this issue.
Sending message data failed.	This indicates that your mail server rejected the body of the email message or timed out during this phase of the test. Look in your mail server logs for the exact SMTP error it returned. This information will help you resolve this issue.

MX Record Test

Typically, you will test your MX records shortly after signing up with the message security service. You might also run the test any time you change MX records or domain names.

To run the MX Record Test:

1. Go to Orgs and Users > Orgs and select the organization containing the domain you wish to check.
2. Click the System Tests icon and click the MX Record Test link.
3. Choose the domain you want to check.
4. Click Test. The results appear on the bottom of the page.

MX Record Test Verify that your MX records are properly configured for a particular domain.
Select the domain that you wish to test:

To run the MX Record Test by batch file:

See the **testmx** command in the “Commands” chapter of the *Batch Reference Guide* for details on submitting the following command:

```
testmx <domain name>
```

<domain name>	Name of the domain whose DNS MX entries you wish to test
---------------	--

Successful Results for the MX Record Test

The following indicates a successful MX Record Test. Mail for the domain you selected (in this case, `jumboinc.com`) is routing correctly to the message security service.

```
jumboinc.com: MX records OK.  
  
jumboinc.com IN      MX      100 s1a1.psmtplib.com  
jumboinc.com IN      MX      200 s1a2.psmtplib.com  
jumboinc.com IN      MX      300 s1b1.psmtplib.com  
jumboinc.com IN      MX      400 s1b2.psmtplib.com
```

Error Messages and Next Steps

If the MX Record Test fails for the selected domain (in this case, `jumboinc.com`), emails may not be filtered or may even be bounced. You will see the results of the test followed by relevant parts of your DNS MX entries as seen by the DNS servers used by the message security service:

For example:

```
testmx to jumboinc.com: No MX record found containing
'sla2.psmtplib.com'
jumboinc.com      IN      MX      100  sla1.psmtplib.com
jumboinc.com      IN      MX      200  mail3.jumboinc.com
jumboinc.com      IN      MX      300  slb1.psmtplib.com
jumboinc.com      IN      MX      400  slb2.psmtplib.com
```

See the table below for details on which errors you may run into, and the next steps you should take.

Error	Next Steps
<p>No MX record found containing 'sNaM.psmtplib.com'</p> <p>or</p> <p>No MX record found containing 'sNbM.psmtplib.com'</p>	<p>Add the appropriate entry. There should be one MX entry for each:</p> <pre>sNa1.psmtplib.com sNa2.psmtplib.com sNb1.psmtplib.com sNb2.psmtplib.com</pre> <p>N is a number — 5, 6, 7, 8, 9, 10, 11, 20, 200 or 201.</p>
<p>Multiple MX records found containing 'sNaM.psmtplib.com'</p> <p>or</p> <p>Multiple MX records found containing 'sNbM.psmtplib.com'</p>	<p>Remove the duplicate entry listed. Look at the entries listed to see what is listed in place of the MX entry pointing to <code>jumboinc.com.sNaM.psmtplib.com</code> or <code>jumboinc.com.sNbM.psmtplib.com</code>.</p> <p>There should be entries for each:</p> <pre>sNa1.psmtplib.com sNa2.psmtplib.com sNb1.psmtplib.com sNb2.psmtplib.com</pre> <p>N is a number — 5, 6, 7, 8, 9, 10, 11, 20, 200, or 201.</p>
<p>Unable to resolve 'jumboinc.com'</p>	<p>Create DNS MX entries for the domain on the authority DNS server. Currently no entries can be found.</p> <p>This may be a symptom of trouble with your authority DNS server.</p>

Error	Next Steps
Non-psmtp MX record found: 'jumboinc.com'	Either your DNS MX entries for the domain have not propagated to the message security service's DNS servers or you need to change the ID for your DNS MX entries to indicate to other servers that they need to ask your DNS server for new entries.
Unable to retrieve MX records for 'jumboinc.com'	This likely indicates trouble with one or all of your authority DNS servers.
Priority of psmtp MX records must be higher than Customer MX records	Change your DNS MX entries for the domain so that the message security service entries are higher than the entries which route to your mail server.

Health Check: Firewall Test

Health Check shows you the best practices and recommended settings for the message security service. You can maximize the performance of the service by making a few quick changes to your configuration.

Click the Health Check tab in the Administration Console to review your settings and identify any settings that you may need to adjust. Use the instructions below to make any adjustments if necessary.

Once your MX records are pointed to the service, all of your legitimate mail should only come from the message security service.

If you do not lock your firewall down to only accept port 25 traffic from the message security service, spammers will be able to connect directly to your mail server and send spam unfiltered.

Health Check will display the results of your firewall tests for your organizations. For detailed instructions on running firewall tests, see "Run a Firewall Test" on page 538.

Related Topics

- **Run a Firewall Test**
- **Health Check: Update User Settings**
- **Health Check: Approved Senders List Cleanup**
- **Health Check: Update Settings for Executable Attachments**
- **Health Check: Update Virus Settings**

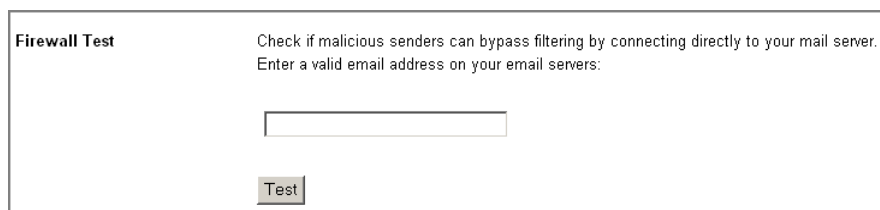
Run a Firewall Test

This tests whether your firewall allows email traffic from IP addresses besides the message security service. Malicious senders may attempt to send traffic directly to port 25 on your server, and bypass filtering and protection. We recommend you configure your email server or firewall to accept traffic only from the message security service. For more details about running this command in the batch interface, see the `testfirewall` command in the “Commands” chapter of the *Batch Reference Guide*.

WARNING: You must be sure to add all of your domains to the message security service before locking down your firewall to accept only email traffic from the service IP range. Otherwise, email sent to unregistered domains may bounce.

To run the Firewall Test:

1. Click the logo at the top of any Administration Console page to go to the Home page.
2. Click the Firewall Test link in the lower left-hand corner of the page.



Firewall Test Check if malicious senders can bypass filtering by connecting directly to your mail server.
Enter a valid email address on your email servers:

Test

3. On the Firewall Test page, enter the email address of a user to be used as the message recipient. You can also enter a user alias, but not a domain alias.
4. Click Test. The results appear on the bottom of the page

Successful Results for the Firewall Test

If your server is blocking connections from outside IP addresses, you will see a message saying that the test passed. This is a desirable result, since this keeps malicious senders from bypassing the message security service. No further action is needed.

For example:

```
Checking firewall from 12.158.34.71...passed (did not accept connection)
```

Error Messages and Next Steps

If your server is accepting connections from outside IP addresses, you will see a message saying that the connection was accepted. This may cause problems, since malicious senders may be able to bypass the message security service.

Note: Some firewalls and mail servers, such as Lotus Domino, accept the initial test connection to port 25 but force a disconnection before mail is sent. This can cause the Firewall test to fail. If you are using a firewall or mail server that accepts port 25 connections initially, verify that port 25 is protected by manually connecting to port 25 and attempting to send a test message.

If this test shows a successful connection, we recommend that you lock down your firewall to block messages from outside IP addresses. Once you have changed your firewall settings, run the Firewall Test again to confirm that the change is successful.

For example:

```
Checking firewall from 12.158.34.71...failed (accepted connection)
```

If the Firewall Test shows accepted connections from an outside IP address:

1. We recommend you change your firewall settings to block connections to port 25 which do not come from the message security service.
2. When you have made these changes, run the Firewall Test again to be sure that outside IP addresses are being blocked.
3. Once you have made these changes, run the SMTP Message Test using the option "Test an email from the data center directly to your mail host" to confirm that mail flow is uninterrupted. See "SMTP Message Test" on page 531 for full steps on running the SMTP Message Test.

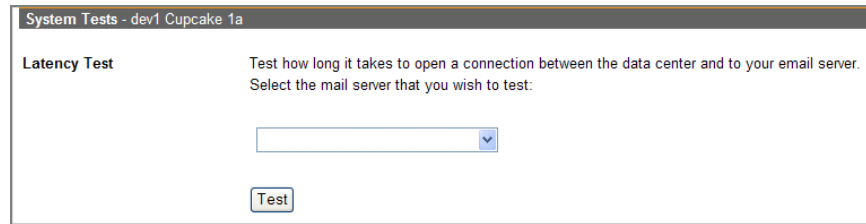
Latency Test

Network latency is the connection delay between the email data center and your email server. Ideally, latency should be as low as possible. Use the Latency Test if you want to see how well the network is responding.

To run the latency test:

1. Go to Inbound Servers > Delivery Manager.
2. Click the Latency Test link in the lower right-hand corner of the page.
3. Choose the email server you want to check.

4. Click Test. The results appear on the bottom of the page.



System Tests - dev1 Cupcake 1a

Latency Test Test how long it takes to open a connection between the data center and to your email server. Select the mail server that you wish to test:

Test

To run the latency test by batch file:

See the checklatency command in the “Commands” chapter of the *Batch Reference Guide* for details on submitting the following command:

```
checklatency <email config org name>, mailhost=<mail server name>
```

<code><email config org name></code>	Name or iid of the email config containing the mailhost
<code>mailhost=<mail server name></code>	The name of the mailhost to check

Interpret Latency Test Results

Latency Test results are relative and must be compared to normal test results for a period when your network is experiencing similar traffic patterns. Increased network latency alone is not a sign of email trouble in the message security service.

The message security service has extremely fast connectivity to the Internet through multiple drops. High latency could be due to problems on any leg of the route between the message security service and your email server. Use the Traceroute Test to narrow down the cause of slow latency.

Latency can be influenced by many factors, such as your Internet connection (T1 or dialup), your LAN/WAN configuration, router problems, and system load across the network.

You may see errors like this:

```
Error - unknown host mail14.jumboinc.com
```

This indicates that the server you are attempting to test does not have DNS entries.

Traceroute Test

Use the Traceroute Test to display the network hops that occur between the email data center and your server.

To run the Traceroute Test:

1. Select an Email Config.
2. Go to Inbound Servers > Delivery Manager.
3. Click the Traceroute Test link in the lower right-hand corner of the page.
4. Enter the hostname of your email server.
5. Click Test. The results appear on the bottom of the page.

Note: When a firewall blocks a traceroute, this may take a few minutes. The Traceroute Test will update when the test is complete.

Traceroute Test

Trace each network hop between the data center and your email server. Also see how long each hop takes. Result show where data must travel to reach the server and where delays might be occurring. Select the mail server that you wish to test:

To run the Traceroute Test by batch file:

See the checkroute command in the “Commands” chapter of the *Batch Reference Guide* for details on submitting the following command:

```
checkroute <email config org name>, mailhost=<server name>
```

<email config org name>	Name or iid of the email config containing the mailhost
mailhost=<server name>	The name of the mailhost to check Replace <server name> with the name or IP address of the server (as configured in the email config)

Interpret Traceroute Test Results

Traceroute tests to your email server are only helpful when paired with traceroute tests from your email server to the message security service. Some service providers prevent traceroutes.

Results will look like this:

```
traceroute to mail4.jumboinc.com (192.168.30.51), 30 hops max,
38 byte packets
 1 dumont (172.16.0.2)  2.910 ms  0.941 ms  0.984 ms
 2 mail4.jumboinc.com (192.168.30.51)  2.990 ms  2.596 ms  2.615 ms
traceroute complete
```

There will be one line for each hop along the network route from the message security service to your email server. Each hop will be tested 3 times, with the times of those test listed. If a * character is listed in place of a time, the test failed. However, this failure may be due to the fact that some hops will not accept traceroutes (rather than a connection issue).

Following is an example showing a traceroute being stopped by a firewall along the route (a normal occurrence):

```
traceroute to mail4.jumboinc.com (192.168.30.51), 30 hops max,
38 byte packets
 1 skinner-38 (64.18.2.2)  0.516 ms  0.505 ms  0.294 ms
 2 br1-exodus1-g1-2 (10.1.252.129)  0.589 ms  0.574 ms  0.594 ms
 3 64.14.3.145 (64.14.3.145)  0.594 ms  0.280 ms  0.294 ms
 4 bhr1-g3-0.SantaClarasc5.savvis.net (216.34.3.9)  0.593 ms  0.278
ms 0.592 ms
 5 dcr1-so-3-1-0.SanFranciscosfo.savvis.net (208.172.147.109)  1.793
ms 1.474 ms 1.493 ms
 6 bpr1-so-0-0-0.PaloAltoPaix.savvis.net (206.24.211.74)  3.593 ms
3.574 ms 3.591 ms
 7 * * *
 8 * * *
 9 * * *
10 * * *
[hops 11-29 removed for brevity]
30 * * *
traceroute complete
```

Since a firewall prevents all packets, it takes time for three packets per hop and up to 30 hops of packets to fail. This can cause a multiple-minute delay in retrieving your Traceroute Test results.

You may also see errors similar to this:

```
Error - unknown host mail14.jumboinc.com
```

This indicates that the server you are attempting to test does not have public DNS entries.

Reinjection Test

The Reinjection Test verifies that your reinjection servers, if any, are functioning properly. If you are using Outbound Services, you must have a reinjection server that can accept private relays from the message security service back out to the Internet.

For more information about reinjection servers, see “Outbound Concepts” on page 508.

When you add a new IP range to Outbound Services, the message security service automatically verifies that your reinjection servers are working. Use the ReInjection Test to verify that your existing reinjection servers are still working.

The ReInjection Test connects to every reinjection server you have listed in Outbound Servers and attempts to send a private relay. If the private relay attempt is successful, the ReInjection Test passes for that reinjection server. If not, the ReInjection Test displays an error for that reinjection server.

To run the ReInjection Test:

1. Go to the Administration Console welcome page.
2. In the bottom left corner, under System Tests, click ReInjection Test.
3. The ReInjection Test will run.

Successful Results for the ReInjection Test

On a successful test, the ReInjection Test will show the host name and the text "Ok." This means that your reinjection server is accepting relay messages from the message security service.

Error Messages and Next Steps

If the ReInjection Test fails for a reinjection server, that server may not be able to act as a reinjection server properly. You will see the results of the test.

See the table below for details on which errors you may run into, and the next steps you should take.

For information on setting your reinjection server in the Administration Console, see "Setting Up Outbound Filtering" on page 511.

Error: 0.0.0.0	The reinjection server you have listed is 0.0.0.0, an invalid address. Enter a proper reinjection server in the Administration Console.
Error: <host> is the service IP	Your reinjection server is set to an IP address used by the message security service. Enter a proper reinjection server in the Administration Console.
Error: <host> points back to the service	Your reinjection server is set to a host name that resolves to the message security service. Enter a proper reinjection server in the Administration Console.

Error: Could not resolve host: <host>	Your reinjection server is set to a host name that does not resolve. Enter a proper reinjection server in the Administration Console.
Error: <host> has a MX record that points back to the service	Your reinjection server has an MX record that resolves to the message security service. Change your MX records or enter a proper reinjection server in the Administration Console.
Error: <host> had an unresolvable MX record	Your reinjection server has an MX record that does not resolve. Change your MX records or enter a proper reinjection server in the Administration Console.
Error: Relaying was not allowed for <host>	Your reinjection server resolves to a valid IP, but your server won't relay mail from the reinjection server. Check your firewall and mail server settings to ensure that your reinjection server allows a private relay for the message security service.

Troubleshoot Incoming Email Delivery

A mail delivery emergency is when some or all of your users are receiving no email. This is typically due to one of the following root causes:

- Your mail server configuration is incorrect.
- Incorrect configuration of the message security service.
- MX records configured incorrectly.
- Loss of connectivity to or from your mail server.

If you have problems sending or receiving certain types of messages—for example, if messages are unexpectedly quarantined or bounced—the issue may be a result of filter settings rather than mail delivery. In this case, message headers can help determine the reason. See “Interpreting Header Fields” on page 637 for more information.

Troubleshooting Instructions

Follow these step-by-step troubleshooting instructions before contacting support for assistance. This procedure should take approximately 15 minutes.

To follow the examples, use these references:

- Your domain name is *your_domain.com*
- Your mail server name is *your_mailserver.your_domain.com*
- Your MX records may be *your_domain.com.mailN.psmtp.com* --or-- *your_domain.com.sNaN.psmtp.com* --or-- *sNaN.psmtp.com*.
- A valid user on your mail server is *user@your_domain.com*

If the answer to each question below is “Yes”, move on to the next step. If the answer is “No”, attempt to address the issue raised.

- **Was the message quarantined by the Attachment Manager or Content Manager?**

If a message was not delivered, check to see if it was quarantined by Attachment Manager or Content Manager in the user or administrator quarantine. Also, send a test message from an account that’s in the Approved Senders list to verify that messages are not quarantined by improperly configured Attachment Manager or Content Manager filters.

Action: If your mail delivery problem is limited to certain types of messages or from specific users, see “Troubleshoot False Positives” on page 306.

- **Do the service monitoring systems or support show that email delivery is currently functioning?**

This step confirms the email protection service status. See the Apps Status Dashboard at www.google.com/appsstatus.

.

Action: If the Apps Status Dashboard or your support site show that there's an issue with email delivery, there is no reason to call Customer Care. Customer Care is working on the issue and will post updates as they are available.

- **Can you send email directly to your mail server?**

This step determines whether the problem is with your mail server connection. You test SMTP port 25 connections to your mail server to see whether email can be delivered without the message security service.

- a. Go to the home page (click the logo in the upper left-hand corner) and click SMTP Message Test link in the bottom left-hand corner.
- b. Use the SMTP Message Test to test an email from the data center directly to your mail host. Select the option: "Test an email from the data center directly to your mail host". and click Test
- c. Check your mail server to verify that the email was delivered. If you do not receive the message, there is an issue with your mail server. See "Successful Results for SMTP Test" on page 532 and "Error Messages and Next Steps" on page 534 for more information.

Action: Please consult with your network administrator or support resources for issues with your mail server or firewall.

- **Are the MX records for the domain set up correctly?**

This step checks whether the MX records that route your email to the message security service are configured correctly.

Check the format for the MX records in the Administration Console.

- a. Go to the home page (click the logo in the upper left-hand corner), and click MX Record Test link in the bottom left-hand corner.
- b. Choose the domain you want to check.
- c. Click Test. The results appear on the bottom of the page.

Action: If the MX records for this domain are incorrect, correct or add new records.

Note: Changes to the MX records take time to propagate. See the next step for more information.

- **Have the MX record changes propagated?**

This step determines whether your email delivery issues may be due to delays in changes in MX records taking effect.

Updates to MX records take time to propagate through the Internet. If you have recently updated your MX records, check your time to live (TTL) to see how long this process will take. In this example, the TTL is 10 minutes (10M). You may see TTL also expressed in seconds:

```
jumboinc.com. 10M IN MX 100 s5a1.psmtplib.com
```

Action: Wait the duration of the TTL setting to see if the MX record changes take effect. In the future, you may want to lower your TTL settings to decrease the propagation time (changes made now will not affect the current MX record propagation time).

- **Can your mail server communicate with the message security service across the Internet?**

This step determines whether mail can be sent through the message security service to your mail servers.

- Go to the home page (click the logo in the upper left-hand corner), and click SMTP Message Test link in the bottom left-hand corner.
- On the SMTP Message Test page, enter the email address of a user to be used as the message recipient. You can also enter a user alias, but not a domain alias.
- Select the option, “Test mail flow through the data center” and click Test. See “Successful Results for SMTP Test” on page 532 and “Error Messages and Next Steps” on page 534 for more information on test results.

Action: If there is an error, this indicates a configuration error on your mail server. Check your mail server logs for the associated SMTP error and correct the configuration.

- **Can your mail server use the traceroute command to communicate through the Internet to the message security service?**

- This step tests direct network connectivity from your mail server to the message security service. To test this, log on to your email server, and perform a *traceroute* to the message security service using the highest priority DNS record. For example,

```
> traceroute sNaN.psmtplib.com
```

- Go to Inbound Servers > Delivery Manager.
- Click the Latency Test link in the lower right-hand corner of the page.
- Enter the hostname of your email server.
- Click Test. The results appear on the bottom of the page.
- Compare these results to the traceroute results (from step a). See “Interpret Traceroute Test Results” on page 541 for information.

You should receive back at least one line with `att.net`, `cw.net`, `exodus.net`, or `alter.net` in it. If you do not, there is a network issue between your mail server and the message security service.

Action: There is a networking issue with your mail server. Consult with your network administrator or network support for assistance.

Alerts can proactively notify you when this type of event occurs. Please see “Setting Up Alerts” on page 489 for configuration steps.

- **Is your domain correctly associated with an organization and email config?**

This step determines whether the email delivery problem is with the domain, email config, or organization configuration.

- a. In the Administration Console, go to Orgs and Users > Domains.
- b. Check whether the domain is associated with an organization. If it is not, add the domain to an organization.
- c. Check that the organization is associated with an email config by clicking the Show Hierarchy link in the top menu bar. The organization should be below an email config, or be a sub-org below an email config.

Action: Fix the domain and organization settings and then send a test email to an account in the domain.

- **Does the email config have the correct mail server name?**

This step determines whether the issue is due to incorrect mail server name associated with the email config.

- a. In the Administration Console, go to Inbound Servers > Delivery Manager.
- b. Select the email config from the Choose Org pull-down list.
- c. Click the Edit link in the grey bar to view the mail server settings.
- d. Verify the value in the Email Servers field. Delivery Manager sends mail to this server. This can be either a name or an IP address. If this field is empty or has the incorrect value, you can change it here. (You may see a “% Conn” field next to the Email Server. If the “% Conn” field is blank, this means 100% of load goes to this mail server.)

Action: Fix the mail server name and then send a test email to an account associated with the email config.

- **Is your email being spooled?**

If the email processing service cannot reach your mail server, your email may be spooling for later delivery. By default, Spool Manager will automatically unspool your mail, however, if your Unspooling Control is set to manual, then you must manually start the unspooling process once your mail server is available.

- a. In the Administration Console, go to Inbound Servers > Spool Manager.
- b. Select the email config from the Choose Org pull-down list.
- c. Click the Edit link in the grey bar to view the Spool Manager settings.
- d. If mail has been spooled, you can click the Start Unspooling button in the Unspooling Control section.

Action: Unspool your mail and check that messages have arrived. After unspooling is complete, configure Automatic Unspooling.

- **Contact Support.**

If you have followed the steps above and still require assistance, contact Support for assistance.

Chapter 26

Reports

About Reports

Reports provide visibility into the traffic patterns across your organization. The Administration Console produces different traffic reports based on your product configuration.

Reporting provides extensive analysis into email message traffic, spam, virus, and usage over a day or week. You may also download report data and import it into reporting or spreadsheet software for further analysis.

The following reports are produced by the message security service:

- Daily reports for the previous calendar day
- Custom date range reports from the past 6 weeks
- Current day traffic logs for Content Manager and Outbound Messages

Reports containing the data from the previous day are generally available around mid-morning Pacific Time, the following day. The time of availability fluctuates with quantity of traffic processed.

The reports displayed in the Administration Console show the top 20 results. You can also click the Download link to download reports in a comma-delimited list.

Note: For information on Postini Message Archiving reports, see the “Creating Message Archiving Reports” chapter in the *Postini Message Archiving Administration Guide*.

View a Report

Viewing a report requires selecting the org you wish to report on, specifying whether or not to include sub-orgs in the report, choosing either the daily or the weekly version of the report, and choosing the report type. Viewing a report is described in the steps that follow.

To view a report:

1. In the Administration Console, click the **Reports** tab.
2. Select the organization from the pull-down list. The total number of registered users in organization, including sub-orgs, is displayed above the reports list.

Choose Org: Jumbo Inc. Corporate Account ▾

Detailed Reporting - Jumbo Inc. Corporate Account

Registered Users: 0 (includes sub-orgs)

Inbound	Outbound
Traffic Domain Recipient	Traffic Domain Account Activity Log
Spam Domain Filter Name Account	Virus Domain Account Virus Name
Virus Sender IP Domain Virus Name Account	Content Manager Domain Account Activity Log
Attachments Domain	Attachments Domain

3. Click the report name. You'll see a page similar to this:

Inbound Traffic by Domain - From 11-07-2006 to 11-07-2006 (1 day)

Domain	Messages	Bytes	Acct Msgs	Forwarded Acct Msgs	% of Msgs
jumboinc.com	4,484	6,322,981	4,484	3,895	86.9
Grand Total	4,484	6,322,981	4,484	3,895	86.9

Notes about the report results:

- The reports displayed in the Administration Console show the top 20 results
 - Reports containing the data from the previous day are generally available around noon, Pacific Time, the following day. The time of availability fluctuates with quantity of traffic processed.
4. By default, **Include sub-orgs** is selected, and the report includes data from the sub-orgs. For a report with only data for a specific organization, clear **Include sub-orgs**, and click **Run Report**.

5. Optionally, select the date range and click **Run Report**.



The screenshot shows a report generation interface. It includes a 'Report Length' section with two date pickers, both set to '12 Oct'. Between the date pickers is the text 'to'. To the right of the date pickers is a checked checkbox labeled 'Include sub-orgs'. Further right is a button labeled 'Run Report'.

6. To download a report, click the **Download** link located in the upper right corner of the screen. The report is opened in a new browser window that presents the data in CSV format so it can easily be saved and imported into most reporting and spreadsheet software for further analysis or storage.

The download report provides a comma-delimited list and is ideal when you wish to view more than the top 20 results.

Inbound and Outbound Reports

Following are descriptions of the reports for incoming and outgoing mail traffic. The list of reports in the Administration Console depends on your configuration. For example, you do not see the Content Manager reports unless you have this feature, and have turned it on.

Outbound service is an optional feature; whether the Outbound Reports are displayed depends on your product configuration.

Summary Reports

Summary reports calculate the totals for various types of report for a specific domain -- for example, Spam, Virus, Attachment Manager, and Content Manager reports. The totals are summarized in two different types of report -- the total messages processed and the total bytes processed for that domain.

Summary by Domain Messages

This report displays the total messages processed for various types of reports for a specific domain.

Two types of Summary by Domain Messages reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Domain Messages (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical (with the exception of "Domain Message Traffic"), and each report has the same total messages processed.

Field	Description
Domain Message Traffic (or) Domain with sub-domains	Domain to which messages were sent.
Filtered Good	Number of messages that are forwarded. This does not include messages forwarded as "Delivered from quarantine."
Unfiltered	Number of unregistered account messages that are passed through unfiltered.
Spam	Number of spam messages detected and quarantined.
Virus	Number of virus messages detected and quarantined.
Attachment Manager	Number of messages filtered by Attachment Manager.
Content Manager	Number of messages filtered by Content Manager.
Other Filters	Number of messages blocked by other filters, such as SPF and TLS.
Total Messages	Total number of messages processed for this domain.

Summary by Domain Bytes

This report displays the total bytes processed for various types of reports for a specific domain.

Two types of Summary by Domain Bytes reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Domain Bytes (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical (with the exception of "Domain Message Traffic") and each report has the same total bytes processed.

Field	Description
Domain Message Traffic (or) Domain with sub-domains	Domain to which messages were sent.
Filtered Good	Total bytes of messages that are forwarded. This does not include messages forwarded as "Delivered from quarantine."
Unfiltered	Total bytes of unregistered account messages that are passed through unfiltered.
Spam	Total bytes of spam messages detected and quarantined.
Virus	Total bytes of virus messages detected and quarantined.
Attachment Manager	Total bytes of messages filtered by Attachment Manager.
Content Manager	Total bytes of messages filtered by Content Manager.
Other Filters	Total bytes of messages blocked by other filters, such as SPF, DKIM, IP Lock, and TLS.
Total Messages	Total bytes of messages processed for this domain.

Traffic Reports

Traffic Reports give you visibility into traffic sources and destinations for messages that are quarantined or forwarded to the recipient. Mail that is bounced or blackholed is not recorded in the reports. By clicking links embedded within the report data, you can see granular data regarding which IP addresses are sending messages to specific users.

Traffic by Domain (Inbound)

This report shows inbound mail traffic information for the domains in the selected organization.

Two types of inbound Traffic by Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Traffic by Domain (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Domain	Domain to which messages were sent.
Messages	Total number of messages passed through the message security service.
Bytes	Total size of messages in bytes.
Acct Messages	<p>Account Messages. The number of filtered email messages sent to accounts and aliases <i>registered</i> in the message security service.</p> <p>There may be a difference between Messages and Acct Msgs numbers. This is because the Messages number includes all messages passing through the system that are accepted by your mail server, but Acct Msgs only counts messages sent from the message security service to registered accounts and aliases.</p> <p>If you have a catchall account set up for a domain, all emails for that domain are considered Acct Messages.</p> <p>Note: Catchall account is a legacy feature that is available to some customers. It may not be available for your service.</p>
Forwarded Acct Msgs	Number of Account Messages delivered directly to your mail server for all addresses in the domain.
% of Msgs	Percent of Account Messages delivered.
% of Bytes	Percent of Account Message bytes delivered.
Blocked Acct Msgs	Number of Account Messages blocked by Blatant Spam Blocking, Virus Blocking, Attachment Manager and Content Manager (Attachment Manager and Content Manager are optional features).
% of Msgs	Percent of Blocked Acct Msgs delivered.
% of Bytes	Percent of bytes delivered.
Quarantined Acct Msgs	Number of Acct Messages quarantined.
% of Msgs	Percent of Quarantined Acct Msgs delivered.
% of Bytes	Percent of bytes delivered.

Traffic by Domain (Outbound)

Outbound mail traffic information for the domains in the selected organization:

Field	Description
Domain	The domain from which the messages were sent.
Msgs Deliv	Number of messages delivered.
% Deliv	Percent of messages delivered.
Msgs Bounced	Number of messages bounced.
% Bounced	Percent of messages bounced.
Msgs Quarantined	Number of messages quarantined.
% Quarantined	Percent of messages quarantined.
Total Msgs Processed	Total number of messages processed.
Bytes Processed	Total number of bytes processed.

Traffic by Recipient (Inbound)

This report shows inbound mail traffic information for the users in the selected organization.

Two types of inbound Traffic by Recipient reports are available. One report generates only the primary email addresses in the results. A second type of report -- the **Traffic by Recipient (& aliases)** report -- includes aliases in the results exactly as they were received without any mapping to a primary email address. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Recipient	Email address of recipient account.
Messages	Total number of messages passed through the message security service.
Bytes	Total size of messages in bytes.

Field	Description
Acct Messages	<p>The number of email messages sent to accounts and aliases registered in the message security service.</p> <p>There may be a difference between Messages and Acct Msgs numbers. This is because the Messages number includes all messages passing through the system that are accepted by your mail server, but Acct Msgs only counts messages sent to registered accounts and aliases.</p> <p>Emails processed under a catch-all account are also included in the Acct Messages number.</p> <p>The number of virus-infected messages that are blocked because of Non-Account Virus Blocking is also included in the Acct Msgs column (see “Inbound Traffic Reports and Non-Account Virus Blocking” on page 558).</p>
Forwarded Acct Msgs	Number of Msgs delivered directly to your mail server for the account.
% of Msgs	Percent of Acct Msgs delivered.
% of Bytes	Percent of bytes delivered.
Blocked Acct Msgs	Number of Acct Messages blocked by Blatant Spam Blocking, Attachment Manager and Content Manager (Attachment Manager and Content Manager are optional features).
% of Msgs	Percent of Blocked Acct Msgs delivered.
% of Bytes	Percent of bytes delivered.
Quarantined Acct Msgs	Number of Acct Messages quarantined.
% of Msgs	Percent of Quarantined Acct Msgs delivered.
% of Bytes	Percent of bytes delivered.

Inbound Traffic Reports and Non-Account Virus Blocking

Non-Account Virus Blocking protects your domains by automatically deleting virus-infected messages that are sent to unregistered users (addresses in a domain associated with this organization but that are not registered with your message security service).

Messages that are blocked by Non-Account Virus Blocking appear in the Inbound Traffic Report as “account messages” for the recipient address.

For example, if unregistered user “jsmith@domain.com” receives 10 messages and one is blocked by Non-Account Virus Blocking, the inbound traffic report (by recipient) will show that jsmith@domain.com received 10 total messages, 1 account message, and had 1 message blocked.

Traffic by Account (Outbound)

Outbound mail traffic information for the accounts in the selected organization:

Field	Description
Sender	Address from which messages were sent.
Account	Whether the sender has an account in the message service (Y or N).
Msgs Deliv	Number of messages delivered.
% Deliv	Percent of messages delivered.
Msgs Bounced	Number of messages bounced.
% Bounced	Percent of messages bounced.
Msgs Quarantined	Number of messages quarantined.
% Quarantined	Percent of messages quarantined.
Total Msgs Processed	Total number of messages processed.
Bytes Processed	Total number of bytes processed.

Traffic Activity Log (Outbound)

The Outbound Traffic logs show the detailed data for outgoing messages.

The logs contain data from 20 minutes prior. The timestamps are in PST. The log contains a maximum of 5000 lines of data (the lines are tab-delimited.) Once the size limit is reached, logging continues, with the oldest data deleted first. A sample log entry looks like:

```
2007/11/07 10:13:21 IP:888.888.888.888 IPOrg:000000000
From:kristine@jumboinc.com User:999999999 Org:111111111
Recipients:helene@hugeisp.com Header:760 Size:5616 Disposition:f
Subject:How's the Weather?
```

Following are the descriptions of each field in the log.

Field	Description
IP	The IP of the outbound mail server transmitting the message.
IP Org	The org ID of the outbound email config.
From	The sender address if there is one.
User	The user ID of the user who sent the message, or 0 if there is no associated user.

Field	Description
Org	The org ID of the org which contains the user. If there is no "From" address or no registered user, then this ID is the same as the IP org.
Recipients	All recipient addresses for the message.
Header	The header length in bytes
Size	The message size in bytes
Disposition	The disposition of the message (f=forwarded, q=quarantined, i=reinjected)
Subject	The subject of the message sent.

The following logs are available:

Log	Description
Outbound Traffic Log	Data for the most-recent 24-hour period for the selected org.
Outbound Traffic Log - includes sub-orgs	Data for the most-recent 24-hour period for the selected org and its sub-orgs.

Spam Reports

Spam Reports give a list of the domains that are sending spam, the users receiving spam, and provide detailed information on the most active spam filters.

Spam by Domain (Inbound)

This report shows spam messages quarantined for each domain in the selected organization.

Two types of inbound Spam by Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Spam by Domain (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Domain	Domain to which messages were sent.
Spam	Number of spam messages quarantined.
Spam Bytes	Total size of quarantined spam messages.

Field	Description
Bulk Mail	General category for junk email filtering (may include characteristics of the other specific filter categories).
Special Offer	Number of messages triggering the Special Offer junk email filter.
Get Rich Quick	Number of messages triggering the Get Rich Quick junk email filter.
Sexually Explicit	Number of messages triggering the Sexually Explicit junk email filter.
Racially Insensitive	Number of messages triggering the Racially Insensitive junk email filter.
Blatant Spam Blocking	Number of messages blocked as obvious spam by Blatant Spam Blocking.
Blocked Sender	Messages quarantined because the specific sender address was listed in either the user or org-level Blocked Senders list.
Blocked Server	Messages quarantined because the domain was listed in a Blocked Senders list, not a specific address.

Spam by Filter Name (Inbound)

Number of messages quarantined by each category filter.

Field	Description
Special Offer	Number of messages triggering the Special Offer junk email filter
Bulk Mail	General category for junk email filtering (may include characteristics of the other specific filter categories)
Get Rich Quick	Number of messages triggering the Get Rich Quick junk email filter
Sexually Explicit	Number of messages triggering the Sexually Explicit junk email filter
Blocked Sender	Messages quarantined because the specific sender address was listed in either the user or org-level Blocked Senders list
Blocked Server	Messages quarantined because the domain was listed in a Blocked Senders list, not a specific address
Racially Insensitive	Number of messages triggering the Racially Insensitive junk email filter

Field	Description
Blatant Spam Blocked	Number of messages blocked as obvious spam by Blatant Spam Blocking

Effective Catch Rate (Inbound)

Number of messages per domain identified as spam, how many of those messages were delivered, and the reasons for delivery.

Field	Description
Domain	Domain to which the messages were sent.
Identified Spam Messages	Number of messages identified as spam.
Delivered Spam Messages	Number of spam messages delivered to domain users.
Delivered to registered Users	Number of spam messages delivered to users registered with the message security service.
Delivered due to Org approval	Number of spam messages delivered because the senders were approved at the org level.
Delivered due to User approval	Number of spam messages delivered because the senders were approved by users.
Delivered due to Filter off	Number of spam messages delivered because users had spam filtering turned off, or because spam filtering was bypassed due to another user configuration setting. For example, if a Content Manager filter triggers, and if that filter is configured with a Deliver disposition, the message will be delivered without a spam scan.
Delivered due to Tag and Deliver	Number of spam messages delivered because the org is configured to tag and deliver.
Delivered due to Unregistered Users	Number of spam messages delivered because the recipients were not registered with the message security service.
Delivered due to other reasons	Number of spam messages delivered because of unknown reasons or reasons not identified in this report.
Catch Rate % All users	Effective catch rate for all spam messages. (Total Spam - Total Spam Delivered) / Total Spam = %

Field	Description
Catch Rate % Registered users	Effective catch rate for spam messages addressed to users registered with the message security service. (Total Spam - Spam Delivered to Registered Users) / Total Spam = %

Effective Catch Rate by Org (Inbound)

Number of messages per org identified as spam, how many of those messages were delivered, and the reasons for delivery.

Field	Description
Org	Org to which the messages were sent.
Identified Spam Messages	Number of messages identified as spam.
Delivered Spam Messages	Number of spam messages delivered to org users.
Delivered to registered Users	Number of spam messages delivered to users registered with the message security service.
Delivered due to Org approval	Number of spam messages delivered because the senders were approved at the org level.
Delivered due to User approval	Number of spam messages delivered because the senders were approved by users.
Delivered due to Filter off	Number of spam messages delivered because users had spam filtering turned off.
Delivered due to Tag and Deliver	Number of spam messages delivered because the org is configured to tag and deliver.
Delivered due to Unregistered Users	Number of spam messages delivered because the recipients were not registered with the message security service.
Delivered due to other reasons	Number of spam messages delivered because of unknown reasons or reasons not identified in this report.
Catch Rate % All users	Effective catch rate for all spam messages. (Total Spam - Total Spam Delivered) / Total Spam = %
Catch Rate % Registered users	Effective catch rate for spam messages addressed to users registered with the message security service. (Total Spam - Spam Delivered to Registered Users) / Total Spam = %

Spam by Account (Inbound)

Spam statistics at the account level. This includes most of the same fields as the Spam by Domain (Inbound), and the field Delivered from Quarantine, which is the number of messages delivered from quarantine to the user's mailbox.

Note: Messages delivered from the User Quarantine page in the Administration Console are not included in the Spam by Account Report.

Field	Description
Account	Registered user's primary address. The report totals include messages sent to the primary address and any associated aliases.
Spam	Number of spam messages.
Spam Bytes	Total size of quarantined spam messages.
Bulk Mail	General category for junk email filtering (may include characteristics of the other specific filter categories).
Special Offer	Number of messages triggering the Special Offer junk email filter.
Get Rich Quick	Number of messages triggering the Get Rich Quick junk email filter.
Sexually Explicit	Number of messages triggering the Sexually Explicit junk email filter.
Racially Insensitive	Number of messages triggering the Racially Insensitive junk email filter.
Blatant Spam Blocking	Number of messages blocked as obvious spam by Blatant Spam Blocking.
Blocked Sender	Messages quarantined because the specific sender address was listed in either the user or org-level Blocked Senders list.
Blocked Server	Messages quarantined because the domain was listed in a Blocked Senders list, not a specific address.
Delivered from Quarantine	<p>Number of messages delivered to the user's inbox from quarantine (either directly from the users's quarantine or a quarantine redirect).</p> <p>Note: Spam by Account reports only include users who deliver quarantined messages on the day they actually receive the spam (some users may delay for a day or two before delivering to their inbox). To view a report with more details on quarantine deliveries, view the Quarantine Delivery Activity Log (see "Quarantine Delivery Reports" on page 579.)</p>

Email Authentication Reports (SPF Check)

Some organizations publish Sender Policy Framework (SPF) records to help reduce email spoofing of their domains. SPF records include a range of IP addresses that are authorized to send mail on a domain's behalf. To help reduce the chance that your users will receive spoofed emails, you can enable the SPF Check feature at the Email Config level in the Administration Console (see "Enabling SPF Check" on page 503).

Note: SPF Check is available for *Google Message Security* customers only.

SPF by Sender Domain

Field	Description
Sender Domain	Sender's domain name.
Pass	Number of messages with an SPF Check that passed successfully.
None/Neutral	Number of messages where no SPF record was found during the SPF Check.
Soft Fail	Number of messages with the Soft Fail response type during the SPF Check.
Fail	Number of messages with the Fail response type during the SPF Check.
Error	Number of messages that triggered an error during the SPF Check.
Total Messages	Total number of SPF Check messages for a sender domain.

SPF by Recipient Domain

Two types of inbound SPF by Recipient Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **SPF by Recipient Domain (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Recip Domain	Recipient's domain name.
Pass	Number of messages with an SPF Check that passed successfully.
None/Neutral	Number of messages where no SPF record was found during the SPF Check.

Field	Description
Soft Fail	Number of messages with the Soft Fail response type during the SPF Check.
Fail	Number of messages with the Fail response type during the SPF Check.
Error	Number of messages that triggered an error during the SPF Check.
Total Messages	Total number of SPF Check messages for a recipient domain.

Virus Protection Reports

Virus Reports show which viruses are being sent to and from your servers, from where, at what times. User virus activity is included.

Note: Messages that are blocked by Non-Account Virus Blocking appear in the Inbound Traffic Report as “account messages” for the recipient address (see “Inbound Traffic Reports and Non-Account Virus Blocking” on page 558).

Virus by Sender IP (Inbound)

Per sender IP, the total number of quarantined viruses and the total size of viruses in bytes.

Field	Description
Sender IP	Sender’s IP address.
Viruses detected	Number of viruses detected and quarantined.
Virus Bytes	Total size of viruses detected and quarantined.

Virus by Domain (Inbound)

Per domain name, the total number of viruses blocked for the domain, and total byte size of blocked viruses.

Two types of inbound Virus by Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Virus by Domain (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Domain	Domain to which messages were sent.
Viruses detected	Number of virus-infected messages for that domain.
Virus Bytes	Total size of virus-infected messages sent to that domain.

Virus by Domain (Outbound)

Per domain name, the number and percent of virus-infected messages bounced and quarantined, and the total number and size of virus-infected messages processed.

Field	Description
Domain	Domain to which virus-infected messages were sent.
Msgs Bounced	Number of virus-infected messages bounced.
% Bounced	Percent of virus-infected messages bounced.
Msgs Quarantined	Number of virus-infected messages quarantined.
% Quarantined	Percent of virus-infected messages quarantined.
Total Msgs Processed	Total number of virus-infected messages processed.
Bytes Processed	Total size of virus-infected messages processed.

Virus by Account (Inbound)

Per account, the number of viruses quarantined, the total byte size of quarantined viruses, the number of viruses cleaned, the number of virus cleaning failures, and the number of infected deliveries from quarantine.

Field	Description
Account	Recipient's account. This is normally the recipient's email address, but in the case of an alias, the primary address is used.
Viruses Detected	Number of virus-infected messages sent to that account.

Field	Description
Virus Bytes	Total size of virus-infected messages sent to that account.
Viruses Cleaned	Number of messages successfully cleaned and delivered to the recipient. Only applicable if your virus settings allow clean and deliver.
Virus Cleaning Failures	Number of messages that the message security service attempted to clean but was unable to clean. Only applicable if your virus settings allow clean and deliver.
Infected Deliveries from Quarantine	Number of infected messages manually delivered from the quarantine to the recipient. Only applicable if your virus settings allow delivery of infected messages.

Virus by Account (Outbound)

Per account, the number and percent of virus-infected messages bounced and quarantined, and the total number and size of virus-infected messages processed.

Field	Description
Sender	Address from which messages were sent.
Account	Whether the sender has an account in the message service (Y or N).
Msgs Bounced	Number of virus-infected messages bounced.
% Bounced	Percent of virus-infected messages bounced.
Msgs Quarantined	Number of virus-infected messages quarantined.
% Quarantined	Percent of virus-infected messages quarantined.
Total Msgs Processed	Total number of virus-infected messages processed.
Bytes Processed	Total size of virus-infected messages processed.

Virus by Virus Name (Inbound)

By virus name, the number of quarantined messages containing that virus, and total byte size for that virus.

Field	Description
Virus Name	Name of the virus, based on virus filtering data.
Viruses detected	Number of virus-infected messages of that virus type.

Field	Description
Virus Bytes	Total size of virus-infected messages of that virus type.

Virus by Virus Name (Outbound)

Per virus name, the number and percent of virus-infected messages bounced and quarantined, and the total number and size of virus-infected messages processed.

Field	Description
Virus Name	Name of the virus, based on virus filtering data.
Msgs Bounced	Number of virus-infected messages bounced.
% Bounced	Percent of virus-infected messages bounced.
Msgs Quarantined	Number of virus-infected messages quarantined.
% Quarantined	Percent of virus-infected messages quarantined.
Total Msgs Processed	Total number of virus-infected messages processed.
Bytes Processed	Total size of virus-infected messages processed.

Attachment Manager Reports

Attachment Manager is an optional feature; whether the Attachment Manager Reports are displayed depends on your product configuration.

Attachments by Domain (Inbound)

Per domain, the number of messages with attachments, and how those messages were handled by the system.

Two types of inbound Attachments by Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Attachments by Domain (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Domain	Domain to which messages were sent.
With Attachments	Number of messages with attachments passed through the message security service.

Field	Description
Messages Filtered	Number of messages with attachments filtered by the message security service.
Quarantined	Number of messages with attachments quarantined.
Bytes Quarantined	Total size of quarantined messages with attachments.
Bounced	Number of messages with attachments bounced.
Bytes Bounced	Total size of bounced messages with attachments.
Size	Number of messages with attachments bounced by attachment size restrictions.
File Extension	Depending upon how you configured your Custom File Types filter, this item returns the number of messages with attachments either bounced, approved, or quarantined. The filtering is based upon the attachment's file extension.
System Threat	Depending upon how you configured your System Threat filter, this item returns the number of messages with attachments either bounced, approved, or quarantined. The filtering is based upon the attachment's file extension.
Productivity	Depending upon how you configured your Productivity filter, this item returns the number of messages with attachments either bounced, approved, or quarantined. The filtering is based upon the attachment's file extension.
% of Traffic	Percent of messages with attachments filtered in overall inbound traffic flow.

Attachments by Domain (Outbound)

Per domain, the number of messages with attachments, and how those messages were handled by the system.

Field	Description
Domain	Domain from which messages were sent.
Msgs Bounced	Number of messages bounced.
% Bounced	Percent of virus-infected messages bounced.
Msgs Quarantined	Number of messages quarantined.
% Quarantined	Percent of messages quarantined.
Total Msgs Processed	Total number of messages processed.

Field	Description
Bytes Processed	Total size of messages processed.

Attachments by Account (Inbound)

Per receiving account, the number of messages with attachments, and how those messages were handled by the system.

Field	Description
Account	Account to which messages were sent.
With Attachments	Number of messages with attachments passed through the message security service.
Messages Filtered	Number of messages with attachments filtered by the message security service.
Quarantined	Number of messages with attachments quarantined.
Bytes Quarantined	Total size of quarantined messages with attachments.
Bounced	Number of messages with attachments bounced.
Bytes Bounced	Total size of bounced messages with attachments.
Size	Number of messages with attachments bounced by attachment size restrictions.
File Extension	Depending upon how you configured your Custom File Types filter, this item returns the number of messages with attachments either bounced, approved, or quarantined. The filtering is based upon the attachment's file extension.
System Threat	Depending upon how you configured your System Threat filter, this item returns the number of messages with attachments either bounced, approved, or quarantined. The filtering is based upon the attachment's file extension.
Productivity	Depending upon how you configured your Productivity filter, this item returns the number of messages with attachments either bounced, approved, or quarantined. The filtering is based upon the attachment's file extension.
% of Traffic	Percent of messages with attachments filtered in overall outbound traffic flow.

Attachments by Account (Outbound)

Per sending account, the number of messages with attachments, and how those messages were handled by the system.

Field	Description
Sender	Address from which messages were sent.
Account	Whether the sender has an account in the message service (Y or N).
Msgs Bounced	Number of messages bounced.
% Bounced	Percent of virus-infected messages bounced.
Msgs Quarantined	Number of messages quarantined.
% Quarantined	Percent of messages quarantined.
Total Msgs Processed	Total number of messages processed.
Bytes Processed	Total size of messages processed.

Attachments by Filter (Inbound)

Per filter, the number and total size of messages with attachments.

Field	Description
Category	Filter category.
Messages	Number of messages caught by each filter.
Bytes	Total size of messages caught by each filter.

Content Manager Reports

Content Manager is an optional feature; whether the Content Manager Reports are displayed depends on your product configuration.

Domain/Account (Inbound)

By domain or account, the number of messages caught by your filters, the percentage of overall traffic represented by those messages, and the disposition applied to those messages.

Two types of inbound Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the **Domain (& sub-domains)** report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Domain/Account	Recipient's domain or account. For account, this is normally the recipient's email address, but in the case of an alias, the primary address is used.
Messages Filtered	Number of messages caught by a content filter.
% of Traffic	Percentage of overall traffic represented by the filtered messages.
Quarantined	Number of filtered messages sent to a quarantine.
Bounced	Number of filtered messages bounced back to the sender.
Blackholed	Number of filtered messages blackholed (deleted).

Note: If the routing option for a message were, for example, Delete (Blackhole), and the message were copied to two quarantines, then the message would be counted once in the Blackholed column, twice in the Quarantined column, and three times in the Messages Filtered column.

Domain/Account (Outbound)

By domain or account, the number of messages caught by your filters, and how those messages were handled by the system.

Field	Description
Domain (domain report)	Domain from which messages were sent.
Sender (account report)	Address from which messages were sent.
Account (account report)	Whether the sender has an account in the message service (Y or N).
Msgs Bounced	Number of messages bounced.
% Bounced	Percent of virus-infected messages bounced.
Msgs Quarantined	Number of messages quarantined.
% Quarantined	Percent of messages quarantined.
Msgs Relayed and Encrypted	Number of messages relayed and encrypted.
% Relayed and Encrypted	Percent of messages relayed and encrypted.
Total Msgs Processed	Total number of messages processed.
Bytes Processed	Total size of messages processed.

Note: If you use a routing option *and* one or more copy-to-quarantine options, you see the following data in your report: If the routing option for a message were, for example, Bounce, and the message were copied to two quarantines, then the message would be counted once in the Bounced columns, twice in the Quarantined columns, and three times in the Total Msgs Processed and Bytes Processed columns.

Filter Name (Inbound, Outbound)

The filter by which messages were caught, the disposition applied to messages caught by each filter, and the number of messages caught by each filter.

Field	Description
Filter Name	The name of the content filter that caught the messages.
Disposition	The disposition applied to messages caught by each filter.
Events	The number of messages caught by each filter.

Notes:

If you use a routing option *and* one or more copy-to-quarantine options, you see the following data in the Disposition column:

- One entry per filter for the routing option
- One entry per filter for each quarantine to which the message was copied

For example, if the routing option were Delete (Blackhole), and the message were copied to two quarantines, then there would be three entries for that filter. Each entry would have the same event count.

The Filter Name report does not include information about filters with the disposition of Message Encryption, if Message Encryption for the org or user is turned off.

Activity Log (Inbound, Outbound)

The Content Manager Activity Log report shows detailed information by date and time, sender, recipient, filter names, and message disposition. For example:

```
2008/09/26 13:53:35 bschmell@google.com train6@postinitraining.com  
online gamblin2,online gamblin2 blackhole,quarantine
```

Following are the descriptions of each field in the inbound and outbound logs.

Field	Description
Sender	Email address from which the message was sent.
Recipient	Email address to which the message was sent.
Filters Results	Filter and routing applied to the message.

The following logs are available:

Log	Description
Daily Log	Data for the most-recent 24-hour period for the selected org.
Daily Log - includes sub-orgs	Data for the most-recent 24-hour period for the selected org and its sub-orgs.
Weekly Log	Data for the most-recent 7-day period for the selected org.
Weekly Log - includes sub-orgs	Data for the most-recent 7-day period for the selected org and its sub-orgs.

The logs show data from 20 minutes prior. The timestamps are in GMT. The log contains a maximum of 5,000 lines of data (lines are tab-delimited). Once the size limit is reached, logging continues, with the oldest data deleted first.

Message Encryption Reports

Message Encryption is an optional feature; whether the Message Encryption Reports are displayed depends on your product configuration.

Message Encryption by Domain/Account (Outbound)

The domain from which messages were sent, and the number and size of messages encrypted and relayed.

Field	Description
Domain (domain report)	Domain from which messages were sent.
Sender (account report)	Address from which messages were sent.
Account (account report)	Whether the sender has an account in the message service (Y or N).
Msgs Encrypted and Relayed	Number of messages encrypted and relayed from each domain/sender.
% Msgs Encrypted and Relayed	Percent of messages encrypted and relayed from each domain/sender.
Bytes Encrypted and Relayed	Number of bytes encrypted and relayed from each domain/sender.
% Bytes Encrypted and Relayed	Percent of bytes encrypted and relayed from each domain/sender.
Total Msgs Processed	Total number of messages processed.

Message Encryption Activity Log (Outbound)

Message Encryption Logs are daily or weekly reports containing the details on outbound messages that were encrypted.

Following are the descriptions of each field in the logs.

Field	Description
Date	Date on which the message was sent.
Sender	Email address from which the message was sent.
Recipient	Email address to which the message was sent.
Bytes	Message size in bytes.

The following logs are available:

Log	Description
Daily Log	Data for the most-recent 24-hour period for the selected org.
Daily Log - includes sub-orgs	Data for the most-recent 24-hour period for the selected org and its sub-orgs.
Weekly Log	Data for the most-recent 7-day period for the selected org.
Weekly Log - includes sub-orgs	Data for the most-recent 7-day period for the selected org and its sub-orgs.

Archiving Reports

Message Archiving is an optional feature; whether the Message Archiving Reports are displayed depends on your product configuration.

Archiving by Domain (Inbound)

Domains to which archived messages were sent, journaled messages archived for registered and unregistered users, improperly formatted journaled messages, and the total number and size of messages.

Two types of inbound Archiving by Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the Archiving by Domain (& sub-domains) report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed.

Field	Description
Domain	Domain to which messages were sent.
Acct Msgs	Total number of messages archived for registered users.
Acct Bytes	Total size of messages archived for registered users.
Non-Acct Msgs	Total number of messages archived for unregistered users. Messages for unregistered users are archived only when you turn on archiving and use the "All journaled messages" option.
Non-Acct Bytes	Total size of messages archived for unregistered users. Messages for unregistered users are archived only when you turn on archiving and use the "All journaled messages" option.
Invalid Msgs	Total number of archived journal messages that were improperly formatted. Improperly formatted journal messages are archived only when you turn on archiving and use the "All journaled messages" option.
Invalid Bytes	Total size of archived journal messages that were improperly formatted. Improperly formatted journal messages are archived only when you turn on archiving and use the "All journaled messages" option.
Total Messages	Total number of messages archived.
Total Bytes	Total size of messages archived.

Archiving by Account (Inbound)

Address to which archived messages were sent, and the total number and size of messages.

Field	Description
Account	Recipient address to which messages were sent.

Field	Description
Total Messages	Total number of messages archived.
Total Bytes	Total size of messages archived.

Quarantine Delivery Reports

Activity Log (Inbound)

Quarantine Delivery Activity Logs are daily or weekly reports containing the details on messages that were delivered from the Message Center, or by clicking the Deliver button in the Quarantine Summary. The activity logs contain date, source of the delivery, sender, sender's domain, recipient, size, subject.

```
2007/01/18 03:45:12 MC barrie@hugeisp.com hugeisp.com
kristine@jumboinc.com 12345 IMPORTANT EMAIL
```

Following are the descriptions of each field in the inbound and outbound logs.

Field	Description
Date	Date the message was delivered from the Quarantine.
Delivered Method	Method by which the message was delivered from the quarantine.
Sender	Original sender of the message.
Domain	Domain from which the message was originally sent.
Recipient	Message recipient.
Size	Message size in bytes.
Subject	Subject line of message.

The source of delivery for a message in quarantine is always MC (Message Center). See "Deciding Which Approved Senders to Add" for details on how to use Quarantine Delivery Activity Log to determine what organization-level Approved Senders you should add.

Note: Messages delivered by administrators from the User Quarantine in the Administration Console are not recorded in these logs.

The following logs are available:

Log	Description
Daily Log	Data for the most-recent 24-hour period for the selected org.
Daily Log - includes sub-orgs	Data for the most-recent 24-hour period for the selected org and its sub-orgs.
Weekly Log	Data for the most-recent 7-day period for the selected org.
Weekly Log - includes sub-orgs	Data for the most-recent 7-day period for the selected org and its sub-orgs.

Field	Description
Domain/Account	Domain or recipient address to which messages were sent.
Total Messages	Total number of messages archived.
Total Bytes	Total size of messages archived.

TLS Reports

TLS (Transport Layer Security) is an optional feature; whether the TLS Reports are displayed depends on your product configuration.

TLS by Domain/Account (Inbound)

By domain or account, the total number and size of messages that passed through the message security service, and the number, size, and percent of messages transmitted by TLS.

Two types of inbound TLS by Domain reports are available. One report aggregates all messages for sub-domains and aliased domains to the primary domain. A second type of report -- the TLS by Domain (& sub-domains) report -- includes all sub-domains and domain aliases exactly as they were received without any mapping to a primary domain. The fields in these two reports are identical, and each report has the same total emails processed

Field	Description
Domain (domain report)	The recipient's domain (inbound).
Recipient (account report)	The recipient's address.

Field	Description
Msgs	Total number of inbound messages that passed through the message security service.
Msgs Bytes	Total size of inbound messages that passed through the message security service.
TLS msgs Sender Hop	Number of inbound messages that were transmitted by TLS between the sender and the message security service.
TLS bytes Sender Hop	Data size of inbound messages that were transmitted by TLS between the sender and the message security service.
%TLS msgs Sender Hop	Percentage of inbound messages sent that were transmitted by TLS between the sender and the message security service.
%TLS bytes Sender Hop	Percentage of inbound data that was transmitted by TLS between the sender and the message security service.
TLS msgs Recipient Hop	Number of inbound messages that were transmitted by TLS between the message security service and your mail server.
TLS bytes Recipient Hop	Data size of inbound messages that were transmitted by TLS between the message security service and your mail server.
%TLS msgs Recipient Hop	Percentage of inbound messages sent that were transmitted by TLS between the message security service and your mail server.
%TLS bytes Recipient Hop	Percentage of inbound data that was transmitted by TLS between the message security service and your mail server.

TLS by Domain/Account (Outbound)

By domain or account, the total number and size of messages that passed through the message security service, and the number, size, and percent of messages transmitted by TLS.

Field	Description
Domain (domain report)	The sender's domain.
Sender (account report)	The sender's address.
Msgs	Total number of outbound messages that passed through the message security service.

Field	Description
Msgs Bytes	Total size of outbound messages that passed through the message security service.
TLS msgs Sender Hop	Number of outbound messages that were transmitted by TLS between your mail server and the message security service.
TLS bytes Sender Hop	Data size of outbound messages that were transmitted by TLS between your mail server and the message security service.
%TLS msgs Sender Hop	Percentage of outbound messages sent that were transmitted by TLS between your mail server and the message security service.
%TLS bytes Sender Hop	Percentage of outbound data that was transmitted by TLS between your mail server and the message security service.
TLS msgs Recipient Hop	Number of outbound messages that were transmitted by TLS between the message security service and the recipient.
TLS bytes Recipient Hop	Data size of outbound messages that were transmitted by TLS between the message security service and the recipient.
%TLS msgs Recipient Hop	Percentage of outbound messages sent that were transmitted by TLS between the message security service and the recipient.
%TLS bytes Recipient Hop	Percentage of outbound data that was transmitted by TLS between your mail server and the message security service.

Policy-Enforced TLS by Domain (Inbound, Outbound)

By domain, the number and size of messages transmitted by Policy-Enforced TLS that passed through the message security service.

Field	Description
Domain	Domain of the recipient (inbound) or sender (outbound)
Msgs	Total number of messages that passed through the message security service.
Msgs Bytes	Total size of messages that passed through the message security service.

Troubleshooting Reports

Report data seems to be outdated. Why doesn't the report show data from today?

Report data is based on data from the previous day. The report shown is the latest report available. Generally reports for the previous day are available around noon (or earlier) Pacific Time the next day. The exact time of availability fluctuates with quantity of traffic processed.

Why does a domain show up in an organization report when that domain is not located in that organization?

There is at least one address in that domain which is aliased to a primary user account that is in the selected organization.

For example:

The user, `legal@domain.com`, and `domain.com` are registered in the organization "Corporate".

The user `legal@domain.com` has an alias `legal@domain.net`.

`domain.net` is registered in another organization, "Internal".

Quarantined messages for `legal@domain.net` count as statistics for the Message Center of `legal@domain.com`, and therefore count towards `domain.com`

How can statistics on falsely quarantined emails be determined?

An organization's Spam by Account report shows totals on the number of messages delivered from each user's Message Center. The totals include both falsely quarantined e-mails, and junk e-mails which a user wants delivered.

1. Click the Reports tab.
2. Click Spam by Account report.
3. Look at the "Delivered from Quarantine" column.
4. Optionally, click the "Download link" in the upper right-hand corner of the report window.

Reports will show all statistics for the organizations beneath the selected organization.

What is the difference between Messages and Account Messages in reports?

There may be a difference between Messages and Account Message numbers. This is because the Messages number includes all messages passing through the system that are accepted by your mail server, but Acct Msgs only counts messages sent to registered accounts and aliases.

Emails processed under a catch-all account are also included in the Account Messages number.

Any discrepancies should all be accounts for which the receiving mail server will return a 550 user unknown error, or accounts for which the message security service administrator has specifically chosen not to add an account associated with the message security service.

What is the difference between Blocked Senders & Blocked Servers in Spam Reports?

In the reports, Blocked Senders are messages quarantined because the specific sender address was listed in either the user or org-level Blocked Senders list.

Blocked Servers are messages quarantined because the domain was listed in a Blocked Senders list, not a specific address.

I don't have inbound Content Manager configured, yet it is appearing on the Reports tab. Why?

You have outbound Content Manager configured. Inbound Content Manager is included with outbound Content Manager, so configuring outbound Content Manager causes inbound Content Manager to appear on the Reports tab. This applies to Attachment Manager as well.

Chapter 27

Message Log Search

About Message Log Search

As the message security service processes your messages, data about these messages is captured and stored in a log. The Message Log Search feature enables you to run searches on this data using different criteria. You can then view the search results and drill down to details about specific messages.

Use Message Log Search to track messages for inbound and outbound traffic, and to track all messages for a specific sender, recipient, domain, or MTA address. You can also use Message Log Search to confirm whether a specific filter was triggered by a message and confirm the disposition. If necessary, you can later analyze filter settings that may be affecting traffic.

Note: Message Log Search data is managed and stored securely in Google data centers. At this time, Message Log Search is not offered to accounts on Systems 20. For more information, see “About the Data” on page 586.

To get started, click the Log Search tab in the Administration Console.

Your access to the Log Search tab depends on your authorization privileges. Access to Log Search is granted initially only to administrators who have View Reports privileges. For more information about Log Search privileges within your organization, see “Administrative Privileges for Message Log Search” on page 586.

In this chapter:

- “Run a Log Search” on page 587
- “Log Search Fields” on page 592
- “Common Log Search Scenarios” on page 606

About the Data

Note the following about Log Search data:

- Message Log Search data is available within approximately 3 hours of message processing (sent or delivered through the message security service), and messages remain in the log for approximately 45 days. If you want to save search results for later analysis, you can export a .csv file.
- As your messages are processed, information about the messages is captured and stored in a log, but the message security service does not store copies of these messages.
- The maximum number of messages that a Log Search query can return is approximately 15,000. Queries that return more than this limit result in an error message. If this occurs, you can refine your search by including additional criteria -- for example, you can search both by sender and recipient.
- Log Search data for Google Apps Gmail messages is captured for all intradomain mail. Note that separate message IDs will be logged for each message in a Gmail conversation.
- Log Search data is managed and stored securely in Google data centers. For more information, see the *Security and Privacy* help center article.

The Message Log Search feature is different from the Traffic Activity Log, which displays data for outgoing messages only. The Traffic Activity Log includes some fields with similar names to those available with Log Search, and contains data from 20 minutes prior. See “Traffic Activity Log (Outbound)” on page 559 for more information.

Administrative Privileges for Message Log Search

Administrators can use Log Search if they're assigned Modify privileges for this feature. Log Search access privileges are inherited automatically by administrators who have View Reports privileges for the same organization. If you want to add or remove Log Search privileges for an administrator, follow the steps below.

To set administrator privileges for Log Search:

1. From the Administration Console, click the Orgs and Users tab.
2. Click the Authorizations link on the tab bar.
3. Select the org from the Choose Org pull-down list.
4. Click the List button.
5. Click the View/Edit Profile link for a specific user.
6. Scroll down to the Organization Management section of the page.

7. To grant access to Log Search, select the Log Search check box in the Modify column. Clear this check box if you want to disallow access for that user.

Note: For more information about setting access privileges in the Administration Console, see “Descriptions of Privileges” on page 198“.

Run a Log Search

From the Log Search tab in the Administration Console, you can run queries based on the following criteria. Many log searches include the date range, sender, and/or recipient only; but you can also narrow your search by specifying inbound or outbound traffic, as well as the message disposition and other criteria:

- **Date range:** This range corresponds to the time zone for the organization in which you’re running the search. Select a date range that matches the date and time the message was sent. You can use a date range such as *Today*, *Yesterday*, *Last 7 days*, or *Last 30 Days*.

The time zone for an organization is displayed adjacent to the search fields -- for example, *America/New_York*. This format specifies a country or world region, followed by a specific location within that region.

- **From:** Enter the complete email address of the sender -- for example, *angela@cuppamocha.com*. You can also run a search by domain by entering the domain name of the sender -- for example, *cuppamocha.com*.
- **To:** Enter the complete email address of the recipient -- for example, *angela@cuppamocha.com*. You can enter multiple addresses in this field, and you can search by domain by entering the domain name of the recipient -- for example, *cuppamocha.com*. For multiple entries, place a comma or semicolon between each address or domain -- for example, *angela123@cuppamocha.com, dan456@cuppamocha.com, jeff789@cuppamocha.com*.
- **Direction:** Specifies whether your search includes inbound or outbound messages. If you leave this field blank, your search includes both inbound and outbound.
- **Disposition:** Narrows the search to include only messages that were processed in a specific way after passing through the message security service filters -- for example, *Quarantined*, *Bounced*, or *Encrypted*. Select the Disposition from the drop-down list.

- **Subject:** Find Log Search results by entering an exact or partial subject. Searches by subject are case insensitive. Non-ASCII characters are not supported for Subject searches.

Note: For searches on a partial subject, the results only match whole words. For example, if the subject is `Basketball Bracket`, the message will not appear in the results if you search on the words "ball" or "basket." However, if you enter the word `basketball`, the message will appear in the results.

- **Sender MTA:** Sender IP address (mail transfer agent).

Click **More search criteria** to display this field, and enter a numeric value -- for example, `74.125.67.100`.

- **Recipient MTA:** Recipient IP address (mail transfer agent).

Click **More search criteria** to display this field, and enter a numeric value -- for example, `74.125.67.100`.

- **User ID:** Unique number from the message security service that identifies the sender of an outbound message or the recipient of an inbound message. (A user's primary email address can be changed, but its ID always remains the same.) Click **More search criteria** to display this field.

To locate a User ID, log in to the Administration Console. Go to **Orgs and Users > Users**, and then click the relevant user to open the User Overview page. The User ID is displayed in the Summary box on the right side of the page.

Important: When running a Log Search, enter the system number as well as the User ID. For example, if the user's organization is on System 7 and the User ID is 200029564, enter the following in the User ID field: `7-200029564`

- **Org ID:** Unique number from the message security service that identifies the sender's Org ID for an outbound message or the recipient's Org ID for an inbound message. Click **More search criteria** to display this field.

To locate an Org ID, log in to the Administration Console. Go to **Orgs and Users > Orgs**, and then click the relevant organization to open the Organization Management page. The Organization ID is displayed in the Summary box on the right side of the page.

Important: When running a Log Search, enter the system number as well as the Org ID. For example, if the organization is on System 7 and the Org ID is 100003947, enter the following in the Org ID field: 7-100003947.

- **Content Filter:** Enables you to search by the name of the Content Manager filter. Searches on both exact and partial text are supported, and searches are case insensitive.
- **SMTP Message-ID:** A globally unique message identifier that's generated by the sender of a message. If present, the SMTP Message-ID is located in the message header.

Note: The *SMTP* Message-ID differs from the "Message ID," which is a unique identifier specific to the message security service.

The screenshot shows the "Log Search" interface with the following fields and values:

- Log Source:** SMTP Mail Flow (dropdown)
- From:** angela@cuppamocha.com
- Direction:** Inbound (dropdown)
- To:** (empty)
- Disposition:** Encrypted (dropdown)
- Subject:** staff meeting
- Sender MTA:** (empty)
- User ID:** (empty)
- Recipient MTA:** (empty)
- Org ID:** (empty)
- Content Filter:** (empty)
- SMTP Message-ID:** (empty)
- Disposition Filter:** (empty dropdown)
- Search:** (button)
- Using your own query will ignore the fields above.**
- Build my query:** (checkbox) (empty text box)

For additional details about these fields and their possible values, see "Log Search Fields" on page 592. For a description of typical uses for Message Log Search, see "Common Log Search Scenarios" on page 606.

Note: To run searches and view search results, an administrator must receive authorization privileges. If you have no access to the Log Search tab in the Administration Console, see "Administrative Privileges for Message Log Search" on page 586 for more information.

To run a Log Search:

1. From the Log Search tab, choose an organization from the **Choose Org** drop-down list at the top of the page.
2. Select a date range that matches the date and time the message was sent. This range corresponds to the time zone for the organization in which you're running the search. You can use a date range such as **Today**, **Yesterday**, **Last 7 days**, or **Last 30 Days**.

To enter a different date range, choose the **Custom date range** option, and enter the date and time using the following format of year/month/date:

2009/06/23 00:00

To narrow the range, you can also type the hours, minutes, and seconds in the above format.

3. From the Log Source drop-down list, choose **SMTP Mail Flow, Delivered from Quarantine, Dual Delivery, or Rescanner Delivery**.
4. Depending on the search scenario, enter the sender's address in the **From** field, enter the recipient's address in the **To** field. You can also enter the **Direction** and **Disposition**, or enter the **Subject** using both exact and partial searches (See "Common Log Search Scenarios" on page 606.)
5. To expand the search criteria, click **More search criteria**. This displays additional fields: **Sender MTA**, **Recipient MTA**, **User ID**, **Org ID**, **Content Filter**, and **SMTP Message-ID**, and **Disposition Filter**.

6. Click **Search** to open the search results page.

If you want to save a copy of your search results, click **Export Selected** or **Export All** to download a .csv file to your computer.

Note: In the heading row, click and drag the edges of a column to widen it.

7. To view details about a specific message, click the **Message ID** link to open the message details page (example shown below).

Note: The “Message ID” is a unique number for the message security service that identifies a specific message. It differs from the *SMTP Message-ID*, which is often found in the message header.

To view more details about a specific message recipient, expand the row for that recipient.

Message ID : 283366869278469070820

From: matthewsmith@ez4utech.com
 Direction: Inbound Date: 2009/09/10 00:23 Message Size: 149.3KB Sender MTA: 172.16.120.27 Customer ID: 100-100003708
 Session ID: ac12781b1dfbafef Proxy: exst3mxt Sender TLS: Domain Enforced Virus Name: Spam Score: 0.3752
 Commerce Score: 98.6951 Finance Score: 95.539 Legal Score: 95.539 Money Making Score: 97.0282 Sexually Explicit Score: 95.9108
 Racially Inensitive Score: 95.9108

To	User ID	Org ID	Recipient TLS	Recipient MTA	Disposition	Disposition Filter
hamrietamith@jumboinc.com	100-200029046	100-100003740	On	172.17.13.38	Delivered,Archived	
kevinamith@jumboinc.com	100-200029120	100-100003737	On	172.17.13.38	Delivered,Archived	
tedjones@jumboinc.com	100-200029131	100-100003755	On	172.17.13.38	Quarantined	bulk

Primary Address: tedjones@jumboinc.com

Archive Source:	Archive Users:	Archive Action:	Archive Info:	Attachment Setting:
Attachment Type:	Attachment Sender:	Attachment Result:	Content Sender Approved:	Content Filter:
CK Result:	BCC ID:	Quarantine ID:	EDQ Score: 99.9	User Type: Registered
Spam Sender Approved:	Spam Result: quarantine bulk	Spam Setting: On		

To	User ID	Org ID	Recipient TLS	Recipient MTA	Disposition	Disposition Filter
matthew@jumboinc.com	100-200029120	100-100003737	On	172.17.13.38	Delivered,Archived	
helensmith@jumboinc.com	100-200029046	100-100003740	On	172.17.13.38	Delivered,Archived	

For descriptions and definitions for each of the fields in the search results, see “Log Search Fields” on page 592.

For instructions on common search scenarios when using Log Search, see “Common Log Search Scenarios” on page 606.

To build your own Log Search query:

1. Click **More search criteria**.
2. To specify a date range, select a range from the drop-down menu.
3. Enter search strings by clicking the **Build my query** check box and entering keys with the following format, using commas or semi-colons to separate key-value pairs.

From: jeffsmith@ez4utech.com,Disposition:delivered

4. Click **Search** to open the search results page.

You can also use AND, OR, or NOT to separate the key-value pairs. AND, OR, and NOT are case-sensitive (must be typed with all-capital letters), and you must insert a space both before and after. The **to:** and **from:** in your query are not case-sensitive.

Note that you can run a query that combines NOT with AND; however, you cannot run a query that combines NOT with OR.

Examples:

```
to:jeffsmith@ez4utech.com AND from:janesmith@ez4utech.com
```

```
To:jeffsmith@ez4utech.com OR To:janesmith@ez4utech.com
```

NOT is useful when you want to eliminate a specific email address, Sender MTA, or Recipient MTA from the search results. With the following query, all recipients in the organization are included in the search except for *janesmith@ez4utech.com*:

```
NOT to:janesmith@ez4utech.com
```

Log Search Fields

The following two tables -- *Search Results Page* and *Message Details Page* -- describe the fields and values displayed in the Log Search results.

Search Results Page

The following fields are displayed when you run a Log Search query. Note that the fields are arranged in alphabetical order below, but they appear in the Log Search results in a different order.

Note: If you have access to a message and want to determine why a message was quarantine or delivered, it may be faster to use the *Message Header Analyzer*.

Field	Description and Values
Date	Description: Date and time the message was sent, based on the time zone of the organization from which the administrator ran the search. The date follows a 24-hour clock format of year/month/day/hour/minute. Example: 2009/09/23 13:23
Direction	Description: Indicates whether the message was sent inbound or outbound. Values: Inbound or Outbound

Field	Description and Values
Disposition	<p>Description: Specifies how the message was processed after passing through the message security service filters. For example, messages can be bounced back to the sender, deleted with no return message, or placed in a Quarantine. Multiple dispositions can apply to a message.</p> <p>Example: <i>Delivered, Archived</i></p> <p>Possible values:</p> <p>Blank value - Message did not trigger any filters.</p> <p>Admin Quarantined - Message was redirected to an administrator's quarantine. Note: The message security service does not log whether or not a message was <i>delivered</i> from quarantine.</p> <p>Archived - Message was stored in your archive by the Message Archiving service.</p> <p>Bcc Quarantine - Message was redirected to another user in the message security service (applies only to Attachment Manager).</p> <p>Blackhole - Message was discarded with no notification to the sender or recipient.</p> <p>Bounced - Message was returned to sender due to Attachment Manager, Content Manager, spam, or virus filters.</p> <p>Delivered - Message was sent to the recipient's inbox.</p> <p>Encrypted - Outbound message was encrypted using Message Encryption.</p> <p>Log Only - The message security service delivered the message without acting on the Content Manager filter condition.</p> <p>Quarantined - A suspicious message was placed in a quarantine. Note: The message security service does not log whether or not a message was <i>delivered</i> from quarantine.</p> <p>Reinjected - For outbound messages, this may indicate why a message was delayed.</p> <p>Spooled - Message was stored for later release until server or network problems were solved. Note: The message security service does not log whether or not a message was <i>unspooled</i>.</p>

Field	Description and Values
Disposition (cont.)	<p>Tag And Delivered - The message security service delivers the message without acting on the filter condition shown in the message header (spam and virus filtering).</p> <p>Zero Hour - Inbound message was placed in the Early Detection Quarantine (Pending tab) in the Message Center. Note: The message security service does not log the result of the early detection quarantine -- in other words, whether or not the message was delivered from quarantine or processed as virus-infected.</p>
From	<p>The full sender email address</p> <p>Example: matthew@ez4utech.com</p>
Message ID	<p>Description: Unique number for the message security service that identifies a specific message. Click the Message ID link in the search results to view detailed results for a specific message.</p> <p>Values: numeric value</p> <p>Example: 28333777840509347820947</p> <p>(Note: This is different from the <i>SMTP Message-ID</i>, which is described below.)</p>
Recipient MTA	<p>Recipient IP address (mail transfer agent)</p> <p>Example: 74.125.67.100</p>
Sender MTA	<p>Sender IP address (mail transfer agent)</p> <p>Example: 74.125.67.100</p>
SMTP Message-ID	<p>Description: A globally unique message identifier that's sometimes generated by the sender of a message. If present, this ID is located in the message header.</p> <p>Example: 5167e01c8da753\$71acd4c0\$c0a800a3a@qandl</p> <p>(Note: This is different from the <i>Message ID</i>, which is described above.)</p>
Subject	<p>Description: Subject of the message that's displayed in the search results.</p> <p>Example: staff meeting</p>
To	<p>The full recipient email address</p> <p>Example: mary@cuppamocha.com</p>

Message Details Page

The following additional fields and values are displayed when you click a Message ID link on the search results page. These results are specific to an individual message. Note that the fields are arranged in alphabetical order below, but they appear in the Log Search results in a different order.

Field	Description and Values
Archive Action	<p>Specifies whether a message was archived normally, bounced, or ignored/blackholed (silently dropped).</p> <p>Values:</p> <p>Blackholed Bounced Normal</p>
Archive Info	<p>Description: Reason for the Archive Action if the message was not archived normally. If the message was archived normally, this field is left blank in most cases.</p> <p>Values:</p> <p>Bad Ip - The message was sent from an IP address outside of the IP range in your Message Archiving journaling configuration.</p> <p>Bad Journal - The message does not use the correct journaling format.</p> <p>No Arc Users- The message is not addressed to any users who belong to orgs for which Message Archiving is turned on.</p>

Field	Description and Values
Archive Source	<p>Description: The source of the archived message -- for example, from mail flow or from Exchange journals.</p> <p>Values:</p> <p>Domino - Domino journal archiving.</p> <p>Exchange 2k3 - Exchange 2003 journal archiving.</p> <p>Exchange 2k7 - Exchange 2007 journal archiving</p> <p>Exchange 2k7 tnef - Exchange 2007 journal archiving (TNEF format).</p> <p>Mailflow - Unjournalled message between a user or users in an organization for which archiving is enabled. This refers to Inbound and Outbound mailflow archiving.</p> <p>Rearchive - Message was added to your Message Archive through the Postini Rearchiving service (a professional service).</p>
Attachment Result	<p>Description: Indicates the Attachment Manager disposition.</p> <p>Values:</p> <p>BCC Quarantine - Blind carbon copy of message was sent to Attachment Manager's designated quarantine. The message is delivered to the intended recipient if it makes it through the remaining filters.</p> <p>ERROR 582 The file attached violates our email policy - Message was bounced and returned to the sender. If a custom message was set up for this error, the custom message is displayed.</p> <p>Passed - Message was delivered without triggering any Attachment Manager filters.</p> <p>Quarantined - Message was sent to Attachment Manager's designated quarantine and was not delivered to the user.</p> <p>User Quarantine - Message was placed in the user's Message Center quarantine.</p>

Field	Description and Values
Attachment Sender Approved	<p>Description: An Attachment Manager filter was triggered, but the message was allowed through because of an approved sender list.</p> <p>Values:</p> <p>Recipient - Message was allowed through because of an approved mailing list.</p> <p>Sender Org - Message was allowed through because of an org-level approved sender.</p> <p>Sender User - Message was allowed through because of a user-level approved sender.</p>
Attachment Setting	<p>Indicates whether scanning for an attachment filter was On or whether an attachment filter was Not Used.</p> <p>If Not Used is displayed, one of the following is true:</p> <ul style="list-style-type: none"> • Attachment Manager was turned off. • There was no attachment in the message. • The message was quarantined or processed by virus or spam filters which override the Attachment Manager filter. .

Field	Description and Values
Attachment Type	<p>Description: Type of attachment that triggered an Attachment Manager filter.</p> <p>Values:</p> <p>Blocked File Extension - File formats listed in Custom File Types.</p> <p>Compressed Files - File formats such as .zip and .tar.</p> <p>Executable Content - Executable file formats such as .exe, .asp, and .vbs.</p> <p>Multimedia - Movie, film, and video formats such as .avi, .wmv, and .mpg.</p> <p>Music - File formats such as .mp3 and .wav.</p> <p>Images - File formats such as .jpg, .gif, and .bmp.</p> <p>Office/Productivity - Common office and productivity files such as .doc and .xls.</p> <p>Other - File formats not included in the above categories.</p> <p>Note: For a complete list of the filter file types described above, log in to the Administration Console, open the Organization Management page for any organization, click Attachment Manager, click Edit, and then click the links to any of the file types (such as Executables or Compressed Files). For more information, see “ Attachment Manager” on page 403).</p>
BCC ID	<p>This is the user ID of an administrator account for a BCC quarantine. If a BCC ID is displayed, the message was delivered to the recipient, and a blind carbon copy was also sent to an admin quarantine.</p> <p>Value: system number followed by the administrator’s user ID.</p> <p>Example: 7-206340783</p>

Field	Description and Values
CM Result	<p>Indicates the Content Manager disposition.</p> <p>Values:</p> <p>Approved - Message was delivered to the recipient only, or it was delivered both to the recipient and to an admin quarantine or user quarantine.</p> <p>Blackhole - Discards/deletes the message, with no notification to the sender or recipient.</p> <p>ERROR 582 - This message violates our email policy - Message was bounced and returned to the sender. If a customized message was set up for this error, the custom message is displayed.</p> <p>Passed - Content Manager filters were not triggered by the message.</p> <p>Quarantine - Message was sent to the administrator quarantine.</p> <p>User Quarantine - Message was sent to the recipient's quarantine and/or another user's quarantine.</p>
Commerce Score	<p>Special offer spam filter (see "Spam Scores" on page 639 and "Enable and Adjust Spam Filters" on page 301).</p>
Content Filter	<p>The name of the Content Manager filter that was triggered by the message</p>
Content Sender Approved	<p>A Content Manager filter was triggered, but the message was allowed through because the sender was on the recipient's approved sender list.</p>
Customer ID	<p>System number plus unique identifier for each message security service customer. You can find this number in the Administration Console at the account level organization.</p> <p>Example: 7-1000003708</p>

Field	Description and Values
Disposition Filter	<p>Description: Displays which filter set the final disposition of the message.</p> <p>Example: If the final disposition of a message is Quarantined, and if a spam filter caused this disposition, then the Disposition field will display:</p> <p style="padding-left: 40px;">Quarantined</p> <p>The Disposition Filter field will display:</p> <p style="padding-left: 40px;">Spam Filtering</p> <p>Values:</p> <p>Attachment Manager - Filters messages based on the size or file extension of attachments.</p> <p>Blatant Spam Blocking - Automatically deletes most obvious junk messages.</p> <p>Content Manager - Scans messages for specific content -- words, phrases, or text patterns -- and then takes an action on any messages that contain that content.</p> <p>Journal Archiving - All inbound and outbound messages, as well as all intradomain (internal) messages, are sent to Message Archiving.</p> <p>Message Size - Filter setting in Attachment Manager</p> <p>Null Sender Filter - Stops messages such as spam-related non-delivery reports (NDRs) that do not include an SMTP-envelope sender address.</p> <p>Org Blocked Sender - Sender is on the organization's Blocked Senders list.</p> <p>Outbound Bounce Protection - NDR - Setting that quarantines or blackholes undeliverable bounce messages when there is no recipient account.</p> <p>Sexually Explicit - Adult content spam filter.</p> <p>Spam Filtering - Identifies messages with spam.</p> <p>User Blocked Sender - Sender is on the user's Blocked Senders list.</p> <p>Virus Filtering - Scans messages and attachments for viruses.</p>
EDQ Score	<p>Internal score from the message security service's anti-virus engine (see "Levels of Protection" on page 311).</p>

Field	Description and Values
Finance score	Financial-industry heuristics filter (see “Spam Scores” on page 639 and “Enable and Adjust Spam Filters” on page 301).
Legal score	Legal-industry heuristics score (see “Spam Scores” on page 639 “ and “Enable and Adjust Spam Filters” on page 301).
Message Size	<p>Size of message in KB, MB or GB, including attachments</p> <p>Example: 11.29KB or 1.1 GB</p>
Money Making Score	Filter for “get rich quick” schemes (see “Spam Scores” on page 639 and “Enable and Adjust Spam Filters” on page 301).
Org ID	<p>Unique number from the message security service that identifies the sender’s Org ID for an outbound message or the recipient’s Org ID for an inbound message.</p> <p>To locate an Org ID, log in to the Administration Console. Go to Orgs and Users > Orgs, and then click the relevant organization to open the Organization Management page. The Organization ID is displayed in the Summary box on the right side of the page.</p> <p>Value: system number followed by the Org ID.</p> <p>Example: 7-100003947</p>
Primary Address	For registered and catchall users, the Primary Address field specifies the actual user or catchall account address corresponding to the user ID field (note that <i>catchall</i> is a legacy feature). The primary address will differ from the message address if the recipient address is aliased.

Field	Description and Values
Proxy	<p>Description: Specifies the proxy server for the message security service that processed the inbound or outbound message.</p> <p>Examples: exprod8mx8 eu3sys200amx205</p> <p>The proxy value can be used to determine the IP address that delivered the message to your server. When a message is processed by the message security service, the name of the proxy server is located in the message header. However, if you're unable to locate a specific message despite a disposition of Delivered, you'll need to search your company's mail server environment to locate it. The name of the proxy server may be useful in finding this message in your logs and troubleshooting what happened to it.</p>
Quarantine ID	<p>The message was quarantined in an account other than the recipient account.</p> <p>Value: system number followed by the user ID.</p> <p>Example: 7-206340783</p>
Racially Insensitive score	<p>Racially insensitive spam filter (see "Spam Scores" on page 639 and "Enable and Adjust Spam Filters" on page 301).</p>
Recipient TLS	<p>Description: Specifies whether a message was processed using transport layer security (TLS). If TLS is on, this field also specifies whether the TLS was policy enforced or domain enforced.</p> <p>For an inbound message, this refers to the connection between the message security service server and your company's mail server. For an outbound message, this refers to the connection between the message security service server and the recipient's mail server.</p> <p>Values:</p> <p>PE-TLS by domain: Message was processed using Policy Enforced TLS by domain.</p> <p>SMTP: Message was processed via SMTP.</p> <p>TLS: Message was processed via TLS encryption.</p> <p>For more information, see "Transport Layer Security (TLS)" on page 295.</p>

Field	Description and Values
Sender TLS	<p>Description: Specifies whether a message was processed using transport layer security (TLS). If TLS is on, this field also specifies whether the TLS was policy enforced or domain enforced.</p> <p>For an inbound message, this refers to the connection between the sender's mail server and the message security service server. For an outbound message, this refers to the connection between your company's mail server and the message security service server.</p> <p>Values:</p> <p>PE-TLS by domain: Message was processed using Policy Enforced TLS by domain.</p> <p>SMTP: Message was sent via SMTP.</p> <p>TLS: Message was sent via TLS encryption.</p> <p>For more information, see "Transport Layer Security (TLS)" on page 295.</p>
Session ID	<p>Internal number from a legacy feature in the message security service. This temporary field is used for tracking.</p> <p>Example: ac12781b763384629</p>
Sexually Explicit score	<p>Sexually-explicit spam filter (see "Spam Scores" on page 639 and "Enable and Adjust Spam Filters" on page 301).</p>

Field	Description and Values
Spam Result	<p>Description: Indicates the spam disposition.</p> <p>Values:</p> <p>Approved - Message was allowed through because of an approved sender.</p> <p>BSB Blackhole - Spam - Blackholed due to blatant spam blocking</p> <p>BSB Bounce -</p> <p>ERROR 571 Message Refused - Message was bounced due to blatant spam blocking. If a custom message was set up for this error, the custom message is displayed.</p> <p>Passed - Forwarded (same as <i>delivered</i>)</p> <p>Quarantine - Bulk - Quarantined due to spam filters.</p> <p>Quarantine - Org Blocked Sender - Quarantined because of a blocked sender at the org level.</p> <p>Quarantine - Sexually Explicit - Quarantined because of sexually explicit content.</p> <p>Quarantine - User Blocked Sender - Quarantined because of a blocked sender at the user level</p>
Spam Score	Overall spam score (see “Spam Scores” on page 639 and “Enable and Adjust Spam Filters” on page 301).
Spam Sender Approved	<p>Description: A spam filter was triggered, but the message was allowed through because of an approved sender.</p> <p>Values:</p> <p>User - Message was allowed through because of a user-level approved sender.</p> <p>Sender Org - Message was allowed through because of an org-level approved sender.</p> <p>Recipient - Message was allowed through because of an approved mailing list.</p>
Spam Setting	<p>Indicates whether scanning for a spam filter was On, Not Used, or set for Tag and Deliver.</p> <p>If Tag and Delivered, the message security service delivers the message without acting on the filter condition shown in the message header (allows an administrator to test a filter prior to making it fully active).</p>

Field	Description and Values
User ID	<p>Description: Unique number from the message security service that identifies the sender of an outbound message or the recipient of an inbound message. A user's primary email address can be changed, but its ID always remains the same.</p> <p>A User ID is useful for tracking a user even when they have multiple aliases. To locate a User ID, log in to the Administration Console. Go to Orgs and Users > Users, and then click the relevant user to open the User Overview page. The User ID is displayed in the Summary box on the right side of the page.</p> <p>Value: system number followed by the user ID.</p> <p>Example: 7-206340783</p>
User Type	Indicates whether a sender or recipient is a registered user, unregistered user, or catchall user (a legacy feature).
Virus Name	Name of any found virus

Common Log Search Scenarios

The most common search scenarios are presented below. Each section presents a list of the queries you'll need, instructions for running the searches, and tips on interpreting search results.

What happened to an inbound message?

Common answers include:

- The message was delivered to the recipient server.
- The message was quarantined or bounced by a filter.
- The sender connection may have been blocked by Connection Manager.

To track an inbound message, follow these steps:

1. From the Log Search tab, run the following query:
 - Enter the sender's email address in the **From** field.
 - Select **Inbound** for the Direction.
 - Select a time range that matches the time the message was sent.
 - Click **Search**.

Note: You can narrow your search by also including the recipient's email address, the Sender MTA (IP address), and the Disposition in your query.

2. On the search results page, look for the message and view the results in the **Disposition** column:
 - If **Delivered**, the message passed successfully through the message security service. If the message is missing, you'll need to search your company's mail server environment to locate the message.
 - If **Quarantined**, go to the Quarantine and deliver the message. If the message still does not arrive from quarantine after you deliver it, contact Support to troubleshoot the cause.

Note: If a message was sent to Quarantine, you can later refine filtering policies that may have inadvertently mishandled the message. See "Why was a message delivered or quarantined?" on page 609.
 - If **Bounced**, click the **Message ID** link in the search results to view message details. Filters for spam, Content Manager, or Attachment Manager may have been the cause. If necessary, you can refine filtering policies in the Administration Console (see "Spam Filters" on page 293, "Content Manager" on page 329, and "Attachment Manager" on page 403).
 - If the message is still not displayed in the search results from the original query, the sender connection may have been blocked by Connection Manager (although there is a not currently a Log Search field that indicates this result directly). This happens when an incoming message from a sender is dropped because Connection Manager identifies the sender (maybe incorrectly) as a malicious sender. Contact Support to confirm the cause of the missing message and to troubleshoot.

What happened to an outbound message?

Common answers include:

- The message was delivered but may have been lost within the recipient's network.
- The message may have been bounced or rejected by the recipient's network.
- The message may have been delayed due to network issues.
- The message was quarantined or bounced by a filter.

To track an outbound message, follow these steps:

1. From the Log Search tab, run the following query:
 - Enter the recipient's address in the **To:** field.
 - Select **Outbound** for the Direction.
 - Select a time range that matches the time the message was sent.
 - Click **Search**.

2. On the search results page, look for the message and view the results in the **Disposition** column:
 - If **Delivered**, the message passed successfully through the message security service and may be lost within the recipient's network.
 - If **Bounced**, click the **Message ID** link to view message details. Outbound filters for spam, Content Manager, or Attachment Manager may have been the cause. If necessary, you can refine filtering policies in the Administration Console (see "Spam Filters" on page 293, "Content Manager" on page 329, "Attachment Manager" on page 403, and "Configuring Inbound Servers" on page 421).
 - If **Reinjected**, this means the message was relayed back to your server due to a sending error. Reinjection occurs very rarely and may result in a slight delivery delay.
 - If the message is not displayed in the search results, contact Support to troubleshoot the issue.

Was a message encrypted or archived?

To confirm whether or not a message was encrypted or archived, follow these steps:

1. From the Log Search tab, run the following query:
 - Enter the sender's address in the **From** field, and the recipient's address in the **To** field.
 - Select **Inbound** or **Outbound** for the Direction. Leave this field blank to search on both inbound and outbound mail.
 - Click **Search**.
2. On the search results page, view the results in the **Disposition** column to see if the disposition is **Encrypted** or **Archived**.
3. If yes, click the **Message ID** link in the far-left column to view the message details. From the message details page, view the following fields:
 - If **Encrypted**, see the **Sender TLS** and **Recipient TLS** fields for more information.
 - If **Archived**, see the **Archive Source**, **Archive Action**, and **Archive Info** fields for more information.

I want to track messages for a sender or recipient

Using Log Search, you can track all messages for a sender or recipient for a specific time range. You can use this type of search to confirm whether or not an intended recipient received a specific email, or you can also track the results for a specific sender to monitor the triggering of attachment and content filters.

To track all messages for a sender or recipient, follow these steps:

1. From the Log Search page, run the following query:
 - Enter the sender's address in the **From** field, and/or the recipient's address in the **To** field.
 - Select **Inbound** or **Outbound** for the Direction. Leave this field blank to search on both inbound and outbound mail.
 - Click **Search**.
2. On the search results page, view the following fields:
 - View the **To** field to view a complete list of recipients for the sender's messages.
 - View filter fields such as **Commerce Score**, **Finance Score**, or **Legal Score** if you want details about which filters may have been triggered for the sender or recipient.
 - View the **Content Filter** field to see if Content Manager filters were triggered.
 - View the **Attachment Type** field to see if Attachment Manager filters were triggered for that sender or recipient.

Results of this query will include all successful messages delivered by a sender or received by a recipient for the specified time period.

Note: Log Search data is available for approximately 45 days. To save data for a specific user over a longer time period, you can export it to your computer occasionally. Click **Export All** or **Export Selected** on the search results page.

I want to track messages by subject

Using Log Search, you can track all messages by subject for a specific time range. Searches on both exact and partial text are supported, as well as phrases within the text. Searches are case insensitive. For example, you can find search results for an email with the following subject line, "New time for Staff Meeting," by using any of the following search strings in the Subject field:

```
New time for Staff Meeting  
staff meeting  
new time
```

Note that non-ASCII characters in the Subject field are currently not supported.

Why was a message delivered or quarantined?

The Log Search tool enables you to track missing messages for inbound and outbound traffic, or to track all messages for a specific sender, recipient, domain, or IP address. In the search results, you can also view message details to confirm whether specific filters were triggered when the message was sent, and confirm the message disposition. (See "Log Search Fields" on page 592 for a definitions and descriptions of the different fields.)

However, to analyze filter settings and determine the *cause* of a message being delivered or quarantined, you'll need the *Message Header Analyzer*. The message security service inserts custom tags into the message headers of processed email. The Header Analyzer uses these tags to determine why a message was quarantined or allowed through.

Troubleshoot Log Search

Why am I getting no results from my Log Search query?

Sometimes you may receive no results because your search criteria is too narrow. In this case it may help to broaden your search by searching only by sender or recipient plus time range. Also, if a message is not displayed in the search results, the sender connection may have been blocked by Connection Manager. For more details, see "What happened to an inbound message?" on page 606.

Why am I receiving an error message when I enter a Log Search query?

The maximum number of messages a Log Search query can return is approximately 15,000. Queries that return more than this limit result in an error message. If this occurs, you can refine your search by including additional criteria -- for example, search by both sender and recipient.

In some cases you may also reduce the number of messages in the search results by limiting your search to an organization that's lower in the hierarchy.

I am receiving several pages of results from my Log Search query, but I can't find my message.

If this happens, refine your search criteria by including both the sender and recipient in the query, as well as other criteria such as **Sender MTA** or **Disposition**.

I'm unable to find any data for a specific user from two months ago.

Log Search data is available for approximately 45 days. To save data for a specific user over a longer time period, be sure to export it to your computer occasionally. Click **Export All** or **Export Selected** on the search results page.

I can't see the Log Search tab in the Administration Console.

Your access to the Log Search tab depends on your authorization privileges. Access to Log Search is granted initially only to administrators who have View Reports privileges. For more information about Log Search privileges within your organization, see "Administrative Privileges for Message Log Search" on page 586.

Chapter 28

Batch Processing and EZCommand

About Batch Processing

Batch processing is a quick and efficient method to perform a large number of configuration changes by creating, validating and running command scripts in real-time. The batch commands allow you to create, delete, modify, and gather reports on:

- organizations
- users
- domains
- aliases

Important: For detailed information about the batch commands, fields, and protocols, see the *Email Security Batch Reference Guide*.

Batch Validation

The batch validator checks either a batch file or batch commands typed in to the batch page for:

- Syntax errors within each command.
- Ability to process the command based on the administrator's level or authorization.

Resulting success and error messages are displayed on the screen. Validation does not process any commands.

Submitting Batch Commands for Processing

When submitted, batch commands are streamlined and immediately processed in the order listed. Success and error messages are displayed on the screen and mailed to the administrator's address for tracking purposes.

When To Use Batch

Authority privileges determine which batch commands an administrator can run, just as they determine what parts of the Administration Console an administrator can access. Batch processing is independent of your currently viewed location within the Administration Console, since each batch command contains details about where to apply.

A subset of the batch commands can be run through the EZCommand API. See “About EZCommand” on page 612 for more details.

Configuration changes should be made by batch whenever:

- The number of changes is too great to effectively use the Administration Console.
- The changes can be created by automated script (e.g. LDAP server plug-ins), but EZCommand cannot be used due to the EZCommand limited command set or the inability to submit EZCommand changes via HTTPS request.

For example, you want to lower spam filter settings from level 4 to level 3 from 100 users. Configuring the Default User with the change will only affect new users. Since changing user configuration for 100 users by Administration Console interface would be repetitive and downright unpleasant, use the batch interface.

About EZCommand

EZCommand is a Perl-based scripting interface that allows administrators to perform basic tasks without having to log in to the Administration Console. EZCommand facilitates the integration of various administrative functions with the administrator’s tools and applications.

The EZCommand commands, which are a subset of the batch commands available through the Administration Console, perform user-related tasks:

- `adduser`
- `modifyuser`
- `deleteuser`
- `addalias`
- `deletealias`
- `suspenduser`

For detailed information about the EZCommand feature, see the *Email Security Batch Reference Guide*.

Setting Up EZCommand

Prerequisites

The following steps are required to successfully use the EZCommand interface:

- 1. You must be proficient in Perl programming and have the ability to generate valid cross-authentication (XAuth) strings.**

See “Cross-Authentication” on page 616 for information on cross authentication. Enabling Cross authentication or EZCommand requires programming knowledge.

- 2. Set a Shared Secret for each organization that contains an administrator.**

An “EZCommand Shared secret” must be submitted for an org in order to process commands by an Administrator in that org.

- In the Administration Console, go to Orgs & Users > Orgs.
- Choose the organization from the Choose Org pull-down, or click the name in organization list.
- In the Organization Management page, scroll to the Organization Settings section and click General Settings.
- On the General Settings page, enter the shared secret in the EZCommand Shared Secret field and click Save.
- Add shared secrets to other organizations that contain administrators who will submit EZCommands. With EZCommand, the shared secret must be set for each organization; the shared secrets are not inherited down the organization hierarchy.

- 3. Check and set administrator privileges for the organizations you plan to work with.**

EZCommands are only limited by the authorization for the administrator who processes the. For details, see:

Batch Reference Guide

Calling EZCommand

Commands are sent to EZCommand via a secure, cross-authenticated HTTP request to the host name of the web cluster which serves your Administration Console pages:

`https://hostname/exec/remotecmd?auth=authstring&cmd=cmdstring`

Note: SSL is required

hostname	The host name listed in the URL after a successful log in to the Administration Console. It will be of the form <code>ac-sN.postini.com</code> . N is the system in the message security service which processes your mail traffic.
authstring	URL-escaped XAuth string made by combining an administrator account and the EZCommand Shared Secret field on the org containing the administrator. (See “Cross-Authentication” on page 616 for details on the scripting necessary to generate an <code>authstring</code> .)
cmdstring	URL-escaped command to execute (described in next section)

Troubleshooting: Batch

Batch validation fails because a Batch command argument contains the comma “,” character.

The comma character, is used to delimit different arguments passed to a batch command, as described in the *Email Security Batch Reference Guide*.

Within a batch command argument, add quotes around the argument, so that the comma will not be used as a delimiter.

Examples:

```
modifyuser ted@jumboinc.com, approved_senders+="yahoo.com,+aol.com"  
modifyorg "Jumbo, Inc Account", support_contact=joe@jumboinc.com
```

Batch Validation fails although command syntax is correct.

The batch validator does not take into account previous changes made within a batch file. This implies that the following batch command sequence will cause a validation error.

```
adduser username1@jumboinc.com  
addalias username1@jumboinc.com, username2@jumboinc.com
```

If the syntax is correct, then these batch commands can be processed in this sequence without error.

Chapter 29

User Authentication

About User Authentication

When users and administrators log in, the user name and password submitted are authenticated using one of three methods:

- Privately Managed Passwords (PMP)
- SHA1 Cross-Authentication (XAuth)

Important: To change authentication methods, you must contact technical support. If you are direct Postini customer, log in to the Support Portal and submit a work request case with Customer Care, otherwise, please contact your vendor.

When users attempt to log in to the Message Center or Administration Console, the login information is used in conjunction with the *Authentication Data* field to authenticate by PMP or XAuth. Authentication Data is a General Settings field in an organization which contains users. Authentication Data is only visible when using XAuth, and contains handshaking information to ensure that the message security service and your servers speak the same language.

PMP Authentication

Privately managed password authentication (PMP) is the simplest authentication mechanism. When a user attempts to log in, login information is submitted to the message security service securely via HTTPS. User names and passwords are authenticated against the registered user database, which stores the PMP passwords encrypted.

Important: To change your authentication method to PMP authentication, you must contact technical support. If you are direct Postini customer, log in to the Support Portal and submit a work request case with Customer Care, otherwise, please contact your vendor.

Recommended PMP Usage

Since PMP passwords are transmitted across the Internet via HTTPS and stored encrypted in the registered user database for the message security service, there are no significant security concerns.

It is recommended that PMP be used, unless single sign-on is of prime importance. In that case, use XAuth.

PMP Passwords

When a new PMP user is created, a one-time PMP password is generated and sent out in the Welcome and My First Spam notifications.

When an organization is switched to use PMP, a one-time PMP password is generated, however a notification of this new password is not mailed to the users. In this case, suggest that they reset their passwords using the information in “Set Message Center Passwords” on page 265 or “Reset a User’s Password” on page 145.

Restrictions for passwords depend on the settings selected by an administrator. Under Password Policies on the Organization Management page, you can manage and configure password policies for an organization, including Length, Complexity, Maximum Age, History, and Lockout Threshold (see “Set User Password Policies” on page 144). For new customers (May 2007 and later), Complexity is turned ON by default, and the default Length is a 6 character minimum.

Cross-Authentication

When a user needs to be authenticated as authorized to use a particular service, that user is typically authenticated using an identifier and password, which only the user and the service know.

When a pair of services are working together, either the user must authenticate twice, once to each service, or the authenticating service must be able to securely inform the partner service that the user has already been authenticated.

Cross-Authentication uses a technique called a digital signature, which can verify that data was created by a particular authority, and has not been modified since. To authenticate a user, the user identifier is securely signed, and forwarded to the partner service. If the signature has not been forged, one partner can know that only the other partner could have generated the signature and data.

This is done by creating a standard SHA1 hash using the data to be signed and a shared secret or password that has been previously agreed to by the signing authority and the verifier. This process is called *Cross Authentication* (or *XAuth*).

Important: To change your authentication method, you must contact technical support. If you are direct Postini customer, log in to the Support Portal and submit a work request case with Customer Care, otherwise, please contact your vendor.

WARNING: Because of the scripting involved, the message security service does not provide all the elements necessary to implement cross authentication. Cross authentication is intended only for use by experienced programmers.

Recommended XAuth Usage

Since XAuth is secure, it is an ideal solution for single sign-on. If you are not familiar with Perl or C scripting, do not attempt implementation.

XAuth is not compatible with Quarantine Summary links. See “About Quarantine Summary” on page 282 for steps on how to disable Quarantine Summary links.

Configuring XAuth Shared Secret

XAuth uses the Authentication Data field to store the authstring portion of the shared secret used in the XAuth libraries below. Apart from submitting a request through the Support Portal to enable XAuth, this is the only configuration which needs to be made in the message security service. All other configurations are set on your authentication server.

1. **From the Orgs & Users > Orgs page, select the org which contains the users to authenticate.**

This may require using the form to search for the correct org, increasing the number of orgs shown per page, or navigating to a later page.

2. **Select the General Settings header under Organization Settings.**
3. **Click the Authentication Data link.**
4. **Type the shared secret exactly as typed into the XAuth scripts generating the digital signatures.**
5. **Click Submit.**

Whenever the shared secret is changed in the scripts, it should also be changed in the Authentication Data field for the org which contains the users being authenticated.

Note: The Authentication Data field can be configured by the batch command `modifyorg`. For details on using batch commands, refer to “Batch Processing and EZCommand” on page 611.

Using Perl to generate XAuth Strings

1. **Create Auth Object**

```
use PSTNCrossAuth;  
$secret = 'Secret String, used here and in Authentication Data';
```

```
$auth = new PSTNCrossAuth( $secret );
```

This creates a Perl object that used to either generate or verify auth strings.

2. Create Auth String

```
$authString = $auth->authString( 'user@domain.com' );
```

The authString will have 31 base64 characters followed by the string that was signed. If you use this in a URL, you need to escape the + signs by replacing them with %2B tokens.

3. Verify Auth String

```
$address = $auth->checkString( $authString, $secret );
```

If the address is a non-empty string, the address is the authenticated data was originally signed. In this example it would be user@domain.com.

Prerequisites

You must have the `Digest::SHA1` package, available the CPAN at <http://www.cpan.org>.

Source: Perl Interface

```
PSTNCrossAuth.pm:
package PSTNCrossAuth;
use Digest::SHA1( sha1_base64 );
sub new {
    my $class = shift;
    my $self = bless {};
    $self->{secret} = shift;
    return $self;
}
sub authString {
    my $self = shift;
    my $address = shift;
    my $randAddress;
    my $sig;
    $randAddress = chr( rand( 26 ) + 0x41 ) . chr( rand( 26 ) + 0x41 ) .
        chr( rand( 26 ) + 0x41 ) . chr( rand( 26 ) + 0x41 ) .
        $address;
    $sig = sha1_base64( $randAddress . $self->{secret} );
    return $sig . $randAddress;
}
# return null if not good auth string, else return authenticated
# address
sub checkString {
    my $self = shift;
    my $auth = shift;
    my $rand;
    my $address;
    my $sig;
    ( $sig, $rand, $address ) = unpack( 'a27a4a*', $auth );
    if ( sha1_base64( $rand . $address . $self->{secret} ) eq $sig ) {
        return $address;
    }
}
```

```

    } else {
        return 0;
    }
}
sub main::PSTN_authString {
    my $address = shift;
    my $secret = shift;
    my $auth = new PSTNCrossAuth( $secret );
    return $auth->authString( $address );
}
sub main::PSTN_checkString {
    my $string = shift;
    my $secret = shift;
    my $auth = new PSTNCrossAuth( $secret );
    return $auth->checkString( $string );
}
1;
sub urlEscape {
    my $line = shift;

    $line =~ s/%/%25/g;
    $line =~ s/ /%20/g;
    $line =~ s/</%3C/g;
    $line =~ s/>/%3E/g;
    $line =~ s/#/%23/g;
    $line =~ s/{/%7B/g;
    $line =~ s/}/%7D/g;
    $line =~ s/\\/%7C/g;
    $line =~ s/\\/ %5C/g;
    $line =~ s/\^/%5E/g;
    $line =~ s/~/%7E/g;
    $line =~ s/\[/%5B/g;
    $line =~ s/\]/%5D/g;
    $line =~ s/`/%60/g;

    $line =~ s/;/%3B/g;
    $line =~ s/\/%2F/g;
    $line =~ s/\?/%3F/g;
    $line =~ s/:/%3A/g;
    $line =~ s/\@/%40/g;
    $line =~ s/\=/%3D/g;
    $line =~ s/\&/%26/g;
    $line =~ s/\+/%2B/g;

    return $line;
}

```

Using C to generate XAuth Strings

You must know the word ordering of your CPU. If it is big endian (SPARC) and not little endian (Intel), you must define WORDS_BIGENDIAN in your makefile.

```

#ifdef PSTNCrossAuth_h
#define PSTNCrossAuth_h
#ifdef __cplusplus
extern "C" {
#endif
/* the returned string has been malloced, so you should free it */

```

```

/* the string has not been URL encoded, so you should change the
   '+' signs to %2B before sending them to a browser */
extern char *PSTN_authString( char *in, char *secret );
/* the returned string has been malloced, so you should free it */
/* the string will not be URL decoded */
/* this will give unreliable results if the input string is less than
   31 bytes long */
extern char *PSTN_checkString( char *auth, char *secret );
#ifdef __cplusplus
}
#endif
#endif

```

Using Digital Signatures to Log In

To use a digital signature to log in, create a log in URL using your script. Your users and administrators will access their Message Center or Administration Console by logging in to your single sign-on interface and clicking on the generated link.

In the examples below, replace `DigitalSignature` with your script-generated digital signature.

To log in to the Message Center or Administration Console:

```
https://login.postini.com/exec/login?xauth=DigitalSignature
```

To log in to the Message Center or Administration Console if you purchased a frames branding upgrade:

```
https://login.postini.com/exec/
login?display=frame&xauth=DigitalSignature
```

Note: While the shared secret remains the same, the digital signature is static. Make sure to use HTTPS to transmit the signature to ensure the signature is not transmitted unencrypted.

Troubleshooting: Authentication

How do I switch Authentication methods?

To change your authentication method, please contact technical support. If you are direct Postini customer, log in to the Support Portal and submit a work request case with Customer Care, otherwise, please contact your vendor.

Since changing authentication for an org requires assistance from Support, how can I freely create new orgs using different authentication types?

Set up orgs with each type you intend to use, and contact Technical Support to set up those parent orgs with the different authentication types.

When you create a new org, its settings are a copy of its parent org's settings. This includes the authentication type. Therefore, by creating a new orgs below a specific parent org, you will have free use of all authentication types.

User receives an error in red text when attempting to log in.

The error is:

We apologize for the inconvenience but the page that you are trying to reach has been moved. As a result, you will be required to log in again with your email address and password.

If you forgot your password, we suggest that you enter your correct email address and the password to your email account. If log in fails, click on the "Forgot your password?" link for specific instructions to retrieve your password.

If you reached this page from a bookmark, a new bookmark will also need to be created after logging in. Thank you.

The error occurs when using Privately-Managed Password (PMP) authentication for all users. The source of the issue is not having the User Access privilege for Account Settings.

Correct this by:

1. Selecting the organization containing affected users or the affected user:
 - Go to Orgs and User > Orgs and select the Organization containing the users.or
 - Go to Orgs & Users > Users and select the affected user.
2. Click User Access in the Organization Settings or User Settings section of the page (as appropriate).
3. Click the Modify checkbox for Account Settings to enable the Account Settings privilege.

Log in fails despite using correct log in information.

Error message seen is:

Invalid log in or server error. Please try again.
Forgot your password?
Your password is the same as your email account password.
Contact your email service provider for assistance.

This happens when Message Center Access is disabled for a user. Re-enable Message Center Access as described below:

1. Go to Orgs and Users > Users and select the user.
2. Click User Access in the User Settings section of the page.
3. Set Message Center Access to Enabled and click Save.

Authenticating specific users using a different method.

Each organization can only use one authentication method. Create a new organization for users who need to use a different organization method.

1. Create a new organization. See “Create an Organization” on page 91 for steps.
2. Contact the message security service support to change your Authentication method on the new organization.
3. Move users and add users to the new organization. See “Add / Delete / Move Users” on page 120 for steps.

Chapter 30

Configuring Single Sign On (SSO)

Overview

The Postini SSO service provides SSO based on the SAML 1.1 standard for authentication of your Postini administrators and users.

Note: SAML 2.0 and SAML 1.1 are not compatible. However, most SAML 2.0 servers offer a SAML 1.1-compatible option.

Two models of communicating authentication data are supported:

- **Post (Push Model)** The user is authenticated by the identity provider within his own network, and given signed authentication data by the SSO solution to pass to Postini. Postini verifies that the credentials originated from the user's SSO solution, and the user gains access to Postini services.
- **Artifact (Pull Model)** The user is authenticated by the identity provider within his own network, and given a login ticket by the SSO solution to pass to Postini. Postini connects to the user's SSO solution with the login ticket, and Postini's identity is verified by the SSO solution. The SSO solution then provides the authentication data, and Postini gives the user access to services.

Note: There is some latency inherent in this model due to the additional back-channel communication.

Both models support SAML 1.1.

You can find additional information about SAML 1.1 at:

http://en.wikipedia.org/wiki/SAML_1.1

Requirements

To employ the Postini SSO service, you must have:

- Your own SSO solution that supports SAML 1.1
- An identity provider

If you use the Pull model, you must:

- Provide Postini with HTTPS access to your IDP URL
- Store the Postini certificate in your SSO service

Your SSO solution needs to provide the user's Postini-login email address within its communications, either as the Authentication Subject Name or as an attribute value. For more information, see "Troubleshooting SAML Assertion Data" on page 630.

During configuration of your SSO solution, you identify the following URL as the SSO access point for Postini services:

<https://pfs.postini.com/pfs/spServlet>

This URL serves in two capacities:

- The Assertion Consumer URL for the Post (Push Model)
- The Artifact Receiver URL for the Artifact (Pull Model)

Recommendations

Protect Your Ability to Log In

To prevent being locked out of your Postini services in the event of a failure on the part of your SSO solution, we recommend that you:

- Create one user org that does not employ SSO authentication.
- Add an administrator to that org.

With these safeguards in place, that administrator is able to log in to the Postini services in the event your SSO solution fails.

Test Before Full Deployment

Before you implement SSO for your entire organization, we recommend that you employ the following test scenario.

1. Configure your SSO-solution end-point URL for Postini services to:
 - Administrator login to Administration Console:
<https://pfs.postini.com/pfs/spServlet/admin>
 - User log in to Message Center:
<https://pfs.postini.com/pfs/spServlet>
2. Customize your welcome message to direct users to the Message Center log-in URL (<https://pfs.postini.com/pfs/spServlet>).

3. Configure SSO for your account org (see “Configure SSO for Your Account Org” on page 625).
4. Create or designate a single user org for the purpose of this test, and configure SSO for that user org (see “Configure SSO for a User Org” on page 628).
5. Add or move test users to the user org. These users must also be configured in your SSO solution.
6. Have your test users employ SSO and monitor the results.

Configure SSO

You configure SSO first for your account org, and then for each user org for which you want SSO.

Keep in mind that when you configure a user org with SSO authentication, those users are not able to log in to Postini services via `https://login.postini.com`.

Configure SSO for Your Account Org

To configure SSO for your Account org:

1. Open the Organization Management page for your Account org.
2. Under Organization Settings, click **Single Sign On**.

Choose Org:

Must provide certificate data.

Single Sign-On Configuration - Postini Training Account

Enter information about your Single Sign-On (SSO) server. Your SSO server must already be working on your network. Click the links below to choose your SAML binding model: [Post \(Push Model\)](#) or [Artifact \(Pull Model\)](#).
[Post \(Push Model\)](#) [Artifact \(Pull Model\)](#)

Enter your SSO issuer ID and paste your SSO PEM (base64) format certificate (only one) in the box. Click **Add Configuration** to save your changes. You can then review your configuration and add certificates in the table below.

Issuer Name:

Your Certificate:

Your enabled SSO configurations appear below. To delete a configuration entry, select it and click **Delete Selected**. To add a certificate to a configuration, click **Add Cert** on the right.

	Issuer Name	Your Certificate	Certificate Expires
<input type="checkbox"/>			

The page opens with the Post (Push Model) options displayed by default. If these options are not displayed, click the **Post (Push Model)** link at the top of the page.

To configure the Post (Push Model) options:

1. Enter the following information:

For this option...	Enter this
Issuer Name	<p>The Issuer Name entry on your SAML server. For example:</p> <p><code>http://www.electric-automotive.com.</code></p> <p>Note: This string must match the Issuer Name entry on your SAML server.</p>
Your Certificate.	<p>The public key certificate for data signed by your SSO solution.</p> <p>Open your certificate in a text editor, copy the contents, and paste them into this field.</p> <p>Your certificate must be in the PEM format (Base-64 encoded format), and include the header and footer. For example:</p> <pre>-----BEGIN CERTIFICATE----- MIICEjCCAXsCBEJB3HswDQYJKoZ... -----END CERTIFICATE-----</pre>

2. Click **Add Configuration**.

Choose Org: Account

Single Sign-On Configuration - Postini Training Account

Enter information about your Single Sign-On (SSO) server. Your SSO server must already be working on your network. Click the links below to choose your SAML binding model: **Post (Push Model)** or **Artifact (Pull Model)**.
[Post \(Push Model\)](#) [Artifact \(Pull Model\)](#)

Enter your SSO issuer ID and paste your SSO PEM (base64) format certificate (only one) in the box. Click **Add Configuration** to save your changes. You can then review your configuration and add certificates in the table below.

Issuer Name:

Your Certificate:

Your enabled SSO configurations appear below. To delete a configuration entry, select it and click **Delete Selected**. To add a certificate to a configuration, click **Add Cert** on the right.

<input type="checkbox"/>	Issuer Name	Your Certificate	Certificate Expires	
<input type="checkbox"/>	http://www.sksuresh.com/samltest	<input type="checkbox"/> C=US, ST=CA, L=Mountain View, O=Postini, OU=Support, CN=www.sksuresh.com, emailAddress=srinivasan@postini.info	Oct 27 22:53:17 2012 GMT	Add Cert

Your new configuration is displayed at the bottom of the page.

To configure the **Artifact (Pull Model)**:

1. Open the Organization Management page for your Account org.
2. Under Organization Settings, click **Single Sign On**.
3. Click the **Artifact (Pull Model)** link at the top of the page.

Choose Org: Account

Single Sign-On Configuration - test Docs Customer1 Account

Enter information about your Single Sign-On (SSO) server. Your SSO server must already be working on your network. Click the links below to choose your SAML binding model: **Post (Push Model)** or **Artifact (Pull Model)**.
[Post \(Push Model\)](#) [Artifact \(Pull Model\)](#)

Enter your SSO source ID and assertion URL, and then click **Postini Certificate** to download the certificate you must install on your SSO server. Click **Add Configuration** to save your changes. You can then review your configuration in the table below.
Note: Ensure you install the Postini certificate on your SSO server.

Source Id:

Assertion URL:

[Postini Certificate](#)

Your enabled SSO configurations appear below. To delete a configuration entry, select it and click **Delete Selected**.

<input type="checkbox"/>	Source Id	Assertion URL
--------------------------	-----------	---------------

4. Enter the following information:

For this option...	Enter this
Source ID	40-byte base-64 string that identifies the IDP source. Generally obtained from SHA1 digestion of subject field of federated certificate.
Assertion URL	The Assertion Retrieval URL generated by your SSO solution.

5. Click **Add Configuration**.

Enter your SSO source ID and assertion URL, and then click [Postini Certificate](#) to download the certificate you must install on your SSO server. Click **Add Configuration** to save your changes. You can then review your configuration in the table below.
Note: Ensure you install the Postini certificate on your SSO server.

Source Id:

Assertion URL:

[Postini Certificate](#)

Your enabled SSO configurations appear below. To delete a configuration entry, select it and click **Delete Selected**.

<input type="checkbox"/>	Source Id	Assertion URL
<input type="checkbox"/>	8d021df6578f40bf549494ec9a471f0face7651a	https://pfs.postini.com/pfs/spServlet

Your new configuration is displayed at the bottom of the page.

Configure SSO for a User Org

To configure SSO for a User org:

1. Open the Organization Management page for the User org.
2. Under Organization Settings, click **General Settings**.
3. For Authentication Method, select **SAML SSO**.
4. Click **Save**.

Edit an SSO Configuration

You can make the following changes to an existing SSO configuration:

Post (Push Model):

- Add a certificate
- Delete a certificate

Artifact (Pull Model):

- Edit the Assertion URL

Edit a Post (Push Model) Configuration

1. Open the Organization Management page for your Account org.
2. Under Organization Settings, click **Single Sign On**.
3. To add another certificate to a configuration, click **Add Cert**, enter or paste the certificate data in the New Cert Data field, then click **Add Cert**.

The Postini SSO service checks for and accepts any valid certificate that your SSO server is using.

4. To delete a certificate, select the check box next to the certificate, then click **Delete Selected**.

Edit an Artifact (Pull Model) Configuration

1. Open the Organization Management page for your Account org.
2. Under Organization Settings, click **Single Sign On**.
3. Click the **Artifact (Pull Model)** link at the top of the page.
4. To edit the Assertion URL, click in the Assertion URL field and edit the text, then click **Save URL Changes**.

Delete an SSO Configuration

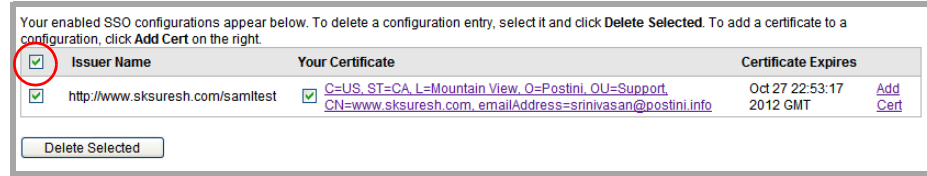
You can delete a single configuration, or delete all of your configurations. The procedures are the same for both Post (Push Model) and Artifact (Pull Model).

To delete a single SSO configuration, select the check box to the left of that configuration, then click **Delete Selected**.

Your enabled SSO configurations appear below. To delete a configuration entry, select it and click **Delete Selected**. To add a certificate to a configuration, click **Add Cert** on the right.

<input type="checkbox"/>	Issuer Name	Your Certificate	Certificate Expires	
<input checked="" type="checkbox"/>	http://www.sksuresh.com/samitest	<input checked="" type="checkbox"/> C=US, ST=CA, L=Mountain View, O=Postini, OU=Support CN=www.sksuresh.com, emailAddress=srinivasan@postini.info	Oct 27 22:53:17 2012 GMT	Add Cert

To delete all of your configurations, select the check box at the top left of the configurations list (this selects all), then click **Delete Selected**.



Troubleshooting SAML Assertion Data

If you are creating your own SSO solution and SAML Assertions, or configuring your server to alter Assertions, keep in mind that your Assertions, when decoded, need to conform to one of the following:

- The Name Identifier of the Subject of the Authentication Statement should be the email address of the user. For example:

```
<AuthenticationStatement><Subject><NameIdentifier>jdoe@google.com
</NameIdentifier></Subject></AuthenticationStatement>
```

- The Attribute Statement should contain an Attribute named "personal_email" or "work_email" (case-insensitive), with the value being the user's email address. For example:

```
<AttributeStatement><Attribute AttributeName="personal_email">
<AttributeValue>dhenders@google.com</AttributeValue>
</Attribute><Attribute AttributeName="work_email">
<AttributeValue>jdoe@google.com</AttributeValue></Attribute>
</AttributeStatement>
```

SAML Post Response HTML

Following is an example of the raw HTML for a SAML Post Response.

In the next section, "Decoded SAML Post Response" on page 632, you can see a decoded version of this HTML.

```
<html>
<head>
<title>Postini IDP Sample of SAMLResponse</title>
</head>
<body>
<center>
<h3>Postini IDP Sample of SAMLResponse</h3>
</center>
<table>
<form action="https://pfs.postini.com/pfs/spServlet" method="post">
<center>
```



```

XV0aGVudG1jYXRpb25JbnN0YW50PSIyMDA5LTAzLTA5VDIzOjM0OjI2Ljk4OVoiIEF
ldGhlnRpyY2F0aW9uTWV0aG9kPSJ1cm46b2FzaXM6bmFtZXM6dGM6U0FNTDoxLjA6Y
W06cGFzc3dvcnQipjxTdWJqZWN0PjxOYW11SWRlbnRpZmllcj5ibGVAc2FuZGllZ28
uZWR1PC90YW11SWRlbnRpZmllcj48U3ViamVjdENvbmZpcmlhdGlvbG9kZm9uZmlyb
WF0aW9uTWV0aG9kPnVybVpYXNpczpuYW1lc3p0YzptQU1MOjEuMDpjbTphcnRpZmF
jdDwvQ29uZmlybWF0aW9uTWV0aG9kPjxTdWJqZWN0Q29uZmlybWF0aW9uRGF0YT5BQ
UNKTW1UMFR5VnBYSFpOZm5LdWptd0pWdXRza1dKc1pVQnpZVzVrYVdWbmJ5NwxaSFh
HbXJ3MzwwU3ViamVjdENvbmZpcmlhdGlvbG9kZm9uZmlybWF0aW9uPjwvU3ViamVjdD48L0F1dGhlnRpyY2F0aW9uU3RhdGVtZW50PjwvQXNzZXJ0aW9
uPjwvUmVzcG9uc2U+ "/>
<input type="hidden" name="TARGET" value="https://pfs.postini.com/
pfs/spServlet"/>
<tr><td></td></tr>
<tr><td></td><td><input type="submit" name="Submit" value="Submit" /
></td></tr>
</center>
</form>
</table>
</body>
</html>

```

Decoded SAML Post Response

Following is the decoded form of the HTML in the example above (“SAML Post Response HTML” on page 630). This is provided to give you an indication of what sort of data your SAML assertions need to include. Note that when it is submitted via HTML, the SAML Response is base64-encoded.

```

<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
IssueInstant="2009-03-09T23:34:27.003Z" MajorVersion="1"
MinorVersion="1" ResponseID="da85bd7580929df9b6f2ea6f8f5754ed">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/
10/xml-exc-c14n#"></ds:CanonicalizationMethod>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#rsa-sha1"></ds:SignatureMethod>
      <ds:Reference URI="#da85bd7580929df9b6f2ea6f8f5754ed">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"></ds:Transform>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#"><ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/
2001/10/xml-exc-c14n#" PrefixList="code ds kind rw saml samlp
typens #default"></ec:InclusiveNamespaces></ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"></ds:DigestMethod>
        <ds:DigestValue>s5S9GXJvlhWQqqJ5bviLkuG0CrM=</
ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>

```

```

<ds:SignatureValue>Qv2WK1p6tuPEuyaQ+7oyVCU60IvLtX97WXtR5+hEWxZsWXa
4IbtHlt6GOr2PvNEWMsckk1I7SYJI/fbexYTaGRFFbOPxbimwEu3Vqg8mECunor/
wVlGQ/xnkQY3Mgs20K1K4ZEagZHkykIVL1XUNJQNa/+IvqUqBsk3xRPy5QFE=</
ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>

<ds:X509Certificate>MIICQDCCAakCBEJ7qeYwDQYJKoZIhvcNAQEEBQAwwZELMA
kGAlUEBhMCMVVMxEzARBgNVBAGTCkNhbG1mb3JuaWEuXjAQBGNVBAsTCUlkcFNhbXBs
ZTEVMBMGAlUEChMMUG9zdGluaSwgSW5jMRgwFgYDVQQDEw9wZnMucG9zdGluaS5jb2
0wHhcNMDUwNTA2MTczMTE4WhcNMTUwNTA0MTczMTE4WjBnMQswCQYDVQQGEwJFUzET
MBEGA1UECBMKQ2FsaWZvcml5YTESMBAGA1UECzMJSWRwU2FtcGxLMRUwEwYDVQQKEw
xQb3N0aW5pLkCBJmMxGDAWBgNVBAMTD3Bmcy5wb3N0aW5pLmNvbTCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwYkCgYEAAtLBCJ4rNCvYfPcIsd/D43X5BF/
1Q99XTLSEmKmKYDHP+hgi8PAT5J9zu3WYghiILB8fm4pbDqPV0aT9IRSrlcQ5EWEIy
BEemYHY6r7mTFiLUZYH4JHuk5p15Uwld73GlsDDyMMWjF7TmgfyfifITX/wuFmn+8/
kRv7GjGpVTn5GkCAwEAATANBgkqhkiG9w0BAQQFAAOBgQCXWzg3eEQfOYagnPrNDVV
18l+Do7igJEQHxgSyP9gydBVIt8VYH8asoLGV7fLiqlmUf/
PpwW00UIxs1KtTKF3R3p/jWKJ2IUVGIDYN9nkkaPzXgV9XM+dohk+Ct4IKP/
mlhLQC3k1falGS/nMeeHDe88cf8TmpLTp42/UGOlFw==</ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<Status>
  <StatusCode Value="samlp:Success"></StatusCode>
</Status>
  <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="a67cc38c45ca10474e6a930ddd74e566" IssueInstant="2009-
03-09T23:34:27.002Z" Issuer="localhost" MajorVersion="1"
MinorVersion="1">
    <Conditions NotBefore="2009-03-09T23:34:26.989Z"
NotOnOrAfter="2009-03-09T23:34:56.989Z"></Conditions>
    <AuthenticationStatement AuthenticationInstant="2009-03-
09T23:34:26.989Z"
AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
      <Subject>
        <NameIdentifier>username@domain.com</NameIdentifier>
        <SubjectConfirmation>

<ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact</
ConfirmationMethod>

<SubjectConfirmationData>AACJMmT0TyVpXHZNfnKuJmwJVutsjWJsZUBzYW5ka
WVnby5lZHXGmrw3</SubjectConfirmationData>
      </SubjectConfirmation>
    </Subject>
  </AuthenticationStatement>
</Assertion>
</Response>

```

SSO Reference

Post (Push Model)

Use this page to configure the Post (Push Model) for authentication.

For this option...	Enter this
Issuer Name	<p>The Issuer Name entry on your SAML server. For example:</p> <p>http://www.electric-automotive.com.</p> <p>Note: This string must match the Issuer Name entry on your SAML server.</p>
Your Certificate.	<p>The public key certificate for data signed by your SSO solution.</p> <p>Open your certificate in a text editor, copy the contents, and paste them into this field.</p> <p>Your certificate must be in the PEM format (Base-64 encoded format), and include the header and footer. For example:</p> <pre>-----BEGIN CERTIFICATE----- MIICEjCCAXsCBEJB3HswDQYJKoZ... -----END CERTIFICATE-----</pre>

To add another certificate to a configuration, click **Add Cert**, enter or paste the certificate data in the New Cert Data field, then click **Add Cert**. The Postini SSO service checks for and accepts any valid certificate that your SSO server is using.

To delete a certificate for a configuration, select the check box next to the certificate, then click **Delete Selected**.

Artifact (Pull Model)

Use this page to configure the Artifact (Pull Model) for authentication.

For this option...	Enter this
Source ID	40-byte base-64 string that identifies the IDP source. Generally obtained from SHA1 digestion of subject field of federated certificate.
Assertion URL	The Assertion Retrieval URL generated by your SSO solution.

To edit the Assertion URL for an existing configuration, click in the Assertion URL field and edit the text, then click **Save URL Changes**.

Appendix A

Interpreting Header Fields

About Header Fields

When messages are processed by the message security service, custom header fields are placed in email-message headers. This header information can be useful for either determining email disposition or for handling support issues.

This chapter describes the following header fields added by the message security service:

- “Received Header Field” on page 638
- “X-pstn-levels Header Field” on page 638
- “X-pstnvirus Header Field” on page 640
- “X-pstn-settings Header Field” on page 641
- “X-pstn-2strike Header Field” on page 642
- “X-pstn-xfilter Header Field” on page 642
- “X-pstn-neptune Header Fields” on page 643
- “Industry Heuristics Header Fields” on page 643
- “X-pstn-addresses Header Field” on page 645
- “X-pstn-disposition Header Field” on page 646
- “X-pstn-nxpr and X-pstn-nxp Header Fields” on page 646
- “Attachment Manager and Content Manager Header Fields” on page 646

The service minimizes processing time by only scanning for categories that the user has enabled. For example, if a user turns off the commercial category, the commercial score is not completed or displayed. If you do not have access to Industry Heuristics (an optional feature), the Industry Heuristics score is not calculated or displayed.

All the numeric header values display 5 digits to the right of the decimal place.

Received Header Field

The service includes a “Received” header field in each message processed. This information includes the IP address of the sender, any details on TLS (Transaction Layer Security, an optional feature) secure transmission from the sending server, the particular server that processed the message, the digital signature that is added to let the system distinguish between legitimate NDRs for your messages and NDRs that result from spammers using forged addresses, and a timestamp.

An email message that passed through the message security service will have header fields similar to the following:

```
Received: from source ([172.18.76.29]) by exprod8ob108.postini.com
([64.18.7.12]) with SMTP
ID DSNKSKPalmOiRJPpHXa+8YGGbDZtHbT3OnGV@postini.com; Thu, 14
Aug 2008 00:11:18 PDT
```

If you don't see a header field with the domain similar to `exprodNmxM.postini.com` (for example, `exprod8mx8.postini.com`), the message did not go through the message security service, and was delivered directly to the recipient's server.

TLS delivery from the sending server to the message security service is indicated by “using TLSv1” or “using SSLv3”, for example:

```
Received: from source ([12.158.40.254]) (using TLSv1) by
exprodNmxM.postini.com; Wed, 08 Jan 2007 14:39:55 PST
Received: from source ([12.158.40.254]) (using SSLv3) by
exprodNmxM.postini.com; Wed, 08 Jan 2007 15:02:31 PST
```

(Your mail server may add similar details to the header to indicate that the message was received via TLS from the message security service.)

The digital signature takes a form like the following:

```
ID DSNKSKPalmOiRJPpHXa+8YGGbDZtHbT3OnGV@postini.com;
```

The digital signature is added to support the Null Sender Disposition spam filter.

X-pstn-levels Header Field

The letter/number pairs that appear on X-pstn-levels tell you which filters (if any) were triggered and to what degree. The letters that may appear on this line are:

General Transport Heuristics Filters

- GT1 = General transport heuristics most trusted
- GT2 = General transport heuristics more trusted
- GT3 = General transport heuristics trusted

Spam Filters

- S = General/bulk spam score
- CV = Internal use only. This has no effect on the overall spam score or message disposition.
- P = Sexually explicit (pornography) spam score
- M = Make-money-fast (MMF) spam score
- C = Commercial or “special offer” spam score
- R = Racially insensitive spam score

Industry Heuristics Filters (optional feature)

- FC = Financial Content score
- LC = Legal Content score

Spam Scores

A spam score of 100 on the S filter would indicate that this email contains nothing that triggers the general spam filter (it is a valid message). The lower the score, the more likely that this message is spam.

Category Scores

A message is assigned to a filter category when its score in that category is an 85 or below.

Example:

```
X-pstn-levels: (S: 0.00000/60.95723 CV:99.9000 R:95.91080
P:95.91081 M:64.93900 C:93.23770 )
X-pstn-settings: 5 (2.00000:8.00000) r p M c
```

The overall spam score is S: 0.00000. This is a Make-Money-Fast (M) spam message, as shown by the capital M in the X-pstn-settings line.

A score of 85 or below triggers a category filter and in this example the Make-Money-Fast score is M:64.9390.

The X-pstn-levels header field is not added if one of the recipients has Bulk Email protection disabled. For example, if the email message is sent to two users, one with the Bulk Email filter turned on and one with it turned off, the message security service does not include this header field.

Blatant Spam Blocking (BSB) Score

A second numeric evaluation, the BSB score, appears after the spam score in the X-pstn-levels header field. The BSB score is used by the spam engine to identify messages that should be bounced or blackholed by Blatant Spam Blocking. Unlike the spam score, the BSB score should not be evaluated directly.

Example:

```
X-pstn-levels:      (S: 0.00010/62.95723 )
```

The spam score (s:) is separated from the BSB score by a slash (“/”). The BSB score will always appear, even if BSB is not turned on.

If a message scores as blatant spam, the BSB disposition of bounce or blackhole results in a discarded message, and there are no spam-related header fields for those messages. The BSB score was added to make it clear to someone evaluating the header that the message did meet the spam score criterion but failed to meet the BSB score criterion.

X-pstnvirus Header Field

When a virus is detected, the message security service inserts the `X-pstnvirus` header field to show what virus was caught. The format of the field when a virus is detected by McAfee is:

```
X-pstnvirus: McAfee_Virus_Name
```

For further details on one of these viruses, you can search for `McAfee_Virus_Name` at the McAfee Virus Information Library site:

```
http://vil.nai.com
```

Following is the format of the field for the Authentium Antivirus engine (an optional feature for service packages) which scans inbound messages:

```
X-pstnvirus: AUTH-Authentium_Virus_Name
```

The text `AUTH-` is not part of the virus name. The text indicates that the virus was not detected by the McAfee engine, and was caught by Authentium. For further details on a virus caught by Authentium Antivirus, you can search for `Authentium_Virus_Name` on the

```
http://www.authentium.com/support/AVMatrix/portal.aspx
```

Following are examples of the same virus if detected by McAfee or Authentium:

```
X-pstnvirus: W32/Mydoom.bb@MM  
X-pstnvirus: AUTH-W32/Mydoom.AY@mm
```

Messages with the `X-pstnvirus` header field are not delivered to your users only in the following cases:

- Virus disposition is set to Message Header Tagging for the organization that contains the user. In this case, all viruses will be tagged with the header field and delivered to your mail server.
- The administrator (or user, if allowed) delivers the infected or cleaned virus to the user.

The `X-pstnvirus` field is omitted only when virus protection is not enabled for a user, or there is no the message security service user associated with the recipient's address.

X-pstn-settings Header Field

User Settings

The X-pstn-settings line shows the recipient's spam settings.

Important: The X-pstn-settings field is not available in a message that was delivered to multiple (envelope) recipients. However, if the sending mail server establishes a separate connection for each recipient, then an individual recipient's spam-setting information is displayed in the header field.

The format of this header field is:

```
X-pstn-settings: Bulk_Filter_Setting (Base_Threshold : Effective_Threshold) category_filters
```

Example:

```
X-pstn-settings: 5 (2.0000:8.0000) r p M C
```

The first number is the user's Bulk Filter (base) spam setting:

- 1= lenient
- 2= less lenient
- 3= moderate
- 4= more aggressive
- 5= most aggressive

In the example above, the user's bulk filter was set to 5, the most aggressive setting.

The parenthesized pair of numbers indicate the user's base threshold and effective threshold. These are derived values and should not be directly interpreted, as they are subject to change.

If any C, M, P, or R filter that the user turned on has a value less than 85, the effective threshold value is a multiple of the base threshold value. If none of these filters is less than 85, the threshold value is the same as the base value.

The final letters on the line indicate which filters the user had turned on and which had values less than 85 (these are in upper case). In the above example, the make-money-fast (M) and the commercial offer (C) category filters were triggered.

If a category filter is turned off, the letter representing it does not appear on this line.

You may also see the letters CV in the X-pstn-settings field. This indicates suspicious (but uncertain) virus-like message content. If the message is otherwise normal, this does not necessarily stop the message.

Determining Whether or Not the Message is Spam

The final step in determining whether an email is quarantined or not is to compare the spam score against the threshold value.

If the spam score is less than the effective threshold, the email is considered spam. If it is greater than or equal to the effective threshold, the email is sent to the recipient's inbox.

Example:

```
X-pstn-levels: (S: 0.00000/60.95723 R:95.91080 P:95.91081
M:64.93900 C:93.23770 )
X-pstn-settings: 5 (2.00000:8.00000) r p M C
```

In this example, the spam score is 0.00000 and the effective threshold is 8.00000. Since 0.00000 is less than 8.00000, this message is spam.

X-pstn-2strike Header Field

An exception to the spam score and threshold calculations is the `x-pstn-2strike` header field. The `x-pstn-2strike` field indicates that the spam score was below the effective threshold, but was likely a valid message. This is based on the IP address of the sender and other message characteristics. If the spam score (S:) is greater than 0.15, the message was allowed through as a valid message.

Example:

```
X-pstn-levels: (S: 0.22604/99.8045 R:97.45080 P:76.42022 M:64.93900
C:93.23770 )
X-pstn-settings: 5 (2.00000:1500.00000) r P M c
X-pstn-2strike: clear
```

In this example, the `X-pstn-2strike` is set to “clear” so the message was delivered.

X-pstn-xfilter Header Field

The `x-pstn-xfilter` header field indicates that the message triggered a global pattern rule. The message security service maintains a minimal number of these rules to ensure that certain messages are quarantined as spam, regardless of the spam score.

One example of a global pattern rule is the presence of “ADV:” in the message subject line. The United States CAN-SPAM act mandates that any message with ADV: in the subject line should be considered an advertisement; even if the message doesn't score as spam, this global rule ensures that the message is quarantined. Global pattern rules may occasionally be used as a method to respond quickly to new types of spam.

Example:

```
X-pstn-xfilter: yes
```

In this example, the X-pstn-xfilter is set to “yes” so the message was processed as junk mail.

X-pstn-neptune Header Fields

This header field indicates that although the message did not score as spam, it was likely a junk message based on the sending system's behavior, and therefore quarantined:

```
X-pstn-neptune-rslt: qtine
```

The header field “X-pstn-neptune” contains only internal scoring information, and looks similar to this:

```
X-pstn-neptune: 287/236/0.8223004.2/59
```

Occasionally, you may see this header field, which is also used for internal monitoring:

```
X-pstn-neptune-rslt: pass
```

You may also see the following header field, which indicates that the message has suspicious behavior and content and may be treated as a virus:

```
pstn-neptune-cave-rslt: virus
```

If a message triggers Early Detection for viruses, this field appears in the message header:

```
X-pstn-neptune-cave-rslt: pbox
```

Industry Heuristics Header Fields

Industry Heuristics (optional feature) generates these header codes:

- **LC**: legal content
- **FC**: financial content
- **LT**: legal transport
- **FT**: financial transport

The transport codes only appear on the settings line; the content codes appear on both the levels and settings lines.

If content or transport filtering is triggered, the code appears in uppercase letters on the `x-pstn-settings` line. If filtering isn't triggered, the codes appear in lowercase letters.

Content Header Field Example

In this header field example, Industry Heuristics for financial and legal content were turned on.

```
X-pstn-levels:      (S: 0.9403/ 9.86262 FC:95.5390 LC:95.5390  
R:95.9108 P:95.9108 M:98.9607 C:66.2733 )  
X-pstn-settings: 3 (1.0000:2.0000) fc lc r p m c
```

The scores for these categories appear on the levels line, **FC:95.5390 LC:95.5390**. As with the other categories, filtering triggers when their scores drop below 85. In this case, neither triggered, so they appear in lowercase on the settings line.

In the next example, the organization had the Industry Heuristic legal content and legal transport categories turned on.

```
X-pstn-levels:      (S: 0.00000/ 4.76962 LC: 0.1839 R:95.9108  
P:95.9108 M:81.1584 C:97.1311 )  
X-pstn-settings: 3 (1.0000:0.0000) LC lt r p M c
```

The score for legal content category appears levels line, **LC: 0.1839**. The score is less than 85, which triggers the category. Because this category was triggered and because the legal-content filter was set to the highest value, the effective threshold on the settings line was set to zero (1.0000:0.0000). The effective threshold is compared to the spam score. If the spam score is less than the effective threshold, the message is spam. In this example, the spam score and effective thresholds are both zero, so the message is considered valid and is passed through to the recipient inbox.

Transport Header Field Example

In this header field example, Industry Heuristics for legal transport were turned on.

```
X-pstn-levels:      (S: 0.0041/ 14.36962 R:95.9108 P:95.9108  
M:99.4056 C:78.1961 )  
X-pstn-settings: 3 (1.0000:2.0000) lt r p m c
```

The **lt** code on the settings line indicates that the legal transport category was turned on, but not triggered (it would be **LT** if triggered). The transport categories are not assigned numeric scores and don't appear in the `X-pstn-levels` line.

General Transport Heuristics Header Fields

The General Transport Heuristics engine analyzes both the contents of a message as well as the source of the message. Senders of ~100% valid email are given a bias against being quarantined as spam. These "trusted senders" are not added to a white list. These senders continue to be subject to spam filters, but the general transport heuristic lowers the risk that email from valid senders might be accidentally quarantined.

The purpose of general transport heuristics is to reduce false quarantines by creating a "reputation" database of sender behavior.

If one of the general transport-heuristic categories triggers, it shows up like any other category in the `X-pstn-settings` header field with a **GT1**, **GT2**, or **GT3**. **GT** stands for General Transport, and the three categories indicate the level of trust, with **GT1** being the most trusted. Each of the levels has an assigned multiplier that adjusts the spam threshold based on its level of trust. If a General Transport heuristic has been triggered, the "GT" is capitalized.

Here's a sample header field where a General Heuristics category was triggered:

```
X-pstn-settings: 3 (1.0000:0.1000) s gt3 GT2 gt1 r p m C
```

All customers benefit from this feature. There are no configurations associated with General Transport heuristics.

X-pstn-addresses Header Field

Following is an example of a X-pstn-addresses header field:

```
X-pstn-addresses: from agoodman@jumboinc.com forward (user good)
[1119/49]
```

agoodman@jumboinc.com is the From address used in evaluating the user's approved- and blocked-sender lists. If the address appears on one of these lists, the processing is terminated and the disposition is noted on this line.

The text after the address can be one of the following options. (If nothing appears, the address was not on any of the following lists.)

forward (org good)	Address is on the organization's Approved Senders list.
quarantined (org bad)	Address is on the organization's Blocked Senders list.
forward (user good)	Address is on the user's Approved Senders list.
quarantined (user bad)	Address is on the user's Blocked Senders list.
forward (good recip)	Address is on the user's Approved Mailing List.

[1119/49] is a summary of the *user's* approved-senders list. The first number is the total number of characters in the approved-senders list. The second number is the total number of entries in the list. In the above example, there are 1119 characters in the approved-senders list, and the total number of entries in the list is 49. If there are no entries in the user's approved-senders list, the summary is displayed as [db-null].

In the example below, the message bypassed the spam filters because the sending address was on the recipient's organizational approved-senders list as noted by (org good). The entry [db-null] indicates the recipient doesn't have any user-level approved senders.

```
X-pstn-addresses: from kersten@jumboinc.com forward (org good) [db-
null]
```

The X-pstn-addresses header field does not appear if the message was sent to multiple users of the message security service.

X-pstn-disposition Header Field

This header field indicates the message was delivered from a user's Message Center. The disposition is shown on the X-pstn-disposition line.

Example:

```
X-pstn-disposition: quarantine
```

This field states that the message was quarantined by the message security service and was then delivered to the inbox from the Message Center.

X-pstn-nxpr and X-pstn-nxp Header Fields

When messages are delivered to Google Gmail, these header fields are added, and display information similar to the following:

```
X-pstn-nxpr: disp=neutral, envrcpt=address  
X-pstn-nxp: bodyHash=e7a578306639faf47072571274493f2ce89341bc
```

These header fields refer to only internal information.

Attachment Manager and Content Manager Header Fields

Attachment Manager and Content Manager add header fields when they quarantine an email message.

Note that if you set Attachment Manager or Content Manager to block or blackhole messages, these fields are not added.

Attachment Manager Header Fields

If Attachment Manager quarantines a message, the message does not have normal spam header fields. Instead, there is only one header field:

```
X-pstn-disposition: quarantine
```

If the sender appears on the organization-based Approved Senders list, the message containing the attachment is passed on to the recipient inbox. The header field looks like this:

```
X-pstn-attach-addresses: from sender@address.com (approved)
```

Attachment Manager does not evaluate the user's Approved Senders list.

X-CM Header

If a Content Manager filter is triggered, the following line appears in the header:

X-CM: *(name of triggered Content Manager filter)*

For example:

X-CM: ConfidentialBilling

You create filter names when you create or edit filters in Content Manager.

Analyzing Header Fields

Following are the header fields in an example message:

```
X-pstn-levels: (S: 0.46800 R:95.91081 P:95.91081 M:99.85141
C:55.44761 )
X-pstn-settings: 5 (2.00000:8.00000) r p m C
X-pstn-addresses: from <junkyjunk9@hotmail.com>
X-pstn-disposition: quarantine
```

The header fields give this information about the message

- The overall spam score is 0.46800.
- The only junk mail filter triggered was the Commercial Offer filter (C).
- The user's Bulk Spam filter was set to Most Aggressive (5).
- The Effective threshold was 8.00000
- This message was quarantined in the Message Center (X-pstn-disposition header)

This message is evaluated as spam based on comparing the spam score (S: 0.46800) against the threshold value (8.00000). If the spam score is less than the effective threshold, the message is considered spam. In this example, 0.46800 is less than 8.0000, so this message is spam.

Appendix B

Customizing Notifications

About Customizing User Notifications

Although it is not necessary to edit notifications messages, you may customize the text of the notification messages. You might do this for branding purposes, or to provide further information or details to your users.

If you choose not to customize any notifications, the default email that is automatically generated includes a basic message with your organization's branding included.

Notification messages use tokens. These are special parts of the notification, which dynamically generate appropriate information each time a notification is sent.

Customizing Notifications

We recommend that you do retain the basic content of the message. Otherwise you may be preventing your users from receiving critical information they need to maintain their Message Center account.

If you choose not to customize any notifications, the default email that is automatically generated includes a basic message with your organization's branding included.

Editing User Notifications Text

Editing notifications for an organization:

1. In the Administration Console, click the Orgs and Users tab, and choose an organization from the Choose Org pull-down list. Typically, you will choose an organization which contains users, rather than an email config or account.
2. Scroll down to the General Settings section and click the Notifications icon.

3. On the User Notifications page, click the link to a notification. For example, click the “Welcome New User” link to edit the welcome message.

User Notifications - Administrators		View	Edit
Manage notification messages sent to users in this organization. To change settings, click the Edit link above. To customize message texts, click a link below. (By default, messages include your company name and don't typically need to be customized.)			
Notification	Status/Frequency		
Welcome New User	Status: On	When Sent: Within 24 hours of account creation	
Virus	Frequency: Immediately		
My First Spam	Status: On	When Sent: Upon receipt of first spam	
New Spam	Status: On	Frequency: Every 7 days	
Suspension	When Sent: Immediately after suspension		

4. Choose one of the four options for customizing notifications.
 - Edit a notification: Insert your own text in the text box, and use “tokens” for displaying variables. See “Editing Text with Tokens” on page 652.
 - Upload a File: Create the notification in an external editor and upload the message. This is useful when editing HTML-based messages (see “HTML Editing for Notifications” on page 653).
 - Remove Notification: You can revert to the default notification which is used if no custom notification is set. This includes basic branding and is a safe choice if your edited notification becomes problematic.
 - Link Notification: You can synchronize your notifications with another organization.

Keep in mind that the “stock” notification and the “default” notification are not the same. The stock notification is what the parent organization supplies one time only to a sub-organization when that organization is created; whereas the default notification is the original system-wide template.

They could be the same”, but if the parent organization modified the default before the sub-org was created, the sub-org received a copy of the customized message. Further, by “linking” to another organization, the notification is updated whenever the other organization makes any changes.

The text customization field in the Edit Notification page:

Edit Notification - Administrators

Select the source of this organization's Welcome notification. Note that if you specify text other than the default, you must include the Date, From, To, & Subject header fields at the very top of the form for the message to deliver properly.

You may include any of these tokens in your custom text. When the message is generated, they will be filled in.

Token	Meaning
<-address->	A specific user's email address (also used as name/ID).
<-date->	The date when the notification is sent.
<-from->	The return address referenced as your organization's support mailto.
<-initialPassword->	Assigns initial password, only if PMP auth (not POP, etc.)
<-isp->	Your organization's "customer name".
<-loginhost->	Login page for accessing the user's Message Center.
<-notice_address->	Used alternatively to "address" if administrator-managed services.
<-passwdNotice->	Password help text that is customized according to auth method. Not applicable to cross-authentication

Scroll down the page to see the other notification options:

OR: you may upload your message from a file on your computer.

OR: you may [Remove this message](#), restoring the default welcome message.

OR: you may link to the welcome message from another organization:

If you have enabled the Quarantine Summary, you will see these editing options:

Message Text

Enter the text for the Quarantine Summary - it will be placed at the top of the message, quarantine tables.
(No more than 500 characters.)

These messages were quarantined before they reached your inbox as potential spam and virus-infected messages. The quarantined messages can be delivered within your personal Message Center.

5. Click the Submit button to save your changes.

Make sure to include header information (“Date:”, “From:”, “To:” & “Subject:”) as seen in the templates at the top of the text field. If no header information is included, then the notification messages will bounce.

Pay special attention to the tokens that you can insert into the text. If they are mis-typed, then they will not be replaced with the associated value.

Editing Text with Tokens

If you decide to edit a notification to customize it for the organization, you should be aware that each message relies upon “tokens” for inserting variables into the message. The available tokens for each notification are listed in the Edit Notification page and described in the following sections.

When you insert a token into your message, one of the following text modifications is made:

- Variables Inserted from the message security service - the message security service inserts the current variable for a system-level parameter. For example, the current location of the standard Message Center login page.
- Customer Variables Inserted - the message security service inserts the variable associated with that customer. For example, the name of the customer.
- User-Specific Variables Inserted - the message security service inserts the variable associated with that specific user. For example, the number of quarantined messages for that user currently pending review.
- Contextual Text Adjustment Inserted - the message security service modifies the text to remain contextually consistent. For example, “it” can be pluralized to “them” depending on the quantity of another token.

The use of tokens provides for a consistent notification template (wrapper text) that includes accurately inserted variable data. It allows notifications to remain accurate by dynamically referencing current data within your organization, even as your user base scales in size.

For example, you should use the token for the “From” address rather than hardcoding an actual support address. Then if you change the “Support Contact” for your organization, you can be assured the change is reflected in all notifications sent to your users.

Wrapping Text around Tokens in Notifications

Once you determine what content your customized message should include for a particular notification, you may simply compose the text and insert any tokens you wish to use within that message. It is advisable that you use all of the tokens supplied for a particular notification, since they all serve a relevant purpose for explaining the nature of the notification. Otherwise, you can use virtually any wrapper text that is relevant to your organization's needs.

To edit a notification, you may use either the editing window provided within the Administration Console or upload a text file, the latter being more helpful for allowing you to compose an HTML message and error check your composition as well.

After you have edited your text or uploaded a file, your notification will be in effect for your organization once you click “Save Text” from the text-editing window. Be sure the text is accurate before proceeding!

HTML Editing for Notifications

If you wish to create an HTML notification, it may be easier to compose your notification message in an external editor to error check the message, send the message to yourself to ensure proper MIME encoding, and then save and upload the finished file. This error checking of your composition beforehand is advisable since HTML tags could potentially conflict with token tags if brackets are not closed properly. You will also want to ensure your message will be viewed and encoded properly.

Editing your notification in HTML allows you to insert links to external images that you can host on your web site—allowing you to brand each notification with custom graphics whenever the user receives and views the notification. For example, the “Virus Alert” notification could include a red stop sign inserted.

HTML messages only differ from plain text messages by including HTML-specific tags that enhance the impact of the message. Organizations that supply their users with a web-based inbox will likely want to send notifications in HTML to remain consistent with current branding, but it is not required to do so.

To include HTML content in notification messages:

1. Insert the following line at the top of the notify text:

```
Content-Type: text/html
```

2. On the next line start with the From, To, and Subject headers in plain text (no HTML).

3. After the Subject of the e-mail, leave a blank line and then include the following HTML text:

```
<html>
<body>
```

4. After the body content of the HTML notification insert:

```
</body>
</html>
```

5. The message should look something like this:

```
Content-Type: text/html
Date: <-date->
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: <-isp-> First Junk Email Safely Quarantined
```

```
<html>
<body>
... </body>
</html>
```

The first line, `Content-Type: text/html`, is the HTML MIME Type header. This is what tells the mail client to expect HTML content in the e-mail. Most content transferred across the Internet has a MIME type. If a MIME type is not set, then plain text is assumed.

The `From`, `To`, and `Subject` headers are important as they control how the message is sent. If these headers are omitted then the message will not be sent properly.

The `<html>` and `<body>` tags are containers for the HTML content. These tags should not be placed before the subject field because that is part of the mail message's headers. Header content should not contain any HTML code since it is straight text data used only for analysis of email.

Between the `<body>` and `</body>` tags, use any HTML code that email clients can interpret. For example, you can use `` tags to display an image which lives on your web server.

6. Save and upload the file as a custom notification. See "Editing User Notifications Text" on page 649 for instructions.

Default Notifications with Tokens

Here is full text for the default notifications including token definitions.

Welcome New User Notification

Users receive a welcome message when they are added to the system. If the user is added manually, this notification arrives within 24 hours; however, if the user is created automatically ("Autocreated"), then the notification is generated immediately when the account is created.

The default Welcome New User notification message:

```
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: <-isp-> has Activated your New Mail Services!
```

Dear <-address->,

<-isp-> has activated your virus and junk mail protection services.
You should log in to your personal, password-protected
<-isp-> Message Center as soon as possible.

Your login address is: <-address->

<-passwdNotice->

To log in to your <-isp-> Message Center, use this link:

<http://login.postini.com/exec/login?email=<-address->>

You may also modify your default settings or deactivate any
services.

Thank You! <-isp->

The "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The tokens available for the New User notification are:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-address->

The specific user's email address.

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line—if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator manages a user's Message Center on behalf of the user — for example, in a corporate environment to enforce user-level settings while also denying account access.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

<-passwdNotice->

Password help text that is customized according to authentication method. Not applicable to cross-authentication.

<-initialPassword->

Assigns an initial password upon user account creation, only if using PMP authentication. (Do not use this token when using other authentication methods such as cross-authentication.)

<-loginhost->

The current login URL for accessing a user's Message Center.

To send users to the standard login page, a compound string is required within your notification message for generating the correct URL and inserting the user's ID in the login page. The complete string would look as follows:

```
http://<-loginhost->/exec/login?email=<-address->
```

When using the above string in your notification, the user would only need to enter a password to log in after clicking the link.

However, if you are using the “Login Widget” on your web site to provide remote, branded, access to the Message Center for your users, you can alternatively send users to the page directly that hosts the Widget by simply inserting the URL and disregarding the use of tokens. For example, you might use in your notification:

```
http://www.jumboinc.com/messagecenter
```

where the URL is the location of the Widget for your organization.

Password Reset Notification

Users receive this notification when an administrator resets their password.

The default Password Reset notification message:

```
Date: <-date->
From: <-from->
To: <-address>
Subject: Password Notification from <-isp->
```

Dear <-address->,

For security reasons, we have reset your password. Please use the temporary password below to log in to your Message Center.

Your new password is:

```
<-initialPassword->
```

Log in by following this link:

```
<-loginhost->
```

Once you log in, you will be asked to change the temporary password. If you require additional assistance, please contact your administrator.

Thank you!
<-isp->

The "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The tokens available for the Password Reset notification:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-address->

The specific user's email address.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

<-initialPassword->

Assigns a password when an administrator resets the password, only if using PMP authentication. (Do not use this token when using other authentication methods such as cross-authentication).

<-loginhost->

The current login URL for accessing a user's Message Center.

Note: To send users to the standard login page, a compound string is required within your notification message for generating the correct URL and inserting the user's ID in the login page. The complete string would look as follows:

```
http://<-loginhost->/exec/login?email=<-address->
```

When using the above string in your notification, the user would only need to enter a password to log in after clicking the link. However, if you are using the "Login Widget" on your web site to provide remote, branded, access to the Message Center for your users, you can alternatively send users to the page directly that hosts the Widget by simply inserting the URL and disregarding the use of tokens. For example, you might use in your notification:

```
http://www.jumboinc.com/messagecenter
```

where the URL is the location of the Widget for your organization.)

My First Spam Notification

Users receive this message when they receive their first junk mail.

The default My First Spam notification message:

```
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: <-isp-> First Junk Email Safely Quarantined
```

Dear <-address->,

<-isp->'s new junk email protection service has quarantined its first suspected junk email message directed at you. Since you have not signed in at your personal <-isp-> Message Center, we are sending this notification informing you of the service's initial action. After this notification, we will begin the standard practice of sending notifications of quarantined messages on a regular basis.

You can inspect your suspicious email at:

<http://login.postini.com/exec/login?email=<-address->>

<-inactive2->

Suspicious email is kept in your <-isp-> Message Center for 14 days, after which it will be automatically deleted.

Please visit your <-isp-> Message Center to deliver valid email or delete messages you do not want.

For help accessing and configuring your <-isp-> Message Center, please visit:

<http://www.postini.com/services/help.html>

Thank You!

<-isp->

The "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The tokens available for the My First Spam notification:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-address->

The specific user's email address.

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line-if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator might manage a user's Message Centers on behalf of the user-for example, in a corporate environment to enforce user-level settings while also denying account access.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

<-inactive2->

Login information for the user if using PMP authentication, otherwise nothing. If using PMP as the authentication method for your organization, you must provide a temporary password for the user to log in to his or her Message Center. The Message Center login recognizes when a first time log in has occurred and will prompt the user to change the password to a permanent one after the successful login. By using this token, a string appears automatically in the notification as:

Your temporary password is: [RANDOM PASSWORD GENERATED]

<-loginhost->

The current login URL for accessing a user's Message Center.

Note: To send users to the standard login page, a compound string is required within your notification message for generating the correct URL and inserting the user's ID in the login page. The complete string would look as follows:

```
http://<-loginhost->/exec/login?email=<-address->
```

When using the above string in your notification, the user would only need to enter a password to log in after clicking the link. However, if you are using the "Login Widget" on your web site to provide remote, branded, access to the Message Center for your users, you can alternatively send users to the page directly that hosts the Widget by simply inserting the URL and disregarding the use of tokens. For example, you might use in your notification:

```
http://www.jumboinc.com/messagecenter
```


where the URL is the location of the Widget for your organization.)

New Spam Notification

Your users receive the New Spam notification when suspicious messages are held in their Message Center quarantine, pending review. The time period between notifications is determined through the “Notification Interval” setting.

The default New Spam notification:

```
Date: <-date->
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: <-isp-> Detected Potential Junk Mail

Dear <-address->,

<-inactive1->

<-isp->'s junk mail protection service has detected some
suspicious email message<-s-> since your last visit and directed
them to your <-isp-> Message Center.

You can inspect your suspicious email at:
  http://login.postini.com/exec/login?email=<-address->
<-inactive2->
Suspicious email is kept for 14 days, after which it will be
automatically deleted. Please visit your <-isp-> Message Center
to delete unwanted messages and check for valid email.

For help accessing and configuring your <-isp-> Message Center:
  http://www.postini.com/services/help.html

Thank You!
<-isp->
```

The “Date:”, “From:”, “To:” & “Subject:” lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The tokens available for the New Spam notification:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-address->

The specific user's email address.

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line-if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator might manage a user's Message Centers on behalf of the user-for example, in a corporate environment to enforce user-level settings while also denying account access.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

<-inactive1->

Inserts a stock warning if a user has never visited the Message Center. This appears as:

```
*****  
** Please Note! You have not yet checked your Message Center. **  
** Log in now to review suspicious messages sent to your account. **  
*****
```

<-inactive2->

Login information for the user if using PMP, otherwise nothing. If using PMP as the authentication method for your organization, you must provide a temporary password for the user to log in to his or her Message Center. The Message Center login recognizes when a first time log in has occurred and will prompt the user to change the password to a permanent one after the successful login. By using this token, a string appears automatically in the notification as:

Your temporary password is: [RANDOM PASSWORD GENERATED]

<-loginhost->

The current login URL for accessing a user's Message Center.

Note: To send users to the standard login page, a compound string is required within your notification message for generating the correct URL and inserting the user's ID in the login page. The complete string would look as follows:

```
http://<-loginhost->/exec/login?email=<-address->
```

When using the above string in your notification, the user would only need to enter a password to log in after clicking the link. However, if you are using the "Login Widget" on your web site to provide remote, branded, access to the Message Center for your users, you can alternatively send users to the page directly that hosts the Widget by simply inserting the URL and disregarding the use of tokens. For example, you might use in your notification:

```
http://www.jumboinc.com/messagecenter
```

where the URL is the location of the Widget for your organization.)

Quarantine Summary Notification

The Quarantine Summary (an optional feature) is an email containing a comprehensive list of all the messages that have been quarantined in the Message Center since the previous Quarantine Summary.

Unlike other notifications, the Quarantine Summary does not include token definitions. You can customize your Quarantine Summary by entering the URL of your own logo, and by changing the Message Text; for example:

```
These messages were quarantined before they reached your inbox as potential spam and virus-infected messages. The quarantined messages can be delivered within your personal Message Center.
```

The message text is placed at the top of the Quarantine Summary email, above the message tables.

Virus Alert Default Notification

Your users receive the Virus Alert whenever a virus-infected message is quarantined within their Message Center, pending review. This notification is generated immediately whenever an infected message is found

The default virus notification is:

```
Date: <-date->
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: <-isp-> Detected Potential Virus
```

Dear <-address-> ,

```
<-isp->'s virus protection service has detected a potential email virus. This suspicious message has been quarantined in
```

your <-isp-> Message Center:
From: <-vfrom->
Subject: <-subject->
Virus: <-virus->
You can read the message without infecting your computer.

Click on the link to access your <-isp-> Message Center:
<http://login.postini.com/exec/login?email=<-address->>

Thank You!
<-isp->

The "Date:", "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

Tokens available for you to use in this message include:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-address->

The specific user's email address.

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line-if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator might manage a user's Message Centers on behalf of the user-for example, in a corporate environment to enforce user-level settings while also denying account access.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

<-virus->

The name of the quarantined virus.

<-vfrom->

The sender of the virus-infected message is provided for reference to the user.

<-subject->

The subject line of the virus-infected message can be provided for reference to the user.

Suspend User Notification

The default Suspend User notification template is:

```
Date: <-date->  
From: "<-isp-> Support" <<-from->>  
To: <-notice_address->  
Subject: Your Account
```

Dear <-address-> ,

Your value-added email services are now DISCONTINUED. Any suspicious messages that may have been quarantined in your private Message Center have been forwarded to your email account.
<-extra->

Please be advised that your request to discontinue these services may result in junk mail or virus-infected messages arriving to your inbox without the benefit of filtering.

<-isp-> Support
<-from->

The "Date:", "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The available tokens for the Suspend User notification are:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-address->

The specific user's email address.

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line-if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator might manage a user's Message Centers on behalf of the user-for example, in a corporate environment to enforce user-level settings while also denying account access.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

<-extra->

If web access is disabled, explains that; otherwise nothing

Attachment Manager Notification

Below is the default notification for both inbound and outbound Attachment Manager quarantined messages. This text is the same for both the user and the administrator notification messages.

```
<-isp->
Date: <-date->
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: Quarantined a Message with an Attachment

Dear <-address->,

<-isp->'s email protection service has quarantined an email message
containing an attachment.

<-quarantine_action->:

Date: <-date->
From: <-sender->
To: <-recipients->
Subject: <-subject->
Attachment(s): <-attachments->

Thank You!
```

The "Date:", "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The available tokens for the Attachment Manager notification are:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line-if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator might manage a user's Message Centers on behalf of the user-for example, in a corporate environment to enforce user-level settings while also denying account access.

<-quarantine_action->

Set automatically based on where the message has been quarantined. If the message is in the user's quarantine, the information displayed is:

Please visit your message center to deliver this message:

If the message is in administrator's quarantine, the information is:

Please contact your administrator for information about delivering this message:

<-address->

The email address of the notification recipient, which can be the user address, the quarantine redirect address or both (specified in the Notifications settings).

<-attachments->

The list of the types and filenames of the attachment.

<-recipients->

The list of recipients for the message that triggered the Attachment Manager filter.

<-sender->

The address of the sender of the message that triggered the Attachment Manager filter.

<-subject->

The subject of the quarantined message.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

Early Detection / Pending Quarantine Notification

Below is the default notification for messages sent to the Pending Quarantine in Message Center.

```
From: "<-isp-> Support" <<-from->>
To: <-notice_address->
Subject: <-isp-> Threat Detection (<-vfrom->)
```

RE: <-subject->

Dear <-address-> ,

<-isp->'s email security service has detected a possible virus and has placed the following message in the Pending Quarantine in your Message Center:

```
From: <-vfrom->
Subject: <-subject->
```

To view the message:

1. Log in to your Message Center: <http://<-loginhost->/exec/login?email=<-address->>
2. Click the PENDING tab to safely view a list of quarantined messages.
3. If the message is not on the Pending tab: The message was automatically delivered to your inbox, or the message contained a virus and was deleted or moved to the Viruses tab.

How the protection works: <-isp->'s email security service automatically performs additional virus scanning on this message for <-release_time-> hours for your protection. If a virus is found, the message is deleted or moved to your Virus quarantine. Otherwise, the email security service delivers the message to your inbox as usual.

Thank You!

<-isp->

The "Date:", "From:", "To:" & "Subject:" lines must be at the top of a custom notification, since they are used as the actual message headers for the message when sent out. If they are not included, then the custom notification messages will bounce.

The available tokens for the Early Detection notification are:

<-date->

The timestamp indicating the date and time the notification was sent.

<-from->

The return address, referenced as your organization's Support Contact in the "Support Address" field (see organization record).

<-notice_address->

Used as the location to send notifications as found on each user's user record. Note: By inserting this address as the "To" recipient, the notification is sent to a recipient which may not necessarily be the owner of the Message Center account. In most cases, you should use the Notice Address for the "To" line-if no "Notice Address" address exists for a user record, this field defaults to inserting the normal user "Address" (above). The Notice Address is especially important if another administrator might manage a user's Message Centers on behalf of the user-for example, in a corporate environment to enforce user-level settings while also denying account access.

<-address->

The email address of the notification recipient, which can be the user address, the quarantine redirect address or both (specified in the Notifications settings).

<-subject->

The subject of the quarantined message.

<-isp->

The <-isp-> token is replaced by the value in the "Customer Name" field of the organization.

Appendix C

Usage Details

About Usage Details

Usage Details is an optional feature in the message security service. Each month the message security service generates data for user accounts and settings.

Important: The pages are for your viewing only; please contact your vendor for your specific account and billing information.

The usage data can be exported in tab-delimited format for your review, use, and analysis.

How are Statements Calculated?

Following are the guidelines used to calculate the data in the statements.

- On the first day of each month, the number of user accounts are counted. This number of accounts is included the current month of the statement.
- The count is taken as a snapshot. For example, accounts that are created and then deleted during the month are not displayed.
- Aliases (alternate addresses) are not counted as separate user accounts.
- Fully suspended users (users suspended using the batch command `suspenduser -hardsuspend`) are not counted as accounts in the statements.

Viewing Usage Details

The statements for your account over the last three months are available in the Administration Console. When a new statement is generated, the last statement is permanently removed.

1. In the Administration Console, go to Orgs and Users > Orgs.
2. Select your account from the Choose Orgs list. The Usage Details information is only available from the account org.

3. In the Account page, click the Usage Details link. (If you do not see the Usage Details link, you may not have viewing permissions, and should contact your administrator.) Customers in the evaluation/trial period will not see the Usage Details link.

Monthly Usage Details - Postini Training Account

The following breakdowns of your usage details are available to download for your review, analysis, and use. These monthly statements (posted on the 1st of every month) can be very helpful for extracting the settings and locations of users.

Detailed Usage	Detailed statement includes: organization name, user name, account creation date if available, number of alternate email addresses, and application settings. Dec 2005 Nov 2005 Oct 2005
Usage by Organization	Summary statement by Organization includes: organization name, # of MCAs (Message Center Accounts), # of MCAs with Spam turned on, # of MCAs with Virus turned on, # of MCAs with Wireless turned on, and number of alternate email addresses. Dec 2005 Nov 2005 Oct 2005
Usage by Domain	Summary statement by Domain includes: organization name, # of MCAs (Message Center Accounts), # of MCAs with Spam turned on, # of MCAs with Virus turned on, # of MCAs with Wireless turned on, and number of alternate email addresses. Dec 2005 Nov 2005 Oct 2005
Alternate Addresses	Sorted by organization, displays user names and their alternate email addresses (aliases). Dec 2005

4. Click a usage link. The usage details will open in a separate window, and can be saved and exported as a tab-delimited file. Usage details are described in the next section.

Interpreting Usage Details

The Usage Details are available in four formats.

- Detailed Usage
- Usage by Domain
- Usage by Organization
- Alternate Addresses

The data and format of the statements are described below.

Note: Since the columns and data in the statements often does not line up visually, you may import the statements (as tab-delimited files) into spreadsheets or other reporting tools for easier reading.

Detailed Usage Details

Following are descriptions of the columns that appear in the Detailed Usage:

Column	Description
Org name	Name of organization
User Name	User account address
Creation Date	Date account was created
Spam	Y (yes) or N (no) indicates whether junk email filtering is turned on or off for that user
Virus	Y (yes) or N (no) indicates whether virus filtering is turned on or off for that user
Wireless	Y (yes) or N (no) indicates whether delivery of email to a wireless device is turned on or off for that user
Alt Address	The number of alternate addresses for the user (for example, <code>user@jumboinc.com</code> and <code>user@corp.jumboinc.com</code> , <code>user@jumboinc.net</code>)

Usage by Organization

Following are descriptions of the columns that appear in Usage by Organization:

Column	Description
Org name	Name of organization
MCAs	Number of user accounts in the organization (MCA stands for "Message Center Account")
Disinfection	Number of users who have the "clean and deliver" setting for viruses
Spam	Number of users who have <i>only</i> spam filtering turned on
Virus	Number of users who have <i>only</i> virus filtering turned on
Spam and Virus	Number of users who have spam and virus filtering turned on
Spam or Virus	Number of users who have either spam or virus filtering turned on
Wireless	Number of users who have the wireless application turned on

Column	Description
Nothing	Number of users who have no filtering (no spam, virus, or wireless email delivery), but are not suspended.
Alt Address	The total number of alternate users addresses in the organization (for example, <code>user@jumboinc.com</code> , <code>user@corp.jumboinc.com</code> , <code>user@jumboinc.net</code>)

Usage by Domain

Following are descriptions of the columns that appear in the Usage by Domain:

Column	Description
Domain name	Name of domain
MCAs	Number of user accounts in the domain (MCA stands for “Message Center Accounts”)
Disinfection	Number of users who have the “clean and deliver” setting for viruses
Spam	Number of users who have only spam filtering turned on
Virus	Number of users who have only virus filtering turned on
Spam and Virus	Number of users who have spam and virus filtering turned on
Spam or Virus	Number of users who have either spam or virus filtering turned on
Wireless	Number of users who have either spam or virus filtering turned on
Nothing	Number of users who have no filtering (no spam, virus, or wireless email delivery) but are not suspended.
Alt Address	The total number of users’ alternate addresses in the domain (for example, <code>user@jumboinc.com</code> , <code>user.name@jumboinc.com</code>)

Alternate Addresses in Usage Details

The Alternate Addresses usage details lists the users by organization, and the user’s alternate addresses (aliases). Unlike the other statements, the Alternate Addresses kept for only a single month.

Appendix D

Configuring Intradomain Filtering

About Intradomain Filtering

You can integrate the message security service into your current mail system to filter intradomain traffic. This appendix explains intradomain routing and how your Sendmail server interacts with intradomain routing.

A traditional mail server configuration is a single email server name for both incoming email (POP/IMAP) and outgoing email (SMTP). In the examples that follow, this server will be referred to as `mail.jumboinc.com`.

When the message security service is activated, all incoming emails from users outside of your mail server are routed first through the message security service servers, and then to `mail.jumboinc.com`. This means the message security service processes all email for junk and virus filtering, and wireless messaging.

However, when a user on your mail server sends to another user on the same mail server, the mail server generally drops the message directly into the receiving user's queue. This bypasses the routing of email through the message security service servers. So emails are not filtered for junk, virus, or wireless.

Setting up intradomain filtering requires two steps:

1. Set up a separate outgoing email server *or* reconfigure your existing email server to respond to two IP addresses (requires 2 NIC cards or virtual IPs).
2. Change the outgoing email server name setting in all your user's client software.

For the examples below, `mail.jumboinc.com` is the incoming mail server name and `smtp.jumboinc.com` is the outgoing email server name.

Two Server Setup

A new server must to be set up that will be used for all outgoing email. There are no special server settings that need to be made. Care should be taken to ensure that the new email server (`smtp.jumboinc.com`) uses a DNS server that shows the MX record for `jumboinc.com` to be at the message security service. The clients will all need to be reconfigured to use `smtp.jumboinc.com` as the outgoing email server.

Single Server Setup

This solution requires the use of two network interface cards or virtual IPs. It is recommended that you create a "jail" which runs a second instance of your MTA.

For more information, please check the support site of your vendor.

Index

A

- activation, summary 21
- Administration Console
 - Choose Org list 85
 - Choose Org pull-down 57
 - Home page 52
 - logging in 49
 - Message Composition chart 56
 - navigating 57
 - passwords 50
 - passwords resetting 52
 - Search feature 53
 - security 49
 - Show Hierarchy panel 58, 85
 - Troubleshooting 59
 - User shortcut 53
- Administration Guide
 - audience 15
 - overview 15
 - related documentation 16
 - sending comments about 19
- administrators
 - account administrators 169
 - archive administrators (search/discovery, audit, retention) 180
 - authority privilege propagation 158
 - authorizing administrators 157
 - comparing types of administrators 167
 - compliance officer 176
 - compliance officers 173
 - creating 163
 - deleting authority record 159
 - editing authorization records 164
 - email config administrators 186
 - fully authorized email administrators 169
 - limiting authority 158
 - monitor administrators 173
 - multiple record updates 160
 - organization hierarchy 157
 - organization policy administrator 190
 - POP authentication 166
 - regional administrators 169
 - security administrator 176
 - security administrators 173
 - setting up administrators 162
 - types 166
 - user administrators 194
 - viewing a user quarantine 135
- alerts
 - configuring 489
 - Connection Manager 491
 - Delivery Manager 492
 - Directory Harvest Attack 492
 - Email Bomb 491
 - Email Host Down 492
 - Organization Email Host Down 492
 - overview 489
 - Policy Enforced TLS 448
 - Spam Attack 492
 - Spool Full 493
 - Spool Initiated 493
 - Spool Manager 493
 - Spool Quota Thresholds 493
 - Unspool Complete 493
 - Unspool Initiated 493
 - Virus Outbreak 492
- API. See EZCommand
- approved domains
 - editing in Message Center 393
 - message delivery 389
- approved mailing lists
 - editing in Message Center 393
 - message delivery 389
- approved recipients 388
- approved senders
 - editing for an organization 391
 - editing in Message Center 393
 - how domains are evaluated 391
 - how they're identified 391
 - overview 387, 388
 - propagation of lists 392
- architecture
 - inbound overview 29
 - outbound overview 44

- pass-through processing 35
- processing order 36
- Attachment Manager
 - configuring 406
 - custom types filter 413
 - filter dispositions 410
 - filter editing 409
 - message header fields 646
 - message size filter 412
 - multiple attachments 406
 - productivity files filter 413
 - scanning methods 404
 - system threats filter 413
 - troubleshooting 414
- attachment scanning in Content Manager 335
- audience for this guide 15
- authentication. See user authentication
- authorization
 - account authorization record positions 169
 - authority privilege propagation 158
 - compliance officer and security authorization record position 177
 - creating administrators 163
 - deleting authority record 159
 - editing authorization records 164
 - email config authorization record position 187
 - limiting authority 158
 - monitor authorization record position 173
 - multiple record updates 160
 - organization hierarchy relationship 157
 - organization policy authorization record position 191
 - overview 157
 - privileges for all standard settings 198
 - privileges for archive search, discovery, audit, and retention 203
 - privileges for help desk 199
 - privileges for inbound mail processing 203
 - privileges for organization management 201
 - privileges for user settings 199
 - recommended account settings 170
 - recommended archive settings 183
 - recommended compliance and security settings 177
 - recommended email config settings 188
 - recommended monitor settings 174
 - recommended organization policy settings 192
 - recommended user administrators settings 196
 - setting up an administrator 162
 - troubleshooting 204
 - types of administrators 166
 - user administrator authorization record position 195
- authorization record 157
- automatic attack blocking. See Connection Manager
- automating commands. See batch processing

B

- batch processing
 - overview 611
 - sender lists 395
 - submitting commands 611
 - TLS Alerts 448

- troubleshooting 614
- validation 611
- when to use 612
- best practices 21
- billing statements
 - alternate addresses 674
 - by domain 674
 - by organization 673
 - detailed statements 673
 - how calculated 671
 - interpreting 672
 - viewing 671
- binary scanning
 - for attachments 404
 - overview 412
- Blatant Spam Blocking, use with Content Manager 297
- blocked domains 389
- blocked senders
 - editing for an organization 391
 - editing in the Message Center 393
 - how domains are evaluated 391
 - how they're identified 391
 - overview 387
 - propagation of lists 392
 - sender lists 389

C

- catchall account 241
- certificate validation 445
- certificates 432
- comments about this guide, sending 19
- Compliance Footer
 - overview 518
 - troubleshooting 530
- compliance policies in Content Manager
 - disabling 348
 - introduction 330
 - reordering 347
 - setting up 345
- Connection Manager
 - alerts 491
 - automatic attack blocking 453
 - automatic attack blocking enabling 455
 - Directory Harvest Attack 454
 - Email Bomb 454
 - events 462
 - manual IP blocking 457
 - manual pass throughs 459
 - Network Effect Protection 460
 - overview 453
 - response to attacks 460
 - sensitivity to attacks 455
 - Spam Attack 454
 - troubleshooting 463
 - View page 461
 - Virus Outbreak 454
- content filters
 - creating and editing 340
 - deleting and disabling 348
 - reordering 347

- testing before deployment 369
- troubleshooting 369
- using regular expressions 349
- using to block profanity 367
- using to block spam 364
- when they apply 333
- where they apply 333

Content Manager

- Add/Edit Filter page 372, 374
- allow approved senders to bypass filters 367
- allow valid null-sender messages 368
- compliance policies, disabling 348
- compliance policies, introduction 330
- compliance policies, reordering 347
- compliance policies, setting up 345
- configuring 338
- content filter limitations 336
- content filters, creating 340
- content filters, deleting and disabling 348
- content filters, reordering 347
- custom content filters, introduction 330
- editing content filters 340
- examples of use 331
- features 330
- file attachment scanning, introduction 331
- filter dispositions, descriptions 379
- filter dispositions, order of precedence 336
- Filter List page 371
- filters and policies, viewing 337
- how it scans email 334
- how it works 333
- how Outbound works 335
- introduction 329
- maximum filters allowed 336
- message header fields 646
- outbound message scanning, introduction 331
- page reference 371
- propagating settings and filters to suborgs 338
- regular expressions, examples 356
- regular expressions, how to use 349
- regular expressions, introduction 330
- regular expressions, support limitations 355
- restrict outgoing messages to specific domain 367
- Settings page 372
- Social Security Numbers policy 381
- tips and best practices 365
- troubleshooting 369
- types of attachments scanned 335
- types of content scanned 334
- use with Blatant Spam Blocking 297
- using to block profanity 367
- using to block spam 364
- when filters apply 333
- where filters apply 333
- which message components are scanned 334

Credit Card Numbers policy in Content Manager

- introduction 330
- setting up 345

custom content filters, introduction 330

customer support, receiving 18

D

- Default User**
 - configuring 76, 116
 - overview 114
- Delivery Manager**
 - Alerts 480
 - Edit 475
 - Event types 480
 - Events 479
 - Failover 478
 - How it works 465
 - Load balancing 476
 - Mail flow verification 479
 - Overview 465
 - Setting up 475
 - Troubleshooting 480
- Directory Harvest Attack**
 - alert 492
 - overview 424, 454
- disaster recovery. See Spool Manager
- disclaimer. See Compliance Footer
- distribution lists 147
- DNS records. See MX records
- documentation, related 16
- domains
 - Add Domain page 237
 - adding 236
 - aliases 239, 242
 - catchall account 241, 242
 - changing MX records 238
 - deleting 244
 - editing 243
 - moving 243
 - overview 233
 - settings interactions 242
 - subdomain stripping 240

E

- Email Bomb** 454
- email config 421, 422
- Email Host Down** 425
- email server configuration. See email config
- email servers. See Inbound Servers
- events
 - Connection Manager 462
 - definitions 424
 - fields 426
 - overview 423
 - viewing details 426
- events, Virus Outbreak 321
- extension scanning, attachments 404
- EZCommand**
 - calling commands 613
 - overview 612
 - setting up 613
 - shared secret 95

F

- feedback about this guide, sending 19
- file attachment scanning in Content Manager,

- introduction 331
- filter and processing order 36

H

- header tags. See message header fields

I

- Inbound Servers

- events 423
- how it works 422
- overview 421
- troubleshooting 427
- when to configure 422

- Industry Heuristics

- configuring 418
- message header fields 643
- overview 417

- intradomain filtering

- overview 677
- single server setup 678
- two server setup 678

- IP Blocking. See Connection Manager

- IP range 498

L

- legal compliance footer. See Compliance Footer

M

- mail delivery troubleshooting 531

- mail flow

- inbound for Policy Enforced TLS 440
- outbound for Policy Enforced TLS 441

- mail servers. See Inbound Servers

- mail transport agent. See Inbound Servers

- Mailbomb 425

- mailing lists 147

- Message Center

- branding 267
- configuring access 252
- disabling subject links 261
- documentation for users 270
- language settings 266
- logging in 264
- notifications 262
- overview 247
- passwords 265
- passwords, resetting 265
- security 266
- troubleshooting 270

- Message Center II 250

- message header fields

- Attachment Manager 646
- Content Manager 646
- determining whether or not spam 642
- example 647
- General Heuristics 644
- Industry Heuristics 643
- overview 637
- received 638
- spam scores 639
- X-CM 646

- X-pstn-2strike 642

- X-pstn-addresses 645

- X-pstn-attach-addresses 646

- X-pstn-disposition 646

- X-pstn-levels 638

- X-pstn-neptune 643

- X-pstn-nxp 646

- X-pstn-nxpr 646

- X-pstn-settings 641

- X-pstnvirus 640

- X-pstn-xfilter 642

- message header tagging 301

- MX records 238

N

- Network Effect Protection 460

- notifications

- configuring 273

- customizing 649

- default templates 654

- disabling and redirecting 280

- editing text 649

- fields for 279

- HTML notifications 653

- my first spam 659

- new spam 661

- overview 273

- suspension 665, 667

- tokens 652

- troubleshooting 290

- virus 321, 663

- welcome new user 654

- wrapping text around tokens 653

O

- Org Down event 425

- organization hierarchy

- account level 61

- administrative authority 70

- authentication method 72

- components 72

- definition 61

- designing 68

- domain assignment 63

- domain examples 65

- domains 69, 70

- email config 62

- email policy 71

- geographically distributed users 70

- organizations 62

- overview 61

- parent/sub-org relationship 62

- user access 71

- when to create an org 68

- organization hierarchy. See also organizations

- organizations

- account settings 259

- add domain 83

- Application Management 257

- Attachment Manager 409

- authorizing administrators 157
 - create a new 91
 - Customer Name 94
 - Default User 96, 114
 - delete 102
 - domains 91
 - download settings 101
 - edit settings 86
 - EZCommand shared secret 95
 - general settings 94
 - hierarchy 81
 - ID 90
 - junk email settings 257
 - list domains 83
 - Message Center subject links 97
 - message header tagging 301
 - Message Limits 93
 - move 100
 - non-account bouncing 96
 - organization ID 94
 - organization summary 90
 - outbound services 88
 - overview 81
 - privileges 201
 - propagation of settings 98
 - searching 92
 - Sender Lists 258
 - Show Deliver-As-Is 258
 - Show Summary 83
 - Spam Disposition 300
 - Spam Filtering 301
 - Support Contact 95
 - troubleshooting 102
 - User Access 252
 - View Hierarchy with Domains 84
 - Virus Settings 258
 - Wireless settings 259
 - org-level sender lists 387
 - outbound message scanning in Content Manager,
 - introduction 331
 - Outbound Servers
 - associating outbound traffic with organizations 517
 - component order of operations 518
 - concepts 508
 - configuration principles 511
 - outbound services 517
 - overview 507
 - overview page 516
 - re injection 509, 510
 - troubleshooting 529
 - undeliverable bounce handling 515
- P**
- passwords
 - Message Center 265
 - overview 50
 - resetting 52
 - user authentication methods 615
 - phishing 304
 - PMP authentication
 - overview 615
 - passwords 616
 - recommended usage 616
 - PMP authentication, resetting passwords 265
 - Policy Enforced TLS
 - alerts 448
 - batch commands 448
 - certification validation 445
 - features and benefits 439
 - inbound mail flow 440
 - outbound mail flow 441
 - prerequisites for setup 439
 - setup 442
 - primary data center 44
 - Privately Managed passwords. See PMP authentication
 - product components 30
 - profanity, blocking with Content Manager 367
- Q**
- Quarantine Summary
 - accessing messages from 283
 - adding logo to 287
 - configuring 284
 - customizing 286
 - delivery time of summary 286
 - frequency of summary 286
 - inbox delivery 286
 - localization 288
 - message text of summary 287
 - overview 282
 - subject links, turning on/off 286
 - viewing a user quarantine 135
- R**
- recommended settings
 - account administrators 170
 - archive administrators 183
 - compliance and security administrators 177
 - email config administrators 188
 - monitor administrators 174
 - organization policy administrators 192
 - user administrators 196
 - regular expressions in Content Manager
 - case sensitivity 355
 - examples 356
 - how to use 349
 - introduction 330
 - multiple expressions in filter 366
 - support limitations 355
 - syntax reference 350
 - test 380
 - related documentation 16
 - Reports
 - Archiving 577
 - Attachment Manager 569
 - Attachments by Account, inbound 571
 - Attachments by Account, outbound 572
 - Attachments by Domain, inbound 569
 - Attachments by Domain, outbound 570
 - Attachments by Filter, inbound 572

- Content by Domain/Account, inbound 572
- Content by Domain/Account, outbound 574
- Content by Filter Name, inbound 575
- Content by Filter Name, outbound 575
- Content Manager 572
- Content Manager Activity Log, inbound 575
- Content Manager Activity Log, outbound 575
- Effective catch rate by org, inbound 563
- Effective catch rate, inbound 562
- How to run 551
- Inbound 553
- Message Archiving by Account, inbound 577, 578
- Message Archiving by Domain, inbound 577, 578
- Message Encryption Activity Log, outbound 577
- Message Encryption by Domain/Account, outbound 576
- Number of registered users 552
- Outbound 553
- Policy-Enforced TLS by Domain/Account, inbound 582
- Policy-Enforced TLS by Domain/Account, outbound 582
- Quarantine Delivery Activity Log, inbound 579
- Spam 560
- Spam by Account, inbound 564
- Spam by Domain, inbound 560
- Spam by Filter Name, inbound 561
- TLS by Domain/Account, inbound 580
- TLS by Domain/Account, outbound 581
- Traffic Activity Log, outbound 559
- Traffic by Account, outbound 559
- Traffic by Domain, inbound 555
- Traffic by Domain, outbound 557
- Traffic by Recipient, inbound 557
- Virus 566
- Virus by Account, inbound 567
- Virus by Account, outbound 568
- Virus by Domain, inbound 566
- Virus by Domain, outbound 567
- Virus by Sender IP, inbound 566
- Virus by Virus Name, inbound 568
- Virus by Virus Name, outbound 569
- resources, support 18
- RFC 2487 445
- routing outgoing mail. See Outbound Servers

S

- searching, Home page 53
- secondary data center 44, 45
- security
 - IP range 498
 - overview 495
 - setting up secure delivery 495
- sender lists
 - approved domains 389
 - approved mailing lists 389
 - approved recipients 388
 - approved senders 388
 - batch commands 395
 - blocked domains 389
 - blocked senders 389
 - filter order 390
 - header information 397
 - industry heuristics and blocked senders 390
 - org level 387
 - organization and user precedence 390
 - quarantine redirect configuration 397
 - size limits 394
 - troubleshooting 397
 - user level 387
 - what to add 396
- signature. See Compliance Footer
- SMTP header tags. See message header fields
- Social Security Numbers policy in Content Manager
 - introduction 330
 - setting up 345
- Social Security Numbers Policy page in Content Manager 381
- Spam Attack 425, 454
- spam filters
 - adjust settings 307
 - and the Approved Senders list 308
 - Approved Mailing Lists 309
 - Distribution lists 307
 - how bulk and category filters work 302
 - Preventing false quarantines 306
 - tuning 303
 - why catch rates vary 297
 - Why spam got through 306
- Spool Manager
 - alerts 487
 - allocating spool 483
 - configuring spool manager 484
 - duration 487
 - how it works 481
 - overview 481
 - settings 484
 - spooling delay 487
 - spooling mechanism 485
 - status 487
 - troubleshooting 488
 - unspooling 486
 - view page 486
- SSO service
 - configure Artifact (Pull Model) 627
 - configure for Account org 625
 - configure for User org 628
 - configure Post (Push Model) 626
 - delete configuration 629
 - edit configuration 628
 - overview 623
 - protect log-in access 624
 - requirements 623
 - test before full deployment 624
- support, technical, receiving 18
- System Tests
 - firewall test 538
 - latency test 539
 - MX record test 534
 - reinjection test 542

- SMTP message test 531
- traceroute test 541

T

- technical support, receiving 18

TLS

- certificates 432
- configuration process 434, 526
- configuring for inbound servers 436
- configuring for outbound servers 522
- testing mail servers 435, 523
- TLS feature for inbound mail 428
- TLS feature for outbound mail 521

- TLS, message header fields 638

- Transport Layer Security. See TLS

troubleshooting

- Attachment Manager 414
- authorization 204
- batch processing 614
- Compliance Footer 530
- Connection Manager 463
- Content Manager 369
- Inbound Servers 427
- mail delivery 531
- Message Center 270
- notifications 290
- organizations 102
- Outbound Servers 529
- sender lists 397
- Spool Manager 488
- user authentication 620
- users 152
- Virus Blocking 322

tuning spam filters

- Approved Senders list 308
- best practices 303
- direct acceptance of messages 322
- enabling protection 307
- overview 293
- virus 323

U

user authentication

- methods 615
- See PMP authentication 615
- See XAuth authentication 616
- troubleshooting 620

- user authentication, administrators 166

user limits

- enable alerts 105
- set maximum number of users 104
- specify alert recipients 105
- view 105
- view current number of users 105

- user notifications. See notifications

- User shortcut 53

- user validation 42

- user-level sender lists 387

users

- adding 120

- alias management 140
- aliases add, remove, view 141
- catchall account 241
- choosing location for 68
- configuring settings 76
- Default User 114
- deleting 123
- downloading settings 150
- List page 108
- mailing and distribution lists 147
- modifying settings 131
- moving 125
- resetting 149
- searching 111
- setting message limit 125
- Settings Summary page 109
- suspending 148
- troubleshooting 152
- user settings 133
- user summary 135
- viewing 107
- viewing a quarantine 135

V

Virus Blocking

- additional zero-hour protection 313
- Advanced Antivirus Heuristics 313
- antivirus definition files 315
- attachment scanning 314
- Authentium virus definitions 311
- configuring for organization 318
- configuring for users 317
- Early Detection Filtering 311
- McAfee virus definitions 311
- notifications 321
- overview 314
- troubleshooting 322
- user access to settings 321
- Virus Outbreak 321

- Virus Outbreak 425, 454

- viruses. See Virus Blocking

X

XAuth authentication

- configuring 617
- implementing using C 619
- implementing using Perl 617
- logging in 620
- overview 616
- recommended usage 617

- X-CM 646

- X-pstn-2strike 642

- X-pstn-addresses 645

- X-pstn-attach-addresses 646

- X-pstn-disposition 646

- X-pstn-levels 638

- X-pstn-neptune 643

- X-pstn-nxp 646

- X-pstn-nxpr 646

- X-pstn-settings 641

X-pstnvirus 640
X-pstn-xfilter 642