Symantec™ Messaging Gateway 10.7 Administration Guide

powered by Brightmail™
Symantec™ Messaging Gateway 10.7 Administration Guide

Documentation version: 1.0

Legal Notice

Copyright © 2019 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com
Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support’s primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html
Chapter 3  Configuring email settings ................................. 77

Configuring email settings ..................................................... 77
Configuring email domains .................................................... 79
  About email domains ......................................................... 80
  Adding or editing domains ................................................. 82
  Importing a domains list .................................................. 85
  Deleting domains ............................................................ 87
  About email domain acceptance settings ......................... 87
  Configuring reverse DNS validation .................................... 88
Configuring email aliases and address masquerades ............... 89
  About aliases and address masquerades ............................ 90
  Adding or editing aliases ............................................... 91
  Importing aliases .......................................................... 92
  Adding or editing address masquerades ............................ 93
  Importing an address masquerade list ............................... 94
  Ignoring text casing in local addresses ............................. 95

Specifying SSL restrictions for TLS communications .................. 96

About invalid recipients ....................................................... 98
  Setting up invalid recipient handling ................................. 99

About email message flow .................................................. 100
  Email message flow phases ............................................. 101

Configuring email for SMTP authentication ............................ 102
  About using SMTP authentication ...................................... 103
  How to set up SMTP authentication ................................... 104
  Configuring SMTP authentication mail settings .................... 106
  Best practices for using SMTP authentication ...................... 110

Specifying address validation criteria .................................... 111
Chapter 9 Detecting viruses, malware, and malicious attacks .......................................................... 204

About detecting viruses, malware, and malicious attacks ......................................................... 204

Product technologies that detect viruses and malicious attacks .............................................. 206

About Disarm ............................................................................................................................. 207

Using Disarm to remove potentially malicious content ........................................................... 208

Potentially malicious content details ...................................................................................... 210

About retrieving Disarmed content ........................................................................................ 213

What you can do with suspicious attachments ....................................................................... 214

Spyware or adware verdict details ............................................................................................ 214

Detecting viruses, malware, and malicious threats ................................................................. 215

Creating email malware policies .............................................................................................. 217

Default email malware policies ............................................................................................... 218

Managing email malware policies ............................................................................................. 222

Modifying email malware policies ........................................................................................... 222

Enabling or disabling email malware policies .......................................................................... 223

Deleting email malware policies ............................................................................................... 224

Copying email malware policies ............................................................................................... 224

Using lists to improve virus scanning performance ................................................................. 224

Excluding file types from virus scanning .................................................................................. 225

Modifying the file types to exclude from scanning .................................................................. 226

Enabling or disabling the lists of file types to exclude from scanning ..................................... 227

Deleting lists of the file types to exclude from scanning .......................................................... 228

Exporting lists of the file types to exclude from scanning ...................................................... 228

Setting limits on nested files ...................................................................................................... 228

Keeping virus definitions current ............................................................................................. 230

About updating virus definitions .............................................................................................. 231

Viewing the status of your virus definitions ............................................................................. 232

Scheduling automatic virus definition updates ........................................................................ 232

Disabling automatic virus definition updates .......................................................................... 233

Initiating virus definition updates on demand .......................................................................... 234

Specifying from where to obtain virus definitions ................................................................... 234

Modifying the artificial intelligence sensitivity level ................................................................. 235
### Chapter 10  Quarantining suspected viruses  .............................................................. 237

- About quarantining suspected viruses ....................................................... 237
- About navigating the Suspect Virus Quarantine ........................................ 238
- Configuring suspect virus message settings ......................................... 239
  - Choosing the language encoding for suspect virus messages .................. 240
  - Specifying the number of suspect virus message entries to view per page ................................................................. 240
  - Specifying how long suspect virus messages are retained in quarantine ................................................................. 241
- Modifying the disk space allotted for Suspect Virus Quarantine .................. 241
- Working with suspect viruses messages .................................................. 242
  - Viewing suspect virus messages in quarantine ........................................ 243
  - Sorting suspect virus messages in quarantine ........................................ 243
  - Deleting suspect virus messages in quarantine ....................................... 243
  - Releasing suspect virus messages from quarantine ............................... 244
- Searching quarantined virus messages ..................................................... 245

### Chapter 11  Filtering spam ................................................................................. 248

- About filtering email spam and unwanted messages .............................. 248
  - Default email spam and unwanted email policies ................................ 250
- Configuring spam and unwanted email detection ...................................... 253
- Scanning text-based attachments ............................................................... 256
- Creating the policies that detect spam and unwanted email .................... 256
- Reducing false positives from unwanted email filtering ......................... 258
- Enabling and disabling spam and unwanted email policies ..................... 259
- Modifying spam and unwanted email policies .......................................... 260
- Copying spam policies .............................................................................. 261
- Deleting spam policies .............................................................................. 262
- Configuring the threshold for suspected spam identification .................... 262
- Enabling or disabling URI reporting to Symantec ................................... 263
- Enabling or disabling URL reputation filtering ....................................... 264
- About submitting messages for customer-specific spam rules .................. 265
  - How rules are created and why messages may not result in custom rules ........................................................................ 267
  - Setting up customer-specific spam submissions .................................... 268
  - Enabling or disabling customer-specific spam submissions ................ 269
  - Provisioning the submitter ID for customer-specific spam submissions ........................................................................ 270
  - Setting the customer-specific spam submission aggressiveness level ........................................................................ 272
Chapter 12 Quarantining spam .......................................................... 280

About quarantining spam ............................................................. 280
Before you use Spam Quarantine .................................................. 281
Quarantining spam sent to unresolved email addresses ............. 282
About navigating Spam Quarantine .............................................. 282
Configuring Spam Quarantine settings ........................................... 283
  Configuring end user quarantine .............................................. 284
  Choosing the language encoding for spam messages ............... 286
  Modifying Spam Quarantine thresholds ................................ 287
  Specifying how long spam messages are retained in quarantine .............................................. 288
  Specifying when and how often Spam Quarantine is expunged .............................................. 289
  Specifying who to notify of false positive messages ............... 290
Viewing messages in the Spam Quarantine ................................. 291
  How Spam Quarantine differs for administrators and users .... 291
  Viewing spam and suspected spam messages in quarantine .... 292
  Viewing spam and suspected spam messages sent to the postmaster mailbox .............................................. 294
Working with messages in the Spam Quarantine ......................... 294
  Specifying the number of entries to appear on the Spam Quarantine Message list page .............................................. 295
  Sorting spam and suspected messages in quarantine by date .............................................. 296
  Searching quarantined spam messages ................................. 296
  Viewing spam message headers ............................................. 298
  Releasing false-positive messages from quarantine ............... 299
  Deleting spam messages in quarantine ................................ 300
  Specifying when to notify users of spam messages in their quarantine .............................................. 301
  Submitting messages from Spam Quarantine for customer-specific rules .............................................. 302
Configuring Spam Quarantine notifications ................................... 302
  About configuring the user and distribution list notification digests .............................................. 303
Chapter 13 Participating in the Symantec Probe Network .......... 313
About the Symantec Probe Network ........................................... 313
About probe accounts ................................................................ 314
About creating probe accounts ...................................................... 315
Setting up probe accounts ............................................................ 316
   Enabling probe participation ................................................... 317
   Creating probe accounts from invalid recipient email addresses ..................................................... 318
   Creating probe accounts manually ........................................... 319
   Enabling probe accounts ....................................................... 320
   Disabling a probe account ...................................................... 320
   Deleting a probe account ....................................................... 321

Chapter 14 Filtering content ...................................................... 322
About content filtering ................................................................. 322
Viewing, editing, adding, and managing your content filtering policies ............................................................................... 323
Creating a content filtering policy .................................................. 325
Defining conditions for a content filtering policy ............................. 327
   Considerations for content filtering policy conditions .................. 328
   Content filtering condition match criteria ................................... 330
   Using regular expressions in content filtering policy conditions .................. 332
Adding actions to a content filtering policy ..................................... 332
   Policy actions and what they do ............................................... 333
   Modifying URLs to protect against threats and unauthorized access ...................................................... 340
Applying content filtering policies to policy groups ..................... 346
Tips for testing a content filtering policy ....................................... 347
Managing how multiple content filtering policies are applied ......... 347
How the Message Audit Log helps to fine-tune and troubleshoot content filtering policies ...................................................... 351
Chapter 15 Filtering content with content filtering resources

About content filtering policy resources 352
Using structured data in a content filtering policy 354
   About your data source files 355
   Creating a record for structured data 358
   Mapping data source file columns to fields in Symantec Messaging Gateway 360
   Uploading data source files 366
   Replicating records 367
   Modifying records 368
   Deleting records 369
About record views 369
   Creating record views 373
   Editing record views 374
   Deleting record views 375
Working with content filtering violation notifications 376
   About policy violation notifications 377
   Creating policy violation notifications 377
   Editing policy violation notifications 379
   Deleting policy violation notifications 380
Working with dictionaries 380
   About content filtering dictionaries 382
   Scanning non-plain text file attachments for content filtering violations 385
   Exporting words or phrases from dictionaries 385
   Disabling and enabling predefined words or phrases in dictionaries 386
   Creating user-defined dictionaries 387
   Importing words or phrases into dictionaries 388
   Editing dictionaries 388
   Deleting user-defined words or phrases from dictionaries 389
   Finding words or phrases in dictionaries 390
   Deleting dictionaries 390
   Premium and custom content filtering dictionaries 391
Using patterns to detect policy violations 395
   About patterns 395
   Creating your own custom patterns 397
   Editing patterns 398
   Deleting patterns 398
Creating and managing annotations for policy violations 399
Using lists to detect prohibited attachments 400
Chapter 16  Working with content filtered incidents .......................... 418

Configuring content incident folders ............................................. 418
About content incident folders ..................................................... 419
About managing the size of content incident folders ....................... 420
Creating content incident folders ................................................. 422
Editing content incident folders .................................................. 425
Deleting content incident folders ............................................... 425
Scheduling the content incident folder Expunger ............................ 426
Configuring message submission options to appear in quarantine
incident folders ........................................................................... 426

Monitoring and acting on incidents .............................................. 427
About monitoring and acting on incidents .................................. 429
Creating incident notifications ..................................................... 430
About remediating incidents from email notifications .................... 432
Viewing incidents in content incident folders ............................... 433
Acting on multiple incidents at a time ........................................ 434
Content incident actions ......................................................... 435
Archiving incidents ............................................................... 436
Monitoring your spam email submissions .................................. 437
Exporting an incident's history .................................................. 440
Forwarding incidents ............................................................. 441
Deleting incidents ................................................................. 442
Submitting messages from quarantine folders for customer-specific
rules ......................................................................................... 443
Remediating quarantined incidents ............................................. 444
Updating an incident's status ..................................................... 445
Changing an incident's severity level ........................................ 446
Viewing an incident's history .................................................... 447
Viewing the text that violated a content filtering policy .................. 447
How the matching text feature is affected by upgrade for existing
content ...................................................................................... 449

Encrypting data with Symantec Content Encryption ....................... 449
Preparing your system for content encryption ............................... 450
Managing host and port information for content encryption ........... 451
Provisioning a content encryption account .................................. 452
Chapter 17  Threat defense scanning with Symantec Content Analysis ................................................................................ 455

About threat defense scanning ...................................................... 455
Preparing Symantec Content Analysis for connection to Symantec Messaging Gateway .............................................................. 456
Connecting Symantec Messaging Gateway to a Content Analysis appliance ............................................................................ 457
Configuring threat defense scan settings ........................................ 458
  Excluding file types from threat defense scanning .......................... 460
Default and sample threat defense policies .......................................................... 460
  Default threat defense policies for Inline mode ............................ 461
  Sample threat defense policies for Monitor mode ........................ 462
  Sample threat defense policies for Secure Preview ..................... 463
Creating new threat defense policy sets ............................................ 465
Selecting threat defense policies for a policy group ........................... 467
Viewing the Content Analysis queue ............................................... 468

Chapter 18  Leveraging Symantec Network Prevent ................................ 469

About integrating Symantec Data Loss Prevention with Symantec Messaging Gateway .............................................................. 470
Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway ................................................ 471
About Data Loss Prevention Network Prevent ................................... 474
Required ports for Data Loss Prevention Network Prevent integration ........................................................................... 475
How Symantec Messaging Gateway and Data Loss Prevention Network Prevent interact .......................................................... 476
Common Data Loss Prevention Network Prevent actions ................. 477
Supported Data Loss Prevention Network Prevent delivery modes ............................................................................. 478
About failure behavior with Data Loss Prevention Network Prevent ......................................................................................... 478
How to resolve a delivery queue back up to Symantec Network Prevent ....................................................................................... 479
Enabling or disabling bypass for Data Loss Prevention Network Prevent ....................................................................................... 481
How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled .................................................... 482
About Data Loss Prevention Network Prevent reports .................... 483
Chapter 22 Monitoring Symantec Messaging Gateway's status

- About monitoring system status ......................................................................... 602
- Using the Dashboard .......................................................................................... 603
  Threat category components .............................................................................. 605
- Monitoring host computers and service status ............................................. 607
  Viewing information about your hardware .................................................. 608
  Viewing the status of your hardware .......................................................... 609
  Viewing the status of your software and services .................................. 609
- Software and services status definitions ......................................................... 610
- Monitoring log data .......................................................................................... 612
  About logs ........................................................................................................ 614
  Log types .......................................................................................................... 615
  Viewing log files ............................................................................................... 617
  Viewing the Control Center error log .......................................................... 618
  Saving log files ................................................................................................. 619
  Managing the log database size ..................................................................... 620
  Configuring log levels .................................................................................... 622
  Manually deleting log files ............................................................................. 624
  About log disk space alerts ............................................................................. 625
  Clear disk space checklist ............................................................................. 625
- Monitoring logs on a remote server ............................................................... 627
  Configuring remote logging to syslog ......................................................... 628
  Standard prefix for Scanner logs sent to remote syslog ..................................... 629
  Log format of boot.log, cron, message, and secure components for remote syslog .................................................. 630
  Log format of Conduit, Brightmail Client, Brightmail Engine, and JLU Controller for remote syslog .................................................. 630
  Log format of mail transfer agent logs for remote syslog .................................. 632
  Log format of message audit logs for remote syslog ...................................... 633
- Working with the message audit log and message queue .................................. 634
  Enabling the Message Audit Log .................................................................. 636
  Searching for a message in the Message Audit Log ..................................... 637
  Exporting Message Audit Log data .............................................................. 641
  About message queues .................................................................................... 642
  Viewing queued messages ............................................................................. 643
  Rerouting messages in the delivery queue ................................................... 643
  Deleting queued messages ............................................................................ 644
  Stopping the mail flow .................................................................................... 645
  Flushing message queues .............................................................................. 646
  Monitoring message queue size and volume ............................................... 647
  Troubleshooting the message queue ............................................................ 647
Chapter 23  Administering your product through the Control Center .......................................................... 652

Managing administrators .......................................................................................................................... 652
  About adding and authorizing administrators using LDAP sources ................................................. 653
  About default administration policies ................................................................................................. 656
  About administrator and end user views ............................................................................................. 658
  Setting up local and LDAP administrator accounts ........................................................................... 658
  Editing an administrator ......................................................................................................................... 667
  Deleting an administrator ....................................................................................................................... 668

Configuring the Control Center ........................................................................................................... 668
  Configuring Control Center settings .................................................................................................... 670
  About simultaneous Control Center access ......................................................................................... 671
  About specifying host names for Control Center access ....................................................................... 672
  Specifying which hosts can access the Control Center ....................................................................... 672
  Configuring SNMP settings to monitor network devices ...................................................................... 673
  Configuring the Control Center listener port ....................................................................................... 675
  Bypassing the security warning when you access the Control Center .................................................. 675
  Designating a Control Center certificate ............................................................................................. 676
  Setting the locale encoding and fallback encoding .............................................................................. 676
  Converting 8-bit MIME messages to 7-bit MIME .................................................................................. 677
  Customizing the date format and time format ......................................................................................... 677

Customizing user preferences in the Control Center ........................................................................... 679
  Specifying a custom user Login help page ............................................................................................ 680
  Enabling users to bypass Control Center login credentials ................................................................... 681
  Configuring the replication of end user preference data ....................................................................... 682
  Setting up your SMTP greetings and postmaster address .................................................................... 683

Setting up alerts ...................................................................................................................................... 683
  Types of alerts ....................................................................................................................................... 684
  Configuring alerts ................................................................................................................................. 688
  Setting scheduled task failure alerts ..................................................................................................... 693
  Configuring Control Center SMTP settings for alerts and reports ....................................................... 694

Managing passwords ............................................................................................................................... 695
  Resetting an administrator password ................................................................................................... 696
  Enforcing strong passwords .................................................................................................................. 696
  Password best practices .......................................................................................................................... 697
Appendix A  Command line reference .................................................. 735
agent-config ................................................................. 737
cat ................................................................................. 739
cc-config ......................................................................... 740
clear ............................................................................... 743
db-backup ....................................................................... 744
db-restore ....................................................................... 749
delete .............................................................................. 752
diagnostics ..................................................................... 757
dns-control ...................................................................... 762
fipsmode ......................................................................... 764
grep ............................................................................... 765
help ............................................................................... 766
ifconfig .......................................................................... 773
iostat ............................................................................ 774
ip .................................................................................... 775
ldapsearch ....................................................................... 776
list ................................................................................. 777
mallog ............................................................................ 779
malquery ......................................................................... 781
monitor ........................................................................... 787
more ............................................................................... 793
mta-control ..................................................................... 794
netstat ........................................................................... 800
nslookup ......................................................................... 801
password ......................................................................... 802
patch ............................................................................. 803
ping ............................................................................... 805
ping6 ............................................................................ 806
reboot ............................................................................ 807
route ............................................................................... 808
rpmdb ............................................................................ 809
rsa-key ........................................................................... 810
service ........................................................................... 811
show ............................................................................. 814
shutdown ......................................................................... 815
sshd-config ..................................................................... 816
symdiag .......................................................................... 819
tail ............................................................................... 821
telnet ............................................................................. 824
traceroute ....................................................................... 825
traceroute6 ....................................................................... 826
## Appendix B  Message filtering options

- Action combinations from multiple verdicts .............................................................. 830
- Verdicts by verdict category ..................................................................................... 836
- Verdict combinations ............................................................................................... 840
- Positive and negative content filtering rule condition examples ............................. 842

## Appendix C  Content filtering templates

- Caldicott Report policy template ............................................................................. 848
- Canadian Social Insurance Number policy template ................................................. 849
- Competitor Communications policy template .......................................................... 849
- Confidential Documents policy template ................................................................. 849
- Credit Card Numbers policy template ..................................................................... 850
- Customer Data Protection policy template .............................................................. 850
- Data Protection Act 1998 policy template ............................................................... 851
- Defense Message System (DMS) GENSER Classification policy template .......... 852
- Design Documents policy template ......................................................................... 853
- Employee Data Protection policy template ............................................................. 853
- Encrypted Data policy template .............................................................................. 854
- EU Data Protection Directives policy template ....................................................... 854
- Export Administration Regulations (EAR) policy template ..................................... 855
- Financial Information policy template ...................................................................... 855
- Gambling policy template ......................................................................................... 856
- Gramm-Leach-Bliley policy template ....................................................................... 856
- HIPAA policy template ............................................................................................ 857
- Human Rights Act 1998 policy template .................................................................. 858
- Illegal Drugs policy template .................................................................................... 858
- Individual Taxpayer Identification Numbers (ITIN) policy template ...................... 859
- International Traffic in Arms Regulations (ITAR) policy template ......................... 859
- Media Files policy template ..................................................................................... 859
- Mergers and Acquisition Data policy template ....................................................... 860
- NASD Rule 2711 and NYSE Rules 351 and 472 policy template ............................. 860
- NASD Rule 3010 and NYSE Rule 342 policy template ............................................. 860
- NERC Security Guidelines for Electric Utilities policy template .............................. 861
- Network Diagrams policy template .......................................................................... 861
- Network Security policy template ............................................................................ 861
- Offensive Language policy template ....................................................................... 862
- Office of Foreign Assets Control (OFAC) policy template ....................................... 862
- Password Files policy template .............................................................................. 863
- Payment Card Industry Data Security Standard policy template ........................... 863
Appendix D Using the Dell Remote Access Controller .......................... 872
About the Dell Remote Access Controller (DRAC) card .................... 872
Restarting the Symantec Messaging Gateway appliance with DRAC
forcefully .................................................................................. 874
Restarting the Symantec Messaging Gateway appliance from DRAC
gracefully .............................................................................. 874
Installing and configuring Symantec Messaging Gateway appliance
with DRAC remotely ................................................................ 875
Installing Symantec Messaging Gateway image with DRAC from virtual
media ...................................................................................... 876
Viewing Dell server diagnostics with DRAC .................................. 877
Deleting logs, configuration information, and data of Symantec
Messaging Gateway appliance with DRAC ................................. 877
Restoring Symantec Messaging Gateway appliance to the original
factory configuration with DRAC .............................................. 878
Introducing Symantec Messaging Gateway

This chapter includes the following topics:

■ About Symantec Messaging Gateway
■ Symantec Messaging Gateway features
■ How Symantec Messaging Gateway works
■ About default policies and features
■ Where to get more information

About Symantec Messaging Gateway

Symantec Messaging Gateway delivers inbound and outbound messaging security, real-time antispam and antivirus protection, advanced content filtering, threat detection and sandboxing, and data loss prevention to your enterprise.

Symantec Messaging Gateway does the following to protect your environment:

■ Detects spam, denial-of-service attacks, and other inbound email threats.
■ Provides outbound sender throttling to protect against outbound spam attacks from compromised internal users.
■ Leverages a global sender reputation and local sender reputation analysis, including expanded URL reputation-based filtering, to block spam, malware and phishing message and to reduce email infrastructure costs by restricting unwanted connections.
■ Filters email by policies to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email.
Symantec Messaging Gateway features

Symantec Messaging Gateway delivers inbound and outbound messaging security, real-time antispam and antivirus protection, advanced content filtering, threat detection and sandboxing, and data loss prevention to your enterprise. In the Symantec Messaging Gateway Control Center, you can customize features to suit the requirements of your company and your users.

- Block unwanted email at the gateway
  Symantec Messaging Gateway provides several features that let you block email from entering your network. When you block unwanted email, you reduce your risk of getting a virus. You also reduce the resources that are needed to scan messages.
  See “About blocking and allowing messages at connection time” on page 141.

- Manage users through policy groups
  You can specify these groups of users according to email addresses, domain names, or LDAP groups. Then you can apply filtering policies to specific policy groups. Symantec Messaging Gateway installs with a Default policy group that consists of all of the users.
Symantec Messaging Gateway can detect spam, suspected spam, and unwanted email with a high level of accuracy. You can define and manage policies to process spam and unwanted email, and set thresholds for suspected spam. You can even allow messages from specified domains to bypass antispam scanning altogether.

You can also store spam messages in Spam Quarantine until they can be reviewed. If you configure user access to Spam Quarantine, recipients receive notifications of quarantined messages and can take appropriate actions.

To help improve the effectiveness of spam filtering, you can choose to participate in Symantec’s probe network.

Enable DMARC, DKIM, SPF, and Sender ID authentication to detect messages that have forged email addresses or forged header information.

Detect malware and other malicious attacks
You can create policies and configure settings to detect malware and other malicious attacks.

Send email to a Symantec Content Analysis server to detect advanced threats.

Filter messages to enforce content policies
You can create the policies that filter inbound and outbound email message content. Such policies can be used to monitor and enforce compliance with corporate and regulatory requirements and to prevent data loss.

Enforce TLS encryption on inbound messages, to allow more secure communication with trusted partners and senders.

Modify URLs in incoming messages to send requests to Symantec Threat Isolation or ProxySG when recipients click the links.

Monitor performance
The Control Center contains a Dashboard that displays the overall system status. It provides statistics about the types of threats that inbound and outbound messages pose to your system. Statistics include data about the messages that are addressed to invalid recipients.
or that come from the addresses that have bad reputations. They also include the number of messages that have triggered virus, spam, and content filtering policies.

See “About monitoring system status” on page 602.

Symantec Messaging Gateway includes over 50 reports that provide statistics on content filtering, email messages, IP connections, spam, and viruses from all Scanners. You can create reports when you need them or configure them to be emailed daily, weekly, or monthly.

■ Keep your malware definitions current
   You can use LiveUpdate to automatically update your protection. When LiveUpdate runs, it downloads and installs any available definitions.
   See “About updating virus definitions” on page 231.

■ Configure Symantec Messaging Gateway to automatically send alerts and notifications about outbreaks, system issues, and policy violations.
   See “Types of alerts” on page 684.

■ Monitor devices, configure and manage Scanners, and manage software updates
   See “Configuring SNMP settings to monitor network devices” on page 673.
   See “About Scanner email settings” on page 43.
   See “Downloading and installing a software update” on page 721.

■ Configure Symantec Messaging Gateway from the command line.
   Each appliance has a set of commands you can use to configure, optimize, and administer your system. Access these commands by logging into the system either through SSH or by the VGA or serial connections on the appliance.

**How Symantec Messaging Gateway works**

Figure 1-1 shows how Symantec Messaging Gateway processes an email message. This diagram assumes that the message passes through the Brightmail Filtering Module to the Mail Transformation Engine without being rejected.
Figure 1-1  Symantec Messaging Gateway Architecture

The path an email message takes is as follows:

1. At the gateway, global reputation determines if the sending IP is a Good Sender or a Bad Sender. It accepts or rejects the connection based on the distinction.

2. Connection Classification classifies the sending IP into one of 10 classes based on local reputation. It either accepts or defers the connection based on class membership.

3. Before the MTA accepts the message, it checks the domain address and email address. The MTA determines if it belongs to the Local Good Sender Domains or Local Bad Sender Domains group. If it does, it applies the configured action to the message. If appropriate, the MTA moves the message to its inbound queue.

4. The Brightmail Filtering Module consults the directory data service to expand the message’s distribution list and determines policy group membership.

5. The Brightmail Filtering Module determines each recipient’s filtering policies.

6. Antivirus filters determine whether the message is infected.

7. Spam filters determine whether the message is spam or suspected spam.
8. Unwanted mail filters (including marketing newsletters, redirect URLs, and customer-specific spam) determine whether the message is unwanted.

9. Content filtering policy filters scan the message and attachments for restricted content.

10. Threat Defense policies send messages to Symantec Content Analysis, which scans the messages for advanced threats, if the two systems are integrated.

11. The Mail Transformation Engine performs actions according to filtering results and configurable policies and applies them to each recipient's message based on policy group membership.

12. Messages may be held in quarantine for review based on policy configuration. Messages in content incident folders can be remediated through the console or through the Enforce Server.

13. Messages are then inserted into the delivery queue for delivery by the MTA.

---

**Note:** Symantec Messaging Gateway does not filter any messages that do not flow through the SMTP gateway. For example, it does not filter the messages that are sent between mailboxes on the same Microsoft Exchange Server or within an Exchange organization. See “About email message flow” on page 100.

---

### About default policies and features

As soon as you install Symantec Messaging Gateway, the system is ready to use. A set of policies and a group of features are enabled for your default policy group.

A policy group is a group of users to whom you assign filtering policies. Symantec Messaging Gateway installs with only the default policy group, which includes all users. One default policy for each spam, malware, or threat defense verdict is assigned to the default group. Additional sample policies for spam, malware, and threat defense are provided for your use. These additional policies are not assigned to any group.

Symantec Messaging Gateway does not provide default content filtering policies. You can use predefined templates to create content filtering policies.

You can create additional policy groups and choose a set of policies for each group from the Administration > Users > Policy Groups page. You create additional filtering policies from the Spam, Malware, Threat Defense, Content, and Administration menus. You cannot delete the default policy group or any of the default policies.

See “Default email spam and unwanted email policies” on page 250.

See "Default email malware policies" on page 218.

See “Default and sample threat defense policies” on page 460.
The following features are enabled by default:

- Connection Classification
- Good and bad sender groups
- Filtering email messages for spam, viruses, and other threats
- Suspected spam
- Hold messages in Suspect Virus Quarantine
- Message audit logging
- A selection of alerts

The following features are not enabled by default upon installation:

- Spam Quarantine
- LDAP directories
- Fastpass
- Directory harvest attack protection
- Email virus attack prevention
- Bounce Attack Prevention
- Sender authentication, including SPF, Sender ID, DKIM
- SMTP authentication
- TLS encryption
- Content filtering
- Threat Defense filtering
- Invalid recipient handling
- Probe accounts
- Data gathering for all report types
- All alert types

Where to get more information

The following resources provide more information about your product.

Documentation

The Symantec Messaging Gateway documentation set consists of the following manuals:
Symantec™ Messaging Gateway 10.6.3 Administration Guide
Symantec™ Messaging Gateway 10.6 Installation Guide
Symantec™ Messaging Gateway 10.6 Getting Started Guide
Symantec™ Messaging Gateway 10.6.3 Command Line Reference Guide
Symantec™ Messaging Gateway 10.6.3 Release Notes
Symantec™ Messaging Gateway 10.6.3 Software Update Notes

For the most current English versions of Symantec Messaging Gateway documents, click the following URL and then click More Articles under the Documentation heading:

The site provides best practices, troubleshooting information, and other resources for Symantec Messaging Gateway.

Product Help system
Symantec Messaging Gateway includes a comprehensive Help system that contains conceptual and procedural information.

Symantec Web site
Visit the Symantec Web site for more information about your product as follows:

  Provides access to the technical support knowledge base, newsgroups, contact information, downloads, and mailing list subscriptions

- https://licensing.symantec.com/acctmgmt/index.jsp
  Provides information about registration, frequently asked questions, how to respond to error messages, and how to contact Symantec License Administration

- www.symantec.com/business/index.jsp
  Provides product news and updates

- www.symantec.com/business/security_response/index.jsp
  Provides you access to the virus encyclopedia, which contains information about all known threats; information about hoaxes; and access to white papers about threats
Deploying Scanners

This chapter includes the following topics:

- About Scanners
- Setting up Scanners
- Adding Scanners
- Verifying or changing Scanner installation settings
- Configuring Scanner email settings
- Configuring SMTP advanced settings
- Specifying internal mail hosts for non-gateway deployments
- Modifying Scanner configurations
- Enabling and disabling Scanners
- Stopping and starting Scanners
- Deleting Scanners
- Changing the IP address of the Control Center host
- Managing services and MTA operations

About Scanners

Scanners process inbound and outbound messages and route messages for delivery. Scanners download virus definitions, spam signatures, and other security updates from Symantec Security Response. Scanners run filters, render verdicts, and apply actions to messages in accordance with the appropriate policies and settings. You can configure Scanners to limit the number of connections, which can help reduce the number of messages to be scanned.
You can do any of the following tasks to administer your Scanners:

- Add a Scanner.
  See “Adding Scanners” on page 35.

- Modify a Scanner.
  See “Modifying Scanner configurations” on page 67.

- Enable and disable a Scanner.
  See “Enabling and disabling Scanners” on page 68.

- Stop and start a Scanner.
  See “Stopping and starting Scanners” on page 68.

- Delete a Scanner.
  See “Deleting Scanners” on page 70.

You must have Full Administration rights or Manage Settings view rights to create, modify, enable, disable, or delete Scanners.

---

### About IPv6 address in Symantec Messaging Gateway

Symantec Messaging Gateway lets any host in a deployment be provisioned with IPv6 addresses. You must first configure your Scanners with at least one primary IPv4 address that Symantec Messaging Gateway can use for communication between the Control Center and Scanner. You configure this primary IPv4 address when you initially install the appliance. Once the initial setup is complete and a Scanner, Control Center, or both have been configured, you can implement IPv6 addresses as needed.

For more information, see the *Symantec Messaging Gateway Installation Guide*.

The following list provides the instances in which you can use IPv6 addresses:

- Enable IPv6 for your Scanners and Control Center and add IPv6 addresses to one or both of your Ethernet interfaces.
  See “Configuring IPv6 Ethernet settings and routes” on page 40.

- Add IPv6 addresses and address ranges for access to your Control Center.
  See “About specifying host names for Control Center access” on page 672.

- If you enable IPv6 for your Ethernet interfaces, you can add IPv6 addresses to your SMTP configuration.
  See “Configuring Scanner email settings” on page 42.

- If you enable IPv6 for your Ethernet interfaces, you can use IPv6 addresses and address ranges for Internal Mail Hosts.
  See “Specifying internal mail hosts for non-gateway deployments” on page 65.

- Use IPv6 addresses in your Good Senders lists and Bad Senders lists.
  See “Supported methods for identifying senders” on page 136.
- Query IPv6 addresses when you perform reputation lookups. See “Researching IP address reputation” on page 163.
- Create reports to return information on IPv6 addresses or a mix of IPv4 and IPv6 addresses. See “Create, save, email, and print a report” on page 578.
- View message audit logs for your IPv6 addresses. See “Searching for a message in the Message Audit Log” on page 637.

IPv6 is not supported for the following features:
- Connection Classification and Fastpass ignore IPv6 addresses and process IPv4 addresses.
- Reputation checking does not conduct DNS-based IP reputation checks for IPv6 addresses.
- SMTP delivery for IPv6 addresses is not supported.
- SMTP authentication forwarding to an IPv6 authentication host is not supported.
- LDAP, SNMP, DHA, NTP, and virus attack functionality does not currently use IPv6 addresses.

## Setting up Scanners

### Table 2-1 Processes for configuring Scanners

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Verify Scanner configurations.</td>
<td>After installing the Scanner software, review your configurations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Specifying DNS server addresses” on page 36.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Verifying or changing the time settings on a host” on page 37.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Specifying proxy settings” on page 38.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring IPv4 Ethernet settings and routes” on page 39.</td>
</tr>
<tr>
<td>Phase 2</td>
<td>Configure Scanner email acceptance and delivery settings.</td>
<td>Configure scanner email settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring mail flow direction” on page 45.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Scanner inbound email delivery settings” on page 48.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring Scanner outbound mail delivery settings” on page 52.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About Scanner email settings” on page 43.</td>
</tr>
</tbody>
</table>
Table 2-1  Processes for configuring Scanners  (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 4</td>
<td>Configure internal mail hosts for non-gateway deployment.</td>
<td>See “Specifying internal mail hosts for non-gateway deployments” on page 65. See “Internal mail servers: non-gateway deployments” on page 66.</td>
</tr>
</tbody>
</table>

Adding Scanners

You must have full administration rights or manage settings modify rights to add a Scanner. After you add a Scanner, you can check its status to ensure that it functions properly.

Note: If you have provisioned content encryption for your messaging system and then add or change the IP address of a Scanner, you must inform your Symantec provisioning representative. For more information, see the Symantec Content Encryption Provisioning page by clicking Content > Settings > Content Encryption and then clicking Click here.

To add a Scanner

1. In the Control Center, click Administration > Hosts > Configuration.
2. Click Add.
3. Complete the Add Scanner Wizard.
   Refer to the Symantec Messaging Gateway Installation Guide for information about completing the Add Scanner Wizard.

Verifying or changing Scanner installation settings

Table 2-2 describes the Scanner installation settings that you can verify or change, and the additional settings that you can customize after installation. You can perform any of these tasks as needed in any order.
### Table 2-2  Scanner verification installation settings

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a DNS server address.</td>
<td>You specify the IP addresses of the DNS servers that a Scanner uses, and you can change the IP addresses after installation. See “Specifying DNS server addresses” on page 36.</td>
</tr>
<tr>
<td>Verify the time settings.</td>
<td>You can specify primary, secondary, and tertiary Network Time Protocol (NTP) time servers or you can manually specify the time. See “Verifying or changing the time settings on a host” on page 37.</td>
</tr>
<tr>
<td>Specify proxy settings.</td>
<td>If you use a proxy host, you must add the proxy server information to your Scanner definition. See “Specifying proxy settings” on page 38.</td>
</tr>
<tr>
<td>Configure Ethernet settings and routes.</td>
<td>You can customize a Scanner’s Ethernet settings to accommodate your site’s mail-flow requirements. See “Configuring IPv4 Ethernet settings and routes” on page 39.</td>
</tr>
</tbody>
</table>

### Specifying DNS server addresses

Domain Name System (DNS) servers translate domain names into IP addresses. You specify the IP addresses of the DNS servers that a Scanner uses during installation, and you can change the IP addresses after installation. If your Scanner hosts email scanning, the DNS servers that you specify are used for email delivery.

**Note:** For DNS servers to function properly, firewall port 53 must be open.

You must have Full Administration rights or Manage Settings modify rights to add or modify DNS server settings.

**To specify DNS server addresses**

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. Click the name of the host whose DNS definitions you want to modify.
3. On the **Edit Host Configuration** page, click the **DNS/Time** tab.
4 Do one of the following tasks:

Click **Use internal DNS server**.

If you need to override the default DNS query port of 53, type the new port number in the **Query source port** field.

Click **Use the following external DNS servers** and type the IP address of each DNS server.

You can specify up to three external DNS servers.

Initially, all servers that you specify have the same precedence. Symantec Messaging Gateway queries the DNS servers in the list, notes the round trip time (RTT) for each server and begins to favor the DNS server with the lowest RTT value. If that server becomes slow or unresponsive, DNS queries are routed to the next server on the list that has the lowest RTT, and so forth. The result is that the primary DNS server is the one that currently has the best RTT performance.

Symantec Messaging Gateway only supports IPv4 addresses for DNS servers. However, it does support AAAA records and IPv6 reverse DNS records for these IPv4 DNS servers.

When necessary, you can also flush buffers for DNS servers or routers.

5 Check **Apply above settings to all hosts** to apply your changes to all hosts.

6 Click **Save**.

See “About Scanners” on page 32.

### Verifying or changing the time settings on a host

You can specify up to five Network Time Protocol (NTP) time servers for a Symantec Messaging Gateway host. Symantec strongly recommends that you use NTP time servers to manage the time settings on your hosts. You also have the option to set the time manually.

You must have Full Administration rights or Manage Settings modify rights to configure time settings.

**To configure time settings**

1 In the Control Center, click **Administration > Hosts > Configuration**.

2 Select the name of the host whose time settings you want to modify and click **Edit**.

3 On the **Edit Host Configuration** page, click the **DNS/Time** tab.

4 Select the time zone of the host to which you want to synchronize the time.

5 Type the NTP host names or IP addresses.

You can specify up to five NTP servers, or you can set the time manually.

6 Optional: click **Apply above settings to all hosts** to apply your changes to all hosts.
7  Click **Save**.
8  Restart the computer for the time changes to take effect.

**Specifying proxy settings**

The Conduit service runs on each Scanner. Through the Conduit, you can register your licenses, update antispam filters, download new virus definitions, and perform software updates. If you use a proxy host, you must add the proxy server information to your Scanner definition.

Proxy errors are logged to BrightmailLog.log at the warning log level. Before you configure proxy access, you may want to configure BrightmailLog.log to log warning-level errors with the command `cc-config cclog --level warnings`. If the proxy host does not function after you configure it, check BrightmailLog.log for errors.

Table 2-3.

See **cc-config** on page 740.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Error in BrightmailLog.log</th>
</tr>
</thead>
<tbody>
<tr>
<td>The proxy host requires a user name and password,</td>
<td>IOException: Server returned HTTP response code: 407 for URL:</td>
</tr>
<tr>
<td>but none was specified.</td>
<td></td>
</tr>
<tr>
<td>The wrong user name or password was specified for the proxy</td>
<td>ProtocolException: Server redirected too many times</td>
</tr>
<tr>
<td>host.</td>
<td></td>
</tr>
<tr>
<td>The wrong address and port were specified for the proxy host.</td>
<td>Various timeout errors can occur</td>
</tr>
</tbody>
</table>

**Note:** LiveUpdate uses the proxy that you define for the Scanner to download virus definitions from Symantec. If you download virus definitions from a LAN host, LiveUpdate uses a proxy only if you have defined one.

See "**Specifying from where to obtain virus definitions**" on page 234.

To specify proxy settings

1  In the Control Center, click **Administration > Hosts > Configuration**.
2  Under **Hostname**, check the name of the Scanner for which you want to specify a proxy and click **Edit**.
3  On the **Edit Host Configuration** page, click the **Proxy** tab.
4  Check **Use proxy server**.
5  In the **Proxy host name** field, type the proxy host name.
In the Proxy host port field, type the proxy port number.

Specify a user name and password if they are required to log on to the proxy host.

Click Save.

Configuring IPv4 Ethernet settings and routes

A Scanner's Ethernet settings for IPv4 addresses can be customized to accommodate your site's mail-flow requirements as follows:

- Configure a Scanner's Ethernet settings and, optionally, enable an Ethernet interface to use up to 50 static routes.
  Static routes direct data from one subnet to a different subnet faster than dynamic routes. Static routes must be updated if addresses change.

- Add or delete virtual addresses to an Ethernet interface as needed.

- Change the IP address of a Scanner.

You must have Full Administration rights or Manage Settings modify rights to modify Ethernet settings.

To configure Ethernet settings for IPv4 addresses

1. In the Control Center, click Administration > Hosts > Configuration.

2. Under Hostname, check the Scanner whose Ethernet settings you want to modify and click Edit.

3. On the Edit Host Configuration page, click the Ethernet tab then click the IPv4 tab.

4. Edit the Ethernet interfaces as needed by entering an IP, netmask, broadcast, and network address for each Ethernet interface.

   Change the Scanner or Control Center IP address if needed. You can change the IP address of a Scanner or the Control Center. If you change the IP address of the Control Center, subsequently log into each Scanner's command-line interface. Use the agent-config command to re-allow the secured connection to the Scanner from the new Control Center IP.

5. Check Enable this interface to activate a second Ethernet interface.

   You can dedicate a second Ethernet interface to handling inbound or outbound traffic only.

6. Add or delete virtual IP addresses to an Ethernet interface as needed.

7. Under Routing, in the Default gateway field, type the IP address of a default gateway.

   A default gateway is required. You must indicate it with an IP address.

8. To optionally define a static route, under Static Routes, specify the following:
■ Destination address—IP address, IP address with subnet mask (for example, 128.113.1.0/255.255.255.0), or CIDR notation (for example, 192.30.250.0/18)
■ Gateway address—IP address
■ Interface—Default, Ethernet 1, or Ethernet 2

9 Click Add to add a static route.
You can add up to 50 static routes per Ethernet interface.

10 Click Save.
You can apply advanced connection settings across all addresses.
See “Configuring advanced Ethernet settings” on page 41.
You can also configure IPv6 addresses for your Ethernet settings.
See “Configuring IPv6 Ethernet settings and routes” on page 40.

Configuring IPv6 Ethernet settings and routes
You can customize Scanner and Control Center Ethernet settings to accommodate your configuration needs as follows:

■ Configure a Scanner's Ethernet settings and, optionally, enable an Ethernet interface to use up to 50 static routes.
  Static routes direct data from one subnet to a different subnet faster than dynamic routes.
  Static routes must be updated if addresses change.
■ Change the IPv4 address of a Scanner or create an IPv6 address.
You must have Full Administration rights or Manage Settings modify rights to modify Ethernet settings. You can assign one or more IPv6 addresses to an Ethernet interface.

To configure IPv6 Ethernet settings and routes

1 In the Control Center, click Administration > Hosts > Configuration.

2 Under Hostname, check the Scanner whose Ethernet settings you want to modify and click Edit.

3 On the Edit Host Configuration page, click the Ethernet tab, then click the IPv6 tab.

4 Check Enable IPv6 to enable IPv6 for the host.
When you enable IPv6, you must configure at least one IPv6 address and the IPv6 default gateway.
5 Edit the Ethernet interfaces as needed by providing an IP address and prefix for each Ethernet interface.

You can specify individual IPv6 addresses in any standard IPv6 format. Addresses are stored and displayed in shortened format. Ranges are expressed in CIDR notation as a combination of an address part and a prefix.

6 Provide a **Prefix** for the IP address for one or both interfaces.

For IPv6 addresses, the prefix value is restricted to an integer value of 64 or lower.

7 Under **Routing**, in the **Default gateway** field, type the IP address of a default gateway.

A default gateway is required. You must indicate it with an IP address in any accepted IPv6 format.

8 To optionally define a static route, under **Static Routes**, specify the following:

   - **Destination Address**: You can use standard IPv6 format for a single host, CIDR notation for a range, or subnet mask.
   - **Gateway address**: IPv6 address.
   - **Interface**: Default, Ethernet 1, or Ethernet 2.

9 Click **Add** to add a static route.

   You can add up to 50 static routes per Ethernet interface.

10 Click **Save**.

   You can apply advanced connection settings across all addresses.

   See “Configuring advanced Ethernet settings” on page 41.

## Configuring advanced Ethernet settings

Use the following procedure to apply advanced connection information across all configured IPv4 and IPv6 Ethernet settings and routes.

### To configure advanced Ethernet settings

1 In the Control Center, click **Administration > Hosts > Configuration**.

2 Click the **Advanced** tab to configure the settings for your new Ethernet interfaces.

3 For each Ethernet interface, check **Auto Negotiation** or select a speed for the connection and specify half or full duplex operation of the connection.

4 Check **Segmentation** if you want to offload TCP segmentation from the gateway CPU to the Ethernet card.

   See “Configuring IPv4 Ethernet settings and routes” on page 39.
Configuring Scanner email settings

Table 2-4 describes the tasks that you can perform to configure and modify Scanner inbound email settings and outbound email settings. You can perform any of these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that you understand about Scanner email settings before you perform any tasks.</td>
<td>Scanner email settings let you control various aspects of inbound and outbound message flow. You can limit the IP addresses from which Symantec Messaging Gateway accepts email messages. You can also control where Symantec Messaging Gateway delivers filtered email. You can reduce the volume of email that any one Scanner filters by configuring separate inbound and outbound Scanners. Even if you use only one Scanner to filter both inbound email and outbound email, you can configure various SMTP settings to control message flow. See “About Scanner email settings” on page 43.</td>
</tr>
<tr>
<td>Specify the mail flow direction.</td>
<td>You can specify whether you want a Scanners to filter inbound email, outbound email, or both. See “Configuring mail flow direction” on page 45.</td>
</tr>
<tr>
<td>Modify the inbound mail settings.</td>
<td>You can change the IP address or port number or add an IPv6 address through which a Scanner accepts inbound mail connections. You can also designate whether or not the Scanner accepts inbound TLS-encrypted connections. See “Changing Scanner inbound mail settings” on page 46.</td>
</tr>
<tr>
<td>Modify the inbound mail acceptance settings.</td>
<td>You can conserve Scanner resources by limiting inbound connections to only IPv4 addresses or IPv6 addresses from which you want the Scanner to filter email. By allowing connections from only certain IP addresses and domains, you exclude all other inbound clients from sending messages at connection time. See “Changing Scanner inbound mail acceptance settings” on page 47.</td>
</tr>
<tr>
<td>Modify the inbound email delivery settings.</td>
<td>After a Scanner filters inbound email, the MTA relays filtered email to a mail server for delivery to recipients. When you configure email delivery for an inbound-only or combined inbound and outbound Scanner, you designate the default local and non-local hosts where filtered inbound mail is routed. See “Configuring Scanner inbound email delivery settings” on page 48.</td>
</tr>
</tbody>
</table>
Table 2-4 Scanner email settings (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify the outbound mail settings.</td>
<td>You can change the IP address or port number or add an IPv6 address where a Scanner accepts outbound mail connections. You can also designate whether or not the Scanner accepts outbound TLS-encrypted connections.</td>
</tr>
<tr>
<td></td>
<td>See “Changing Scanner outbound mail settings” on page 50.</td>
</tr>
<tr>
<td>Modify the outbound mail acceptance settings.</td>
<td>You can configure a Scanner to accept outbound connections from an unlimited number of mail servers. By allowing connections from only certain IPv4 addresses or IPv6 addresses and domains, you exclude all other hosts from sending messages at connection time.</td>
</tr>
<tr>
<td></td>
<td>See “Changing Scanner outbound mail acceptance settings” on page 51.</td>
</tr>
<tr>
<td>Modify the outbound mail delivery settings.</td>
<td>An outbound Scanner relays filtered email to a local or non-local mail server for delivery to recipients. When you configure email delivery for an outbound-only Scanner or a combined inbound and outbound Scanner, designate the IPv4 addresses and port numbers for both local and non-local mail hosts where filtered outbound mail is relayed.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Scanner outbound mail delivery settings” on page 52.</td>
</tr>
<tr>
<td>Specify how you want Symantec Messaging Gateway to handle bad messages.</td>
<td>Symantec Messaging Gateway’s bad message handling feature lets you specify how many times the system scans a potentially malformed message before it classifies it as such. Symantec Messaging Gateway then places it in the bad message queue.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring bad message handling” on page 53.</td>
</tr>
</tbody>
</table>

About Scanner email settings

Scanner email settings let you control various aspects of inbound and outbound message flow. You can limit the IP addresses from which Symantec Messaging Gateway accepts email messages. You can also control where Symantec Messaging Gateway delivers filtered email.

You can reduce the volume of email that any one Scanner filters by configuring separate inbound and outbound Scanners. Even if you use only one Scanner to filter both inbound and outbound email, you can configure various SMTP settings to control message flow.

**Note:** Individual Scanner email settings should not be confused with spam or virus scan settings, which control spam and virus scanning activity for all Scanners.

During site setup, you configure at least one combined inbound and outbound Scanner. This Scanner can be on the same computer that runs the Control Center, or on another computer.
You can instead configure separate inbound and outbound Scanners to run on separate hosts or add dedicated Scanners later.

**Note:** If you use the same IP address and port for inbound and outbound email, the Scanner uses outbound mail acceptance settings to determine if a message is inbound or outbound. The Scanner first checks outbound mail acceptance settings. If the mail is not accepted, the Scanner then checks inbound mail acceptance settings.

See “Changing Scanner outbound mail acceptance settings” on page 51.

The Add Scanner Wizard guides you through the process of configuring a Scanner's email settings. These initial email settings include:

- Scanner role – inbound email, outbound email, or both inbound and outbound email.
- Mail filtering – Scanner IP address and port number.
- Mail acceptance – IP addresses from which the Scanner accepts email to be filtered.
- Mail delivery – mail server to which filtered email is relayed and whether to enable MX Lookup.

See “Adding Scanners” on page 35.

After adding a Scanner to your deployment and testing it, you can modify its settings further by:

- Changing the Scanner role
  See “Configuring mail flow direction” on page 45.

- Modifying the Scanner's inbound email settings
  See “Changing Scanner inbound mail settings” on page 46.
  See “Changing Scanner inbound mail acceptance settings” on page 47.
  See “Configuring Scanner inbound email delivery settings” on page 48.

- Modifying the Scanner's outbound email settings
  See “Changing Scanner outbound mail settings” on page 50.
  See “Changing Scanner outbound mail acceptance settings” on page 51.
  See “Configuring Scanner outbound mail delivery settings” on page 52.

- Configuring advanced SMTP settings
  See “Configuring SMTP advanced settings” on page 54.

In addition, Connection Classification defers some connections based on local reputation data that is collected and implemented on a per-Scanner basis.

See “About managing connection load at the gateway” on page 143.
Configuring mail flow direction

You can configure a Scanner to filter inbound, outbound, or both inbound and outbound email.

To configure mail flow direction for a Scanner

1. In the Control Center, click **Administration > Hosts > Configuration**.

2. On the **Host Configuration** page, click the box next to the Scanner you want to define and then click **Edit**.

3. On the **Edit Host Configuration** page, click the **SMTP** tab.

4. In the **Host name** field, modify the name for the Scanner if necessary to identify it by its role.

5. In the **Host definition** field, modify the definition of the Scanner to reflect its new role.

6. Select the option that describes the role of this Scanner.

   - Inbound mail filtering only – Configure inbound SMTP Scanner settings.
   - Outbound mail filtering only – Configure outbound SMTP Scanner settings.
   - Inbound and Outbound mail filtering – Configure both the inbound and outbound SMTP Scanner settings.

   See “About Scanner email settings” on page 43.

7. At the bottom of the page, check **Apply above settings to all hosts** if you want settings to apply to all Scanners.

8. Click **Save** to store your changes.

On the **Add Policy Group** or **Edit Policy Group** page, you must also enable scanning for each filtering type and mail flow direction. You then choose the policies that you want to apply for the enabled mail flow directions. Symantec Messaging Gateway includes default policies for malware, threat defense, spam, and unwanted email. These default policies are automatically enabled and are assigned to the **Default** policy group of all users during installation. Each policy includes the mail flow direction where the policy can be applied. You can override default policies by creating new policy groups.

See “Default email malware policies” on page 218.

See “Default email spam and unwanted email policies” on page 250.

Content filtering does not have default policies. Mail flow direction is included in the content filtering templates that Symantec Messaging Gateway provides.

See “About content filtering” on page 322.
Changing Scanner inbound mail settings

You can change the IP address or port number through which a Scanner accepts inbound mail connections. You can also designate whether or not the Scanner accepts inbound TLS-encrypted connections.

To change Scanner inbound mail settings

1. In the Control Center, click Administration > Hosts > Configuration.
2. Under Hostname, check the inbound Scanner whose settings you want to modify and click Edit.
3. On the Edit Host Configuration page, click the SMTP tab.
4. Select the address where you want to receive inbound messages in the Inbound mail IP address drop-down menu and enter the port number in the Port text box.

Only those IP addresses, including virtual IP addresses, that have been configured for this Scanner's network interface card appear in the drop-down menu.

5. If IPv6 is enabled, you can select an IPv6 address where you want to receive inbound messages in the Optional Inbound mail IPv6 address drop-down menu and provide the port number in the Port text box.

Only those IPv6 addresses that are configured for this Scanner's network interface card appear in the drop-down menu. You can specify individual IPv6 addresses in any standard IPv6 format. Addresses are stored and displayed in shortened format.

6. Check Accept TLS encryption if you want the host to accept connections using TLS encryption.

If you leave this option unchecked, Symantec Messaging Gateway will not advertise support for TLS encryption during the SMTP session.

- You must configure an MTA TLS certificate and assign it to this Scanner before it can accept TLS encrypted email from a connection.
  See “Assigning an MTA TLS certificate to a Scanner” on page 185.
- The SSL Restrictions setting on the Protocols > SMTP > Settings > SMTP tab affects the TLS versions that Symantec Messaging Gateway advertises and supports.
  See “Specifying SSL restrictions for TLS communications” on page 96.

7. Select the name of a certificate from the drop-down menu to authenticate the Scanner as a trusted source to clients sending over TLS-encrypted connections.

See “About certificates” on page 169.

8. Check Request client certificate if you want the Scanner to request a TLS encryption certificate from a sender before accepting a TLS-encrypted connection.

9. Click Save to save settings for this host only.
Changing Scanner inbound mail acceptance settings

You can conserve Scanner resources by limiting inbound connections to only IP addresses from which you want the Scanner to filter email. By allowing connections from only certain IP addresses and domains, you exclude all other inbound clients from sending messages at connection time.

Warning: If you accept mail only from selected hosts, and your Scanner is not at the gateway, you must add all upstream mail servers. Add the IPv4 and IPv6 addresses, CIDR blocks, or netmasks of upstream mail servers on both the SMTP and Internal Mail Hosts tabs of the Edit Host Configuration page. Symantec Messaging Gateway rejects email from unspecified upstream servers.

See "Specifying internal mail hosts for non-gateway deployments" on page 65.

To change Scanner inbound mail acceptance settings

1. In the Control Center, click Administration > Hosts > Configuration.

2. Under Hostname, check the name of the inbound Scanner whose settings you want to modify and click Edit.

3. On the Edit Host Configuration page, click the SMTP tab.

4. Select one of the following options:

   **Accept inbound mail connections from all IP addresses**
   
   Select this option if you want the Scanner to accept connections from senders of all inbound messages.
   
   Proceed to step 6.

   **Accept inbound mail connections from only the following IP addresses**
   
   Select this option if you want the Scanner to accept only connections from the addresses that you check in the Inbound Mail Acceptance IP Addresses list.
   
   Then in the list, check the IP addresses from which you want this Scanner to accept inbound mail.
   
   Proceed to the next step.
Optionally, under **Inbound Mail Acceptance**, do any of the following tasks:

- **To manually add an IP address**
  Click *Add* and type the host name, or IPv4 address, or IPv6 address of a local domain from which you want to filter inbound email.
  You can specify individual IPv6 addresses in any standard IPv6 format. IPv6 addresses are stored and displayed in shortened format. Ranges are expressed in CIDR notation, as a combination of an address part and a prefix.

- **To edit an IP address**
  Check the host name or IP address of the email client whose settings you want to change, click *Edit*, then make the necessary changes.

- **To delete one or more IP addresses**
  Check the addresses or domains from which you no longer want to accept inbound connections and click *Delete* to delete them from the list.
  To delete all of the existing addresses or domains, click *Delete All*.

- **To import IP addresses**
  Click *Import*, browse to the file location, and click *Import*.
  You can import files with comma, semicolon, space, and tab delimiters.

- **To export IP addresses**
  Click *Export* and specify the name of the export file and location where you want to save it.

6. Click *Save* or check **Apply above settings to all Scanners** and then click *Save*.

**Configuring Scanner inbound email delivery settings**

After a Scanner filters inbound email, the MTA relays filtered email to a mail server for delivery to recipients. When you configure email delivery for an inbound-only or combined inbound and outbound Scanner, you designate the default local and non-local hosts where filtered inbound mail should be routed.

You can designate an unlimited number of local or non-local mail servers for delivery of inbound mail. Multiple downstream mail servers can improve load distribution and fault tolerance for filtered inbound mail if you accept mail that is addressed to different domains. You must specify the order in which a default relay (static route) delivers inbound email by assigning a preference number to each mail host. The Scanner attempts to deliver email to lower-numbered mail hosts first. If only one mail server is configured, its preference defaults to 1. If you want to load balance, specify equal preference numbers for each server.

Additionally, you can assign a mail server to each domain for which the Scanner accepts inbound email. Each mail server can host multiple local domains.

See “**About email domains**” on page 80.
You can enable MX Lookup for any mail host that you specify using a hostname. MX Lookup then determines which server to use to deliver email that is addressed to a recipient at a local domain.

To configure Scanner inbound email delivery settings

1. In the Control Center, click **Administration > Hosts > Configuration**.

2. Under **Hostname**, check the Scanner to which you want to add or edit a local mail server and click **Edit**.

3. On the **Edit Host Configuration** page, click the **SMTP** tab.

4. Under **Inbound Local Mail Delivery**, check the local host whose delivery information you want to change and click **Edit**.

   Alternatively, click **Add** to add delivery information about a local mail host.

   You can configure inbound mail delivery for an unlimited number of local mail hosts.

5. Enter or modify the IP address and port number or hostname in the text boxes that appear.

6. Check **MX Lookup** if you want the local mail host to use MX Lookup to determine which IP address to use for delivery to email recipients.

   You can only check MX Lookup if you specified a hostname.

7. If you have more than one host specified, type a number in the **Preference** field.

   Connections for lower numbered servers are attempted first.

8. If the Scanner role is **Inbound and outbound mail filtering**, click **Save** to save settings or check **Apply above settings to all hosts** and then click **Save**. Skip the rest of this procedure.

9. If the Scanner role is **Inbound mail filtering only**, click one of the radio buttons under **Inbound Non-Local Delivery**:

   - **Use MX Lookup for non-local mail** to have Symantec Messaging Gateway route mail for non-local recipients by MX query on recipient domains.

   - **Relay non-local mail to** to specify mail hosts for delivery of non-local mail.

10. Click **Add** to add the hostname or IP address and port number for a non-local mail host.

    You can configure inbound mail delivery for an unlimited number of non-local mail hosts.

    You can check the non-local host you want and click **Edit**, then modify the IP address and port number in the text boxes that appear.

11. Check **MX Lookup** if you want the local mail host to use MX Lookup to determine which IP address to use for delivery to email recipients.

    You can only check MX Lookup if you specified a hostname.
12 If you have more than one host specified, type a number in the **Preference** field. Connections for lower numbered servers are attempted first.

13 Click **Save** to save the delivery settings for an Inbound-only scanner or check **Apply above settings to all hosts** and then click **Save**.

**Changing Scanner outbound mail settings**

You can change the IP address or port number where a Scanner accepts outbound mail connections. You can also designate whether or not the Scanner accepts outbound TLS-encrypted connections.

**To change Scanner outbound mail settings**

1 In the Control Center, click **Administration > Hosts > Configuration**.

2 Under **Hostname**, click the name of the Outbound or Inbound and Outbound Scanner whose settings you want to modify and click **Edit**.

3 On the **Edit Host Configuration** page, click the **SMTP** tab.

4 In **Outbound mail IP address** and **Port**, enter the IP address and port number where you want outbound messages to be received.

5 In **Optional Outbound mail IPv6 address** and **Port**, select an optional IPv6 address and provide a port number where you want outbound messages to be received.

   You can specify individual IPv6 addresses in any standard IPv6 format. IPv6 addresses are stored and displayed in shortened format.

6 Check **Accept TLS encryption** if you want the host to accept TLS-encrypted outbound connections.

   ■ You must configure an MTA TLS certificate and assign it to this Scanner before it can accept TLS encrypted outbound mail for filtering.
   
   See “**Assigning an MTA TLS certificate to a Scanner**” on page 185.

   ■ The **SSL Restrictions** setting on the **Protocols > SMTP > Settings > SMTP** tab affects the TLS versions that Symantec Messaging Gateway accepts.
   
   See “**Specifying SSL restrictions for TLS communications**” on page 96.

7 From the **Certificate** drop-down menu, select a certificate to authenticate the Scanner as a trusted source to clients sending over TLS-encrypted connections.

   See “**About certificates**” on page 169.

8 Click **Save** or check **Apply above settings to all hosts** and then click **Save**.
Changing Scanner outbound mail acceptance settings

You can configure a Scanner to accept outbound connections from an unlimited number of mail servers. By allowing connections from only certain IP addresses and domains, you exclude all other hosts from sending messages at connection time.

**Note:** If you use the same IP address and port for inbound and outbound email, the Scanner uses outbound mail acceptance settings to determine if a message is inbound or outbound. The Scanner first checks outbound mail acceptance settings. If the mail is not accepted, the Scanner then checks inbound mail acceptance settings.

See “Changing Scanner outbound mail settings” on page 50.

**To change the outbound mail acceptance settings for a Scanner**

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. Under **Hostname**, check the Outbound or Inbound and Outbound Scanner whose settings you want to modify and click **Edit**.
3. On the **Edit Host Configuration** page, click the **SMTP** tab.
4. Under **Outbound Mail Acceptance**, do any of the following tasks:

   - **To manually add an IP address**
     - Click **Add** and type the host name or an IPv4 address or IPv6 address of a local domain from which you want to filter outbound email.
     - You can enter a range of IP addresses using CIDR notation. Individual IPv6 addresses are specified in any standard IPv6 format and are stored and displayed in shortened format.

   - **To edit an IP address**
     - Check the host name or IP address of the email client whose settings you want to change, click **Edit**, then make the necessary changes.

   - **To delete one or more IP addresses**
     - Check the addresses or domains from which you no longer want to accept outbound connections and click **Delete** to delete them from the list.
     - To delete all of the existing addresses or domains, click **Delete All**.

   - **To import IP addresses**
     - Click **Import**, browse to the file location, and click **Import**.
     - You can import files with comma, semicolon, space, and tab delimiters.

   - **To export IP addresses**
     - Click **Export** and specify the name of the export file and location where you want to save it.

5. Click **Save** or check **Apply above settings to all Scanners** and then click **Save**.
Configuring Scanner outbound mail delivery settings

An outbound Scanner relays filtered email to a local or non-local mail server for delivery to recipients. When you configure email delivery for an outbound-only or a combined inbound and outbound Scanner, you supply the IP addresses and port numbers for the local and non-local mail hosts where filtered outbound mail should be relayed.

You can specify multiple mail servers to relay outbound email to the Internet or to the next hop in your network. A maximum of 3 mail servers per scanner is recommended.

To configure Scanner outbound mail delivery settings

1. In the Control Center, click **Administration > Hosts > Configuration**.

2. On the **Host Configuration** page, under **Hostname**, check the name of the Scanner whose settings you want to modify and click **Edit**.

3. On the **Edit Host Configuration page**, click the **SMTP** tab.

4. Under **Mail Filtering**, select **Outbound mail filtering only** or **Inbound and outbound mail filtering**.

   See “Configuring mail flow direction” on page 45.

5. Click the **Outbound** tab.

   If you chose **Inbound and outbound mail filtering**, skip to step 10.

   If you chose **Outbound mail filtering only**, go to the next step to configure **Outbound Local Mail Delivery** settings.

6. Under **Relay local domain mail to the following hosts**, check a local host and click **Edit**.

   As an alternative, you can click **Add** to add delivery information about a local email host or **Delete** to delete a host.

7. In the host table, edit the **Host** (hostname or IP address) or **Port** (number) of the mail server to which you want the filtered outbound mail delivered.

8. Check **MX Lookup** if you want to enable MX lookup for this host.

   You can only use MX lookup if you specified a hostname.

9. If there is more than one host in the list, enter a number in the **Preference** field for each host.

   ▪ Connection to the host with the lowest Preference number is attempted first. If that host is unavailable (all connections are in use or there is a hardware failure, for example), Symantec Messaging Gateway switches to the host with the next lowest Preference number, but returns to a host with a lower Preference number as soon as that host becomes available.
- If you assign a Preference value of 1 to two hosts, Symantec Messaging Gateway randomly picks one of them. If that host becomes unavailable, Symantec Messaging Gateway connects to the other host with Preference 1. If that host becomes unavailable, Symantec Messaging Gateway attempts to reconnect with the first host. A host with the next highest Preference is used only if both hosts with Preference 1 are unavailable.

10 Under **Outbound Non-Local Mail Delivery**, click one of the following options:

- **Use MX Lookup for non-local domain mail** to have Symantec Messaging Gateway route mail for non-local recipients through MX query on recipient domains.
  If you choose this option, skip to step 15.

- **Relay non-local domain mail to the following hosts** to specify mail hosts for non-local delivery of outbound email.

11 In the **Host** list, check the non-local host whose delivery information you want to change and click **Edit**.

12 In the host table, edit the **Host** (hostname or IP address) or **Port** (number) of the mail server to which you want the filtered outbound mail delivered.

  As an alternative, you can click **Add** to add delivery information about a local email host or **Delete** to delete a host.

13 Check **MX Lookup** if you want to enable MX lookup for this host.

  You can only use MX lookup if you specified a hostname.

14 If there is more than one host in the list, enter a number in the **Preference** field for each host. See step 9 for a description of how Preference values work.

15 Click **Save** to save the delivery settings or check **Apply above settings to all Scanners** and then click **Save**.

### Configuring bad message handling

In rare instances, a malformed email message may cause the Brightmail Engine to fail. If this situation occurs, Symantec Messaging Gateway isolates the small number of messages that were being processed at the time of the failure and rescans them one at a time until the message that caused the failure is identified (causing the Brightmail Engine to fail again). The Brightmail Engine recovers from these failures quickly. The flow of mail is neither interrupted nor significantly delayed. When a bad message is detected, an alert is sent.

With Symantec Messaging Gateway's bad message handling feature, you can specify how many times the system scans a potentially malformed message before it classifies it as such and places it in the bad message queue.
Note: For each retry (every time the system scans the malformed message) the Brightmail Engine fails. Use caution when setting this value.

You can then access and manage messages in the bad message queue with the \texttt{mta-control} command-line option.

Once the malformed message is identified, you have several options when you use the \texttt{mta-control} command as follows:

- List email messages in the bad message queue
- View or export the message to a specified URL or to the screen
- Delete a message from the bad message queue
- Bypass the Brightmail Engine and deliver the message to its original recipient
- Deliver the message to system administrator(s) by email
- Resend the message through the Brightmail Engine

See "Administering Symantec Messaging Gateway through the command line" on page 730.

To configure bad message handling

1. Click Protocols > SMTP > Settings and then click the Content Scanning tab.
2. Check Enable bad message handling.
3. Type a value in the Number of retries before classifying a message as bad field.
4. Click Save.

Configuring SMTP advanced settings

Specifying the MTA host name lets you define the HELO banner during the initial portion of the SMTP conversation. The MTA host name also appears in Received headers. This host name is not connected to the OS-level host name of the Scanner. If you change the host name on the Edit Host page, the MTA host name is not changed.

To configure SMTP advanced settings

1. In the Control Center, click Administration > Hosts > Configuration.
2. Click the underlined name of the host you want to configure.
3. Click the SMTP tab.
4. Scroll to the bottom of the page and click Advanced Settings.
5. Make the desired configurations changes.
6 Click **Continue**.

7 On the **Host Configuration** page, click **Save**.

See “SMTP advanced inbound settings” on page 55.

See “SMTP advanced outbound settings” on page 56.

See “SMTP advanced delivery settings” on page 59.

See “SMTP advanced settings for delivery bindings” on page 61.

See “SMTP advanced authentication settings” on page 63.

**SMTP advanced inbound settings**

Table 2-5 describes inbound SMTP settings that you can configure to further define the Scanner SMTP connections.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of connections</td>
<td>Sets the maximum number of simultaneous inbound connections. The default is 2,000 connections.</td>
</tr>
<tr>
<td>Maximum number of connections from a single IPv4 address or IPv6 range</td>
<td>Sets the maximum number of simultaneous inbound connections that can be made from a single IPv4 address or IPv6 range. If Connection Classification is enabled, the settings for each Connection Class override this setting for IPv4 senders. The default value is 20 connections.</td>
</tr>
<tr>
<td>IPv6 CIDR prefix for maximum number of connections from a single IPv6 range</td>
<td>Describes the CIDR prefix to be used if an IPv6 range is used. The prefix value must be an integer from 0 to 128. The default value is 64.</td>
</tr>
<tr>
<td>Maximum number of connections from a single IP address</td>
<td>Sets the maximum number of simultaneous inbound connections that can be made from a single IP address. The default is 20. If Connection Classification is enabled, the settings for each Connection Class override this setting.</td>
</tr>
<tr>
<td>Maximum number of recipients per message</td>
<td>Sets the maximum number of recipients for a message. The default is 1,024 recipients.</td>
</tr>
</tbody>
</table>
Table 2-5  SMTP Advanced Settings—Inbound Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of messages per session</td>
<td>Indicates the maximum number of email messages that are permitted in a single session.</td>
</tr>
<tr>
<td></td>
<td>The default value is 0 if you have upgraded from a prior version. The default value is 100 if this is an initial installation.</td>
</tr>
<tr>
<td></td>
<td>This field is disabled if Connection Classification is enabled, and the settings for each Connection Class overrides the setting.</td>
</tr>
<tr>
<td>Maximum message size in bytes</td>
<td>Sets the maximum size of a message before it is rejected. The default is 10,485,760 bytes.</td>
</tr>
<tr>
<td>Maximum number of messages in inbound queue</td>
<td>Sets the maximum threshold. When this threshold is met or exceeded, alerts are sent (when enabled) and connections are deferred. The default is 5,000 messages.</td>
</tr>
<tr>
<td>Defer new connections when inbound queue is full</td>
<td>When the number of messages in the inbound queue exceeds the maximum, defers messages, by issuing an SMTP 4xx error. If unchecked, messages are accepted for as long as resources allow.</td>
</tr>
<tr>
<td></td>
<td>See “Troubleshooting the message queue” on page 647.</td>
</tr>
<tr>
<td>Insert a RECEIVED header to inbound messages</td>
<td>Places a RECEIVED header in the message during inbound SMTP processing.</td>
</tr>
<tr>
<td>Enable reverse DNS lookup</td>
<td>Causes the system to perform reverse DNS lookup on the SMTP client IP addresses to resolve the IP address to a name when checked. This is the default condition. When unchecked, reverse DNS lookup is not performed for inbound messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you enable the global reverse DNS settings on Protocols &gt; SMTP &gt; Settings &gt; SMTP tab, under DNS Validation, you override this local setting.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring reverse DNS validation” on page 88.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>This setting controls how long the MTA waits for a request or response from the connecting MTA. If this limit is exceeded, the appliance will drop the connection.</td>
</tr>
</tbody>
</table>

See “About Scanners” on page 32.

SMTP advanced outbound settings

Table 2-6 describes the advanced outbound SMTP settings that you can use to further define your SMTP configuration.
### Table 2-6  SMTP Advanced Settings—Outbound Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of connections</td>
<td>Sets the maximum number of simultaneous outbound connections. The default is 2,000 connections.</td>
</tr>
<tr>
<td>Maximum number of connections from a single IPv4 address or IPv6 range</td>
<td>Sets the maximum number of simultaneous outbound connections that can be made from a single IPv4 address or IPv6 range. The default value is 20 connections.</td>
</tr>
<tr>
<td>IPv6 CIDR prefix for maximum number of connections from a single IPv6 range</td>
<td>Describes the CIDR prefix to be used if an IPv6 range is used. The prefix value must be an integer from 0 to 128. The default value is 128.</td>
</tr>
<tr>
<td>Maximum number of connections from a single IP address</td>
<td>Sets the maximum number of simultaneous outbound connections that can be made from a single IP address. The default is 20 connections.</td>
</tr>
<tr>
<td>Maximum message size in bytes</td>
<td>Sets the maximum size allowable for a message before it is rejected. The default is 10,485,760 bytes.</td>
</tr>
<tr>
<td>Maximum number of recipients per message</td>
<td>Indicates the maximum number of recipients permitted to receive a message. The default is 1,024 recipients.</td>
</tr>
<tr>
<td>Maximum number of messages per session</td>
<td>Indicates the maximum number of email messages that are permitted in a single session. The default value is 0 if you have upgraded from a prior version. The default value is 100 if this is an initial installation.</td>
</tr>
<tr>
<td>Default domain for sender addresses with no domain</td>
<td>Sets a default domain when none can be found in the message.</td>
</tr>
<tr>
<td>Maximum number of messages in outbound queue</td>
<td>Sets the maximum threshold. When this threshold is met or exceeded, alerts are sent (when enabled) and connections are deferred. The default is 5,000 messages.</td>
</tr>
<tr>
<td>Maximum number of outbound recipients per sender in a specific time-frame</td>
<td>Sets the maximum number of recipients to which a sender can send mail in the specified time-frame (per minute or per hour). The default value is 0. The value 0 indicates that unlimited email messages are permitted in a single session.</td>
</tr>
</tbody>
</table>
Table 2-6 SMTP Advanced Settings—Outbound Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defer new connections when outbound queue is full</td>
<td>When the number of messages in the outbound queue reaches or exceeds the maximum, defers messages, by issuing an SMTP 4xx error. If unchecked, messages are accepted for as long as resources allow.</td>
</tr>
<tr>
<td>Insert RECEIVED header</td>
<td>Places a RECEIVED header in the message during outbound SMTP processing when checked. When unchecked, no RECEIVED header is inserted during outbound SMTP processing. If this option and Strip pre-existing RECEIVED headers are both checked, the outbound SMTP RECEIVED header remains when the message goes to the delivery queue.</td>
</tr>
<tr>
<td>Strip pre-existing RECEIVED headers</td>
<td>Removes all RECEIVED headers for outbound messages when checked. When headers are stripped, message looping can occur depending on the settings of other MTAs. When unchecked, RECEIVED headers remain in the message during outbound processing. The RECEIVED header for outbound SMTP processing remains in the message when both Insert RECEIVED header and Strip pre-existing RECEIVED headers are checked.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> Enabling this setting can reduce your ability to diagnose message flow issues.</td>
</tr>
<tr>
<td>Enable reverse DNS lookup</td>
<td>Causes the system to perform reverse DNS lookup on the SMTP client IP addresses to resolve the IP address to a name when checked. This is the default condition. When unchecked, reverse DNS lookup is not performed for outbound messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you enable the global reverse DNS settings on <strong>Protocols &gt; SMTP &gt; Settings &gt; SMTP</strong> tab, under DNS Validation, you override this local setting.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring reverse DNS validation” on page 88.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>This setting controls how long the MTA waits for a request or response from the connecting MTA. If this limit is exceeded, the appliance will drop the connection.</td>
</tr>
</tbody>
</table>

See “About Scanners” on page 32.
SMTP advanced delivery settings

*Table 2-7* describes SMTP delivery configuration message settings for your site.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of external connections</td>
<td>Sets the maximum number of simultaneous external connections. The default is 100 connections.</td>
</tr>
<tr>
<td>Maximum number of external connections to a single IP address</td>
<td>Sets the maximum number of simultaneous connections made to a single IP address. The default is 50 connections.</td>
</tr>
<tr>
<td>Maximum number of connections to all internal mail servers</td>
<td>Sets the maximum number of connections that can be made to all defined internal mail servers. The default is 100 internal mail server connections.</td>
</tr>
<tr>
<td>Maximum number of connections per single internal mail server</td>
<td>Sets the maximum number of connections to one internal mail server. The default is 50 connections.</td>
</tr>
<tr>
<td>Maximum number of messages in delivery queue</td>
<td>Sets the maximum threshold. When this threshold is met or exceeded, alerts are sent (when enabled) or connections are deferred. The default is 150,000 messages.</td>
</tr>
<tr>
<td>Maximum number of recipients per message in delivery queue</td>
<td>Specifies the number of recipients that are allowed per message in the delivery queue when recipients are batched. If the number of recipients for a message exceeds this value, the message is bifurcated until each messages' list of recipients no longer exceeds the limit. You can enter values from 1 to 1024. The default value is 100.</td>
</tr>
<tr>
<td>Maximum number of outgoing messages for a connection</td>
<td>Sets the maximum threshold for the number of messages the MTA can send over a single connection. A setting of 0 disables the limit. The default setting is 0.</td>
</tr>
<tr>
<td>Defer new connections when delivery queue is full</td>
<td>When the number of messages in the delivery queue reaches or exceeds the maximum, defers messages, by issuing an SMTP 4xx error. If unchecked, messages are accepted for as long as resources allow.</td>
</tr>
<tr>
<td>Minimum retry interval</td>
<td>Sets the smallest interval the SMTP server waits before trying to deliver a message again. The default is 15 minutes.</td>
</tr>
<tr>
<td>Maximum retry interval</td>
<td>Sets the maximum interval the SMTP server waits before trying to deliver a message again. The default value is 7 hours. Do not set this value to less than the value of the Minimum retry interval.</td>
</tr>
</tbody>
</table>
Table 2-7: SMTP Advanced Settings—Delivery Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent message time-out</td>
<td>Sets the time after which an undelivered message times out and is rejected from the queue. The default is 5 days.</td>
</tr>
<tr>
<td>Bounce message time-out</td>
<td>Sets a time-out period for deletion of messages in your bounce queue. This can be particularly useful in environments where you cannot configure LDAP settings. The default is 1 day.</td>
</tr>
<tr>
<td>Message delay time in queue before notification</td>
<td>Sets the time a message waits in the mail queue before notification of nondelivery is sent. The default is 4 hours.</td>
</tr>
<tr>
<td>Attempt TLS encryption for all messages</td>
<td>Instructs the MTA to attempt TLS encryption for all messages delivered.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you enable SSL Restrictions on the Protocols &gt; SMTP &gt; Settings &gt; SMTP tab, SMG attempts encryption only with a supported TLS protocol.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying SSL restrictions for TLS communications” on page 96.</td>
</tr>
<tr>
<td>Offer TLS client certificate</td>
<td>Instructs the MTA to offer a client certificate with every TLS connection.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>The amount of time in seconds to spend waiting for the connect system call to return. The default value is 30 seconds.</td>
</tr>
<tr>
<td>EHLO/HELO timeout</td>
<td>The amount of time in seconds to wait for a response to the EHLO or HELO command. The default value is 5 minutes.</td>
</tr>
<tr>
<td>MAIL FROM timeout</td>
<td>The amount of time in seconds to wait for a response from the MAIL FROM command. The default value is 5 minutes.</td>
</tr>
<tr>
<td>RCPT TO timeout</td>
<td>The amount of time in seconds to wait for a response to the RCPT TO command. The default value is 5 minutes.</td>
</tr>
<tr>
<td>DATA timeout</td>
<td>The amount of time in seconds to wait for a response once the DATA phase is terminated by a CRLF.CRLF. This timeout is relatively long because it is the only phase of transmission which involves significant network transmission. The default value is 10 minutes.</td>
</tr>
<tr>
<td>RSET timeout</td>
<td>The amount of time to wait for a response to a RSET command. RSET commands are used to reset the state of an SMTP session in which a transaction has only partially succeeded. It allows subsequent messages to be delivered down a single SMTP session immediately following a transient or permanent failure response from the remote server before the complete and successful delivery of the previous message. The default value is 10 minutes.</td>
</tr>
</tbody>
</table>
Table 2-7  SMTP Advanced Settings—Delivery Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle timeout</td>
<td>The amount of time in seconds to hold open an idle connection when there are no messages currently deliverable for that domain. The default value is 5 seconds.</td>
</tr>
</tbody>
</table>

See “About Scanners” on page 32.

SMTP advanced settings for delivery bindings

Table 2-8 describes the settings available for delivery bindings. Delivery bindings allow you to specify the IP addresses from which messages are sent.

You can also set domain-specific delivery bindings for non-local messages. For each of your local domains, this feature enables you to define one or more IP addresses that messages from that domain are sent from.

Table 2-9 describes the settings available for per-domain delivery bindings for non-local messages.

Table 2-8  SMTP Advanced Settings—Delivery Bindings

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local messages</td>
<td>Sets the IP address that delivers messages locally.</td>
</tr>
<tr>
<td></td>
<td>The drop-down menu provides a list of IP addresses for this Scanner from which you can choose: the inbound listener IP address, the outbound listener IP address, all virtual addresses, or Auto. If you choose Auto, Symantec Messaging Gateway automatically chooses the best route based on current traffic flow.</td>
</tr>
<tr>
<td>Non-local messages</td>
<td>Sets the IP address that delivers non-local messages.</td>
</tr>
<tr>
<td></td>
<td>The drop-down menu provides a list of IP addresses for this Scanner from which you can choose: the inbound listener IP address, the outbound listener IP address, all virtual addresses, or Auto. If you choose Auto, Symantec Messaging Gateway automatically chooses the best route based on current traffic flow.</td>
</tr>
</tbody>
</table>
### Table 2-8  SMTP Advanced Settings—Delivery Bindings (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamically routed messages</td>
<td>Sets the IP address that delivers messages to non-static routes. The drop-down menu provides a list of IP addresses for this Scanner from which you can choose: the inbound listener IP address, the outbound listener IP address, all virtual addresses, or Auto. If you choose Auto, Symantec Messaging Gateway automatically chooses the best route based on current traffic flow. <strong>Note:</strong> If you are using multiple IP addresses and your system is provisioned for content encryption, <strong>Dynamically routed messages</strong> must be set to &quot;Auto.&quot; See &quot;Managing host and port information for content encryption&quot; on page 451.</td>
</tr>
<tr>
<td>Messages destined for the Control Center</td>
<td>Sets the IP address that delivers mail to the Control Center for storage in Spam Quarantine, Suspect Virus Quarantine, or content incident folders. The drop-down menu provides a list of IP addresses for this Scanner from which you can choose: the inbound listener IP address, the outbound listener IP address, all virtual addresses, or Auto. If you choose Auto, Symantec Messaging Gateway automatically chooses the best route based on current traffic flow.</td>
</tr>
</tbody>
</table>

### Table 2-9  SMTP Advanced Settings—Non-Local SMTP Delivery Bindings Per Domain

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>This list includes all domains defined for this Scanner, as local or non-local domains. To select multiple domains, hold down Ctrl.</td>
</tr>
<tr>
<td>IP addresses</td>
<td>This list includes all IP addresses available on this Scanner. To select multiple IP addresses, hold down Ctrl.</td>
</tr>
<tr>
<td>Add</td>
<td>Click to add the combination(s) of domains and IP addresses selected to the Domain/IP Address list. By selecting more than one domain or IP address first, you can add multiple rows with one click.</td>
</tr>
<tr>
<td>Delete</td>
<td>Check the box next to a row in the Domain/IP Address list and click <strong>Delete</strong> to delete that row.</td>
</tr>
<tr>
<td>Delete All</td>
<td>Click to delete all rows in the Domain/IP Address list, including any rows not currently visible.</td>
</tr>
</tbody>
</table>
Table 2-9  SMTP Advanced Settings—Non-Local SMTP Delivery Bindings Per Domain (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entries per page</td>
<td>Set the number of entries to display per page.</td>
</tr>
<tr>
<td>Display</td>
<td>Select a range of entries to display.</td>
</tr>
<tr>
<td></td>
<td>Go to beginning of entries.</td>
</tr>
<tr>
<td></td>
<td>Go to previous page of entries.</td>
</tr>
<tr>
<td></td>
<td>Go to next page of entries.</td>
</tr>
<tr>
<td></td>
<td>Navigate to last page of members or 50 pages ahead if there are more than 50 pages.</td>
</tr>
<tr>
<td>Domain/IP Address list</td>
<td>Each row in this list shows only one domain and one IP address. You can use the Add button to add multiple rows simultaneously. Each row defines the delivery binding for non-local messages from one domain.</td>
</tr>
</tbody>
</table>

SMTP advanced authentication settings

Table 2-10 describes the advanced authentication SMTP settings that you can use to further define your SMTP configuration.

Table 2-10  SMTP Advanced Settings—SMTP Authentication Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of connections</td>
<td>Sets the maximum number of simultaneous SMTP authentication connections. The default is 2,000 connections.</td>
</tr>
<tr>
<td>Maximum number of connections from a single IPv4 address or IPv6 range</td>
<td>Sets the maximum number of simultaneous SMTP authentication connections that can be made from a single IPv4 address or IPv6 range. The default value is 20 connections.</td>
</tr>
<tr>
<td>IPv6 CIDR prefix for maximum number of connections from a single IPv6 range</td>
<td>Describes the CIDR prefix to be used if an IPv6 range is used. The prefix value must be an integer from 0 to 128. The default value is 64.</td>
</tr>
</tbody>
</table>
### Table 2-10: SMTP Advanced Settings—SMTP Authentication Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of connections from a single IP address</td>
<td>Sets the maximum number of simultaneous SMTP authentication connections that can be made from a single IP address. The default is 20 connections.</td>
</tr>
<tr>
<td>Maximum message size in bytes</td>
<td>Sets the maximum size allowable for a message before it is rejected. The default is 10,485,760 bytes.</td>
</tr>
<tr>
<td>Maximum number of recipients per message</td>
<td>Indicates the maximum number of recipients permitted to receive a message. The default is 1,024 recipients.</td>
</tr>
<tr>
<td>Maximum number of messages per session</td>
<td>Indicates the maximum number of email messages that are permitted in a single session. The default value is 100.</td>
</tr>
<tr>
<td>Insert RECEIVED header</td>
<td>Places a RECEIVED header in the message during outbound processing of messages sent using SMTP authentication when checked. When unchecked, no RECEIVED header is inserted during outbound SMTP processing. If this option and Strip pre-existing RECEIVED headers are both checked, the outbound SMTP RECEIVED header remains when the message goes to the delivery queue.</td>
</tr>
<tr>
<td>Strip RECEIVED headers</td>
<td>Removes all RECEIVED headers for outbound messages sent using SMTP authentication when checked. When headers are stripped, message looping can occur depending on the settings of other MTAs. When unchecked, RECEIVED headers remain in the message during outbound processing. The RECEIVED header for outbound SMTP processing remains in the message when both Insert RECEIVED header and Strip pre-existing RECEIVED headers are checked. <strong>Warning:</strong> Enabling this setting can reduce your ability to diagnose message flow issues.</td>
</tr>
<tr>
<td>Enable reverse DNS lookup</td>
<td>Causes the system to perform reverse DNS lookup on the SMTP client IP addresses to resolve the IP address to a name when checked. This is the default condition. When unchecked, reverse DNS lookup is not performed for outbound messages sent using SMTP authentication. <strong>Note:</strong> When you enable the global reverse DNS settings on Protocols &gt; SMTP &gt; Settings &gt; SMTP tab, under DNS Validation, you override this local setting. See “Configuring reverse DNS validation” on page 88.</td>
</tr>
</tbody>
</table>
Table 2-10  SMTP Advanced Settings—SMTP Authentication Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable optional SASL plain support</td>
<td>By default, Symantec Messaging Gateway uses SASL login authentication. You can choose to also enable SASL plain authentication. For more information, see the following RFCs: 4954 4616</td>
</tr>
<tr>
<td>Session timeout</td>
<td>This setting controls how long the MTA waits for a request or response from the connecting MTA. If this limit is exceeded, the appliance will drop the connection. The default value is 30 seconds.</td>
</tr>
</tbody>
</table>

Note: The SMTP authentication listener uses the outbound message queue, and inherits some behavior from the outbound listener.

See “About Scanners” on page 32.

Specifying internal mail hosts for non-gateway deployments

Internal mail hosts are mail transfer agents (MTAs) that pass email from the Internet to a Scanner. If your Scanners are at the Internet gateway, you do not need to specify internal mail hosts. However, if your network is configured with one or more MTAs that are, with respect to inbound mail flow, upstream from your Scanners, you must specify the IPv4 addresses or IPv6 addresses of these MTAs as internal mail hosts. IPv6 addresses can be specified as addresses or ranges.

If your network has MTAs that are upstream from Symantec Messaging Gateway, it is important to specify these MTAs as internal mail hosts for the following reasons:

■ Email from upstream MTAs to Scanners will likely contain some spam messages. Scanners will see all external email as coming from the IP addresses of the gateway MTAs. If you have enabled Connection Classification, this may result in all email arriving from the Internet being deferred.

■ Scanners will not be able to determine the IP address of a sender. Sender groups that match IP addresses such as Local Bad Sender IPs will not function properly.

In addition to internal mail hosts you can add, Symantec Messaging Gateway displays a series of IP address ranges in the internal hosts list.
Follow these procedures to add or delete internal mail hosts from which the Scanner is always allowed to receive mail.

**To add an internal mail host to the list of allowed hosts**

1. From the Control Center, click **Administration > Hosts > Configuration**.
2. Check the Scanner that you want to configure.
3. Click **Edit**.
4. Click the **Internal Mail Hosts** tab.
5. Specify the IP address for an internal mail host.
   - You can specify an IPv4 address or an IPv6 address.
   - Individual IPv6 addresses can be specified in any standard IPv6 format and are stored and displayed in shortened format. Ranges are expressed in CIDR notation, as a combination of an address part and a prefix.
6. Click **Add**.
7. Click **Save** to store the information.

**To delete an internal mail host**

1. From the Control Center, click **Administration > Hosts > Configuration**.
2. Check the Scanner you want to configure.
3. Click **Edit**.
4. Click the **Internal Mail Hosts** tab.
5. Select an internal mail host.
6. Click **Delete**.
   - If you delete any of the default internal mail hosts, a warning message appears.
7. Click **Save** to store the information.

See "Internal mail servers: non-gateway deployments" on page 66.

**Internal mail servers: non-gateway deployments**

When deployed at the gateway, Symantec Messaging Gateway obtains the physical or peer IP connection for an incoming message and compares it to entries in the good sender and bad sender groups. If a Scanner is deployed elsewhere in your network, for example, downstream from a gateway MTA that is not identified as an internal mail host, Symantec Messaging Gateway may identify the IP address of your gateway server as a source of spam. You should accurately identify all internal mail hosts that are, with respect to inbound mail flow, upstream from your Symantec Messaging Gateway appliance.
See “Specifying internal mail hosts for non-gateway deployments” on page 65.

In addition to internal mail hosts you can add, Symantec Messaging Gateway includes a series of IP address ranges in the internal hosts list as follows:

- 0.0.0.0/255.0.0.0
- 10.0.0.0/255.0.0.0
- 127.0.0.0/255.0.0.0
- 169.254.0.0/255.255.0.0
- 172.16.0.0/255.240.0.0
- 192.168.0.0/255.255.0.0
- ::/128
- ::/128
- fe80 ::/10
- fc00::/7

Symantec Messaging Gateway will exclude the IP addresses of internal mail hosts from the following verdicts:

- Local Good Sender IPs
- Third Party Good Senders
- Local Bad Sender IPs
- Third Party Bad Senders
- Directory Harvest Attacks
- Symantec Global Bad Senders
- Symantec Global Good Senders
- Connection Classification
- Email Virus Attacks
- Fastpass

### Modifying Scanner configurations

You can modify a Scanner’s configuration at any time. For example, you can suspend the flow of mail or enable different components and services.

You must have Full Administration rights or Manage Settings modify rights to modify Scanner settings.
To modify Scanner configurations

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. Click the linked name of the Scanner that you want to edit.
3. Make any changes to the host or its included components and services.

**Note:** If you provision content encryption for your messaging system and you later add or change the IP address of a Scanner, you must inform your Symantec provisioning representative. For more information, see the Symantec Content Encryption Provisioning page by clicking **Content > Settings > Content Encryption** and then clicking the **Click here** link.

See “Encrypting data with Symantec Content Encryption” on page 449.

See “Adding Scanners” on page 35.

See “About Scanner email settings” on page 43.

Enabling and disabling Scanners

You can disable or enable a Scanner, or delete a Scanner. When you disable a Scanner, you stop the flow of email messages, statistics, logs, and configuration information between that Scanner and your Control Center. The Scanner stops processing messages. The Scanner neither sends nor receives messages. The Control Center stops routing Spam Quarantine mail to the Scanner. Message Audit Log queries omit the Scanner.

**To disable or enable a Scanner**

1. In the Control Center, click **Administration > Hosts > Configuration**.

   This page lists your Scanners. A black dash in the Enabled column indicates that the Scanner is disabled. A green check in the Enabled column indicates that the Scanner is enabled.

2. Check the Scanner that you want to change.

3. Click **Enable** to enable the Scanner or click **Disable** to disable the Scanner.

Stopping and starting Scanners

You may have an occasion when you want to stop a Scanner. For example, you may want to temporarily stop the mail flow so that you can troubleshoot an issue. After you resolve the issue, you can restart the Scanner. Or you may want to stop a Scanner so that you can delete it. Otherwise, you can lose the email messages that are in the Scanner email queues. You must have Full Administration rights or Manage Setting modify rights to stop and start Scanners.
Symantec recommends that you stop a Scanner before you delete it. A Scanner does not process mail when it is stopped.

**Note:** You cannot stop the host on which the Control Center is running.

If you have a Scanner that you want to stop permanently or remove, you can delete it.

See “Deleting Scanners” on page 70.

**Note:** The best procedure to stop a Scanner may vary based on your system parameters and message flow characteristics. You can design your own procedure for stopping a Scanner based on the impact of each of the settings.

See “MTA and message queue behavior” on page 74.

See “Services and MTA operations” on page 71.

To stop a Scanner

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. Click the Scanner that you want to stop.
3. Click **Do not accept incoming messages**.
4. Click **Save**.
5. Click **Status > SMTP > Message Queues**.
6. In the **Host** drop-down list, choose a Scanner.
7. In the **Queue** drop-down list, choose a queue.
8. In the **List** drop-down list, click **All**.
   - Or to proceed more quickly on a high-volume Scanner, click **10 in queue longest** instead.
9. Click **Display Filtered**.
10. Click **Flush All**.
11. Repeat steps 7 - 10 for the other queues.
12. Let the messages drain from the queue.
   - To check the message queue status, repeat steps 7 - 9 for each queue.
13. Click **Administration > Hosts > Configuration**.
14. Click the Scanner that you want to stop.
15. Check **MTA** and click **Stop**.
Click Save to save your changes and return to the Host Configuration page.

Check the box next to the Scanner that you want to stop and click Disable.

The Scanner list updates to reflect your change.

To start a Scanner
1. In the Control Center, click Administration > Hosts > Configuration.
2. To enable a Scanner that is currently disabled, check the box next to the Scanner and click Enable.
   
   You can check multiple boxes.
   
   The Scanner list updates to reflect your change.

Deleting Scanners
When you delete a Scanner, you permanently remove that Scanner's services from the Control Center. Symantec recommends that you stop a Scanner before you delete it. Otherwise, you can loose the email messages that are in the Scanner email queues. You cannot delete the host on which the Control Center is running. You must have Full Administration rights or Manage Setting modify rights to delete Scanners.

Once you delete a Scanner, you cannot retrieve or access its configuration settings. If you are uncertain as to whether you want to delete a Scanner, you can stop the Scanner. When you stop a Scanner, it still exists but no longer scans messages.

To delete Scanners
1. In the Control Center, click Administration > Hosts > Configuration.
2. Check the box next to the Scanner that you want to delete.
3. Click Delete.

See “Stopping and starting Scanners” on page 68.

See “Enabling and disabling Scanners” on page 68.

Changing the IP address of the Control Center host
If you must change the IP address of the appliance that is hosting your Control Center, you must first change the IP address of the Control Center host using the Control Center and then run the agentconfig command from each Scanner's command line interface to re-allow connections from the new Control Center host IP to that Scanner.

See “Configuring IPv4 Ethernet settings and routes” on page 39.
See agent-config on page 737.
Managing services and MTA operations

Use the following procedures from the Services tab to manage individual Scanner services and MTA operations.

To start and stop services
1. In the Control Center, click Administration > Hosts > Configuration.
2. Click the name of the Scanner on which you want to stop or start a service.
3. Check the services to be started or stopped.
4. Click Stop to stop a running service or Start to start a stopped service.

To manage a Scanner’s MTA operations
1. In the Control Center, click Administration > Hosts > Configuration.
2. Click the name of the Scanner that you want to change.
3. On the MTA Operation portion of the page, perform one of the following actions:
   - To pause message delivery, click Pause message scanning and delivery. Inbound and outbound messages are placed in a queue for future scanning and delivery.
   - To reject incoming messages, check Do not accept incoming messages. All messages currently in message queues are scanned and delivered, but all new messages are rejected.
   - To restore normal operation, click Accept and deliver messages normally.
4. Click Save to store your changes.

See “MTA and message queue behavior” on page 74.
See “Services and MTA operations” on page 71.
See “Scanner Services” on page 73.

Services and MTA operations

Table 2-11 lists the various settings that you use to start or stop services, view the status of services, and configure MTA operations.
### Table 2-11  Edit Host Configuration page—Services tab

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start/Stop</strong></td>
<td>Allows you to start or stop one or more services by checking the box next to the service name under Scanner Services and clicking Start or Stop. Stopping the MTA service will stop the inbound, outbound, and delivery listeners. To stop one or more listeners separately or in sequence, stop the corresponding message queues on the Status &gt; SMTP &gt; Message Queues page. <strong>Note:</strong> If you use SMTP authentication, Symantec Messaging Gateway employs an additional listener for authentication. This listener is controlled by the outbound listener controls. If you stop the outbound listener, the authentication listener also stops. See “MTA and message queue behavior” on page 74. <strong>Note:</strong> If you stop the Brightmail Engine or the MTA on a host configured to receive alerts, and wish to continue receiving alerts, specify an operating MTA IP address under SMTP Host on the Administration &gt; Settings &gt; Control Center page.</td>
</tr>
</tbody>
</table>
| **Scanner Services** | Lists the Scanner services available to the selected host. These are:  
  - Conduit  
  - LiveUpdate  
  - Brightmail Engine  
  - MTA  
  - Directory Data Service  
Check the name of the service you want to start or stop for this host. Check Scanner Services to select all the services. |
| **Status** | Indicates whether a particular service is either Running (in black) or Stopped (in red). If the service crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. |
Table 2-11  Edit Host Configuration page—Services tab (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTA Operation</td>
<td>Use the radio buttons to determine how the host handles messages. Choices are:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Accept and deliver messages normally</strong> – Processes messages in accordance with defined policies.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Pause message scanning and delivery</strong> – Accepts inbound and outbound messages; holds messages in queues for future scanning and delivery. This option can be useful if you want to pause incoming messages while waiting for new virus definitions.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Do not accept incoming messages</strong> – Rejects incoming messages; scanning and delivery of messages in message queues continues. This option is useful when you need to drain queues in order to remove a host from use. When a message is rejected, the SMTP server is sent a <em>service not available (450)</em> error message. Once this option is selected, all previously received messages are processed, but no new messages are accepted.</td>
</tr>
</tbody>
</table>

See “MTA and message queue behavior” on page 74.

Scanner Services

Use the **Services** tab to configure a Scanner to perform any of the following tasks:

- Enable or disable the following services on a Scanner using the **Services** tab on the **Edit Host Configuration** page. Each host runs several services that it uses to communicate with the Internet and other servers on your network.

Conduit


LiveUpdate

Automatically downloads virus definitions from Symantec Security Response to the Scanner. This information is used by the Scanner’s Brightmail Engine to identify known security threats.

Brightmail Engine

Scans email and attachments and file transfers for viruses, spam, and content filtering according to filter polices that you have configured.

MTA

The mail transfer agent routes inbound and outbound messages to the Brightmail Engine for processing and delivers filtered messages to their internal destinations or to the Internet.
The directory data service lets you use the information that is stored in your Lightweight Directory Access Protocol (LDAP) directories for features in the Symantec Messaging Gateway.

**Note:** If you stop the Brightmail Engine or the MTA service on a host configured to receive alerts, you must specify another host to continue receiving alerts. To avoid an interruption in alerting, modify the *SMTP Host and Port* fields on the *Control Center Settings* page (Administration > Settings > Control Center) before stopping either of these services.

See “Managing services and MTA operations” on page 71.

- Enable, disable, or pause incoming message scanning
  Enabling a Scanner to accept and deliver messages normally is the default behavior. However, if you have to take a Scanner offline, you can limit MTA operations in stages while you assign them to other Scanners.
  See “Services and MTA operations” on page 71.
  See “MTA and message queue behavior” on page 74.

### MTA and message queue behavior

Each Scanner includes an MTA and corresponding message queues: inbound, outbound, and delivery. Each message queue is managed by a corresponding listener: inbound, outbound, and delivery. In the Control Center, you can perform a variety of actions on the MTA and on message queues.

**Note:** If you use SMTP authentication, Symantec Messaging Gateway employs an additional listener for authentication. This listener is controlled by the outbound listener controls. If you stop the outbound listener, the authentication listener also stops.

Table 2-12 describes the expected behavior for new messages and messages in queues when you perform specific actions on the Services tab of the Administration > Hosts > Configuration/Edit page.

<table>
<thead>
<tr>
<th>Action performed</th>
<th>New messages are</th>
<th>Messages in queues are</th>
<th>Message delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click MTA, then click Stop.</td>
<td>Not accepted. There is no MTA running. External MTAs treat this as an SMTP 4xx error.</td>
<td>Not scanned, not delivered.</td>
<td>Stops.</td>
</tr>
</tbody>
</table>
### Table 2-12
Manage MTA and message queues on the Edit Host Configuration page, Services tab (continued)

<table>
<thead>
<tr>
<th>Action performed</th>
<th>New messages are</th>
<th>Messages in queues are</th>
<th>Message delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click <strong>Pause message scanning and delivery</strong>. <strong>Note:</strong> This action is equivalent to issuing the <code>mta-control pause-mode pause-scan</code> command.</td>
<td>Accepted.</td>
<td>Not scanned, not delivered. Accumulate in the inbound and outbound message queues.</td>
<td>Stops.</td>
</tr>
<tr>
<td>Click <strong>Do not accept incoming messages</strong>. <strong>Note:</strong> This action is equivalent to issuing the <code>mta-control pause-mode pause-accept</code> command.</td>
<td>Rejected, issuing SMTP service not available (450) error messages.</td>
<td>Scanned and delivered.</td>
<td>Continues.</td>
</tr>
</tbody>
</table>

**Table 2-13** describes the expected behavior for new messages and messages in queues when you perform specific actions on the **Status > SMTP > Message Queues** page.

**Note:** Each action in **Table 2-13** affects only one message queue. For example, stopping the inbound message queue has no effect on the outbound or delivery message queues.

### Table 2-13
Manage MTA and message queues on the Message Queues page

<table>
<thead>
<tr>
<th>Action performed</th>
<th>New messages are</th>
<th>Messages in queues are</th>
<th>Message delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display a message queue, click <strong>Flush All</strong>.</td>
<td>Accepted.</td>
<td>Any messages deferred due to delivery problems are retried.</td>
<td>Continues.</td>
</tr>
<tr>
<td>Display a message queue, click <strong>Delete All</strong>.</td>
<td>Accepted.</td>
<td>Deleted.</td>
<td>Continues.</td>
</tr>
<tr>
<td>Display the inbound message queue, click <strong>Stop</strong>.</td>
<td>Not accepted. External MTAs treat this as an SMTP 4xx error.</td>
<td>Not scanned.</td>
<td>Continues.</td>
</tr>
<tr>
<td>Display the outbound message queue, click <strong>Stop</strong>.</td>
<td>Not accepted. External MTAs treat this as an SMTP 4xx error.</td>
<td>Not scanned.</td>
<td>Continues.</td>
</tr>
</tbody>
</table>
Table 2-13

Manage MTA and message queues on the Message Queues page (continued)

<table>
<thead>
<tr>
<th>Action performed</th>
<th>New messages are</th>
<th>Messages in queues are</th>
<th>Message delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the delivery message queue, click Stop.</td>
<td>Accepted.</td>
<td>Scanned, not delivered. Accumulate in the delivery message queue.</td>
<td>Stops.</td>
</tr>
</tbody>
</table>

See “Services and MTA operations” on page 71.
See “Scanner Services” on page 73.
See “Turning off an appliance” on page 703.
See “About message queues” on page 642.
Configuring email settings

This chapter includes the following topics:

■ Configuring email settings
■ Configuring email domains
■ Configuring email aliases and address masquerades
■ Specifying SSL restrictions for TLS communications
■ About invalid recipients
■ About email message flow
■ Configuring email for SMTP authentication
■ Specifying address validation criteria

Configuring email settings

Table 3-1 describes the process to set up email settings for your Scanner.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Set up domains.</td>
<td>Understand how email domains work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Determine which domain configuration is right for you.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;About email domains&quot; on page 80.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Adding or editing domains&quot; on page 82.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import an existing list of domains.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Importing a domains list&quot; on page 85.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify domain acceptance settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;About email domain acceptance settings&quot; on page 87.</td>
</tr>
<tr>
<td>Phase 2</td>
<td>Configure email aliases and address</td>
<td>Understand how aliases and address masquerades work.</td>
</tr>
<tr>
<td></td>
<td>masquerades.</td>
<td>See &quot;About aliases and address masquerades&quot; on page 90.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map a source email address and destination for each alias.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Adding or editing aliases&quot; on page 91.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Alias addresses&quot; on page 92.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import an existing list of aliases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Importing aliases&quot; on page 92.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add, edit, and import address masquerades.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Adding or editing address masquerades&quot; on page 93.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Importing an address masquerade list&quot; on page 94.</td>
</tr>
<tr>
<td>Phase 3</td>
<td>Configure invalid recipient email</td>
<td>IR handling options vary depending on features you want to enable. Determine your needs before specifying up IR handling.</td>
</tr>
<tr>
<td></td>
<td>handling.</td>
<td>See &quot;About invalid recipients&quot; on page 98.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify what you want the system to do with invalid recipient emails.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See &quot;Setting up invalid recipient handling&quot; on page 99.</td>
</tr>
</tbody>
</table>
Table 3-1  Process for configuring Scanner email settings (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 4</td>
<td>Understand SMTP (Simple Mail Transfer Protocol) message flow phases.</td>
<td>See “About email message flow” on page 100. Use the message flow phases as a guideline to creating and maintaining your Scanner email configurations. See “Email message flow phases” on page 101.</td>
</tr>
</tbody>
</table>

Configuring email domains

Scanner message processing requires initial setup based on your email needs. For example, you can indicate the domains for which you accept inbound mail.

Table 3-2 describes the tasks that you can perform to set up email domains after you determine which domain configuration is appropriate. You can perform any of these tasks as needed in any order.

Table 3-2  Working with email domains

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about email domains to help you make good decisions about working with them.</td>
<td>You must define any domain for which you want Symantec Messaging Gateway to accept inbound email as a local domain. Symantec Messaging Gateway only accepts inbound email that is addressed to local domains. However, a domain from which you send email can be a local domain or a non-local domain. Defining more than one domain lets you assign different routing and delivery options to each domain, including TLS encryption for secure delivery, for local or non-local domains. By configuring TLS encryption options for non-local domains, you can secure connections for delivery by external servers. See “About email domains” on page 80.</td>
</tr>
<tr>
<td>Add or modify a domain.</td>
<td>You must define any domain for which you want Symantec Messaging Gateway to accept inbound email as a local domain. Symantec Messaging Gateway only accepts inbound email that is addressed to local domains. However, a domain from which you send email can be a local domain or a non-local domain. Defining more than one domain lets you assign different routing and delivery options to each domain, including TLS encryption for secure delivery, for local or non-local domains. By configuring TLS encryption options for non-local domains, you can secure connections for delivery by external servers. Configuring separate local and non-local domains provides you with different routing and delivery options. See “Adding or editing domains” on page 82.</td>
</tr>
</tbody>
</table>
### Working with email domains (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Import a domains list.** | Lists of domain definitions and email addresses can be imported from an ASCII file, similar to the Sendmail mailertable. You can include optional routing information to default local destination hosts can be included as part of the definition.  
See “Importing a domains list” on page 85. |
| **Delete domains to which you no longer want email sent.** | Deleting a local domain means that the MTA no longer accepts inbound email messages that are addressed to that domain. Deleting a non-local domain means that any routing or TLS options that are configured for that domain no longer operate.  
See “Deleting domains” on page 87. |
| **Learn more about email domain acceptance settings.** | During site setup, you designate at least one local domain for which Symantec Messaging Gateway accepts inbound email. You also define a single mail host to which the inbound Scanner routes email addressed to local domains. Any domain that is added during site setup is by default a local domain and uses this static route as its default relay to deliver inbound email.  
See “About email domain acceptance settings” on page 87. |
| **Use reverse DNS as an additional form of sender verification.** | A reverse DNS lookup finds the domain name based on the IP address. Because a reverse DNS lookup enables anyone to view the source of a connection, many bad senders do not have reverse DNS records, or have false reverse DNS records.  
See “Configuring reverse DNS validation” on page 88. |

### About email domains

When inbound mail arrives at a Scanner, Symantec Messaging Gateway verifies that the message is addressed to a valid local domain before accepting it to the appropriate message queue.

You must define any domain for which you want Symantec Messaging Gateway to accept inbound email as a local domain. Symantec Messaging Gateway only accepts inbound email that is addressed to local domains. However, a domain from which you send email can be a local domain or a non-local domain.

Defining more than one domain lets you assign different routing and delivery options to each domain, including TLS encryption for secure delivery, for local or non-local domains. By configuring TLS encryption options for non-local domains, you can secure connections for delivery by external servers.
You can also enable DKIM signing for a local or non-local domain, so that each message sent from that domain will include a DKIM signature that enables DKIM authentication by the receiving MTA.

You can also add non-local domains. You specify non-local domains primarily to route outbound email over established connections to external servers for non-local delivery. You can also define delivery options for non-local domains.

Several features of Symantec Messaging Gateway make use of domain designations.

You can add or edit domains to:

- Create different email acceptance settings for each domain.
  See “About email domain acceptance settings” on page 87.

- Define different delivery options for each domain.
  You can route inbound email addressed to different local domains using an unlimited number of default relays.
  You can designate an directory data routing source for delivery of email that is addressed to specified non-local domains.
  MX Lookup and TLS encryptions options are available for delivery of email that is addressed to non-local domains.
  See “Adding or editing domains” on page 82.

- Configure Recipient Validation to validate recipients of incoming email against your LDAP directory.
  See “About invalid recipients” on page 98.

  **Note:** If you intend to set up probe accounts from invalid recipient email addresses you must check Enable Recipient Validation for the domains you plan to use for probe accounts.
  See “Creating probe accounts from invalid recipient email addresses” on page 318.

- Configure static routing, to route inbound or outbound email to specified mail servers for internal delivery.
  See “Adding or editing domains” on page 82.

- Configure domain-specific delivery bindings for non-local messages. This lets you define one or more IP addresses that messages from a domain are sent from.
  See “SMTP advanced settings for delivery bindings” on page 61.

You can import lists of domains that you then edit individually.

See “Importing a domains list” on page 85.

Typically, a domain is the part of the recipient's email address that follows the @ sign. For example, anywhere.com is the domain for someone@anywhere.com. Domains can include
subdomains. For example, somewhere.anywhere.com is a subdomain of anywhere.com. Alternatively, you can specify a single email address as a domain.

If you want to include all subdomains with a domain, enter a period before the domain. For example, if you want to include all subdomains in example.com, enter .example.com. However, entering a period before the domain omits the domain itself. For example, to accept email that is addressed to example.com and all subdomains of example.com, you must specify both example.com and .example.com.

If you want to include only certain subdomains, you must specify each subdomain separately. For example, you must specify both elsewhere.anywhere.com and somewhere.anywhere.com as separate domains to accept email that is addressed to either subdomain but not overthere.anywhere.com.

Note: A domain can be a fully qualified domain name (FQDN), subdomain, or RFC5321-compliant email address. These levels of granularity allow you maximum control over what addresses are acceptable and how email that is addressed to them are routed.

Adding or editing domains

Local domains are domains and email addresses for which Symantec Messaging Gateway accepts inbound messages. When adding or editing a local domain, you can assign routing behaviors based on MX Lookup, designated hosts, or directory data sources, and enable or disable recipient validation for messages accepted from the domain. You can also import lists of local domains.

Note: If you have provisioned content encryption for your messaging system and add a domain or change the address of a domain, you must inform your Symantec provisioning representative. For more information, see the Symantec Content Encryption Provisioning page. Click Content > Settings > Content Encryption and then click the Click here. You might also need to replace your certificate or certificate bundle to include the domain.

See “Encrypting data with Symantec Content Encryption” on page 449.

Configuring separate local and non-local domains provides you with different routing and delivery options. For example:

- You can route inbound email addressed to different local domains using an unlimited number of default relays.
- You can route outbound mail sent to non-local domains using a non-local default relay for delivery by an external mail host at a subsidiary or business partner.
- You can route outbound email that is addressed to a specified non-local domain to an internal mail server that you reserve for confidential communications.
Non-local domains are typically used to route outbound mail to external mail hosts with which you regularly exchange email. You can also route outbound email that is addressed to a non-local domain to an internal mail host. Because email addressed to non-local domains is first scanned for policy violations, adding non-local domains provides you with options to securely exchange mail with business partners or parts of your own organization whose networks reside behind separate firewalls.

Configure any non-local domains that you add to:

- Static route outbound email addressed to non-local domains to any one of an unlimited number of mail hosts for non-local delivery. You can optionally enable MX Lookup on any non-local domains for which you define a static route. Symantec recommends that you enable MX Lookup for delivery to multiple mail hosts.
- Enable TLS encryption options for specified domains.

**Note:** You can enable routing for a domain once it has been imported by editing the domain name in the Domains list.

You can also query a routing data source to route outbound email addressed to recipients at remote domains.

During site setup, you specify one or more local domains for which the appliance accepts messages. Any domain that you designate during site setup is by default a local domain. Symantec Messaging Gateway only accepts connections from a sender IP when an email is addressed to a local domain. After processing, the Scanner relays any email that does not violate policy conditions or setting limitations to the mail server that hosts the local domain for delivery to recipients.

A mail host that serves as a default relay can host more than one local domain. If only one mail host is specified for local domains, it acts as the default relay for delivery of all inbound mail. You can designate an unlimited number of additional destination servers as default relays for inbound email addressed to local domains.

On the **Protocols > SMTP > Domains** page you can:

- Add more local domains for which you want Symantec Messaging Gateway to accept inbound email.
- Add probe account domains.
    - If you intend to create probe accounts from unused or invalid recipient email addresses, the probe account domain must be added to your list of local domains.
    - If you intend to set up probe accounts from invalid recipient email addresses, you must also enable Recipient Validation for that domain.

See “Setting up probe accounts” on page 316.
Limit inbound mail that is addressed to local domains to valid recipients. Symantec Messaging Gateway checks recipients of email addressed to specified local domains against LDAP directory data before allowing the sender IP to connect to the scanner to inbound email interface. You must configure an appropriate data source, enable the recipient validation function, and enable Invalid Recipient Handling to reject or drop inbound email that is addressed to invalid recipients.

Define different delivery options for separate domains.

To add or edit a domain

1. In the Control Center, click **Protocols > SMTP > Domains**.
2. On the Domains page, click **Add** or click the name of a domain whose settings you want to edit.
3. In **Domain or email address for which to accept inbound mail**, enter a local domain, subdomain, or email address or edit the domain name.
   
   Placing a period in front of the domain enables Symantec Messaging Gateway to accept all subdomains.
4. If you are adding or editing a non-local domain, deselect the **Local domain** checkbox.
5. If you want to require that mail from this domain is sent using TLS encryption, select **Reject mail from this domain if not sent using TLS**.
   
   The **SSL Restrictions** setting on the **Protocols > SMTP > Settings > SMTP** tab affects the TLS versions that SMG can use to encrypt mail from this domain.
   
   See “Specifying SSL restrictions for TLS communications” on page 96.
6. If you wish to reject or drop invalid recipients, or if you are a probe account participant, check **Enable Recipient Validation for this domain**.
   
   You cannot enable recipient validation on an email address or a non-local domain.
   
   Further configurations are required if you want to accept or reject invalid recipient email.
   
   See “Setting up invalid recipient handling” on page 99.
7. To define delivery options for this domain, click the **Delivery** tab.
8. If you wish to have messages addressed to this domain routed via MX lookup, to specific destination servers via host-based routing, or based on directory data, check **Optionally route this domain or email address**.
   
   If you do not check this option, messages are routed to the default relay that you configure under Inbound Local Mail Delivery on the SMTP tab of the Edit Host Configuration page.
9. Choose one of the following options:
   
   - Click **MX Lookup** to route messages to the host indicated by the recipient address using MX lookup.
If you specified a fully qualified domain name or an email address, MX lookup is performed on the specified domain for messages to recipients in that domain. If you specified a subdomain parent, MX lookup is performed on the fully qualified domain name of the recipient address, for messages to recipients in any of the subdomains of the specified parent domain.

- Click **Destination hosts** to specify one or several specific hosts to route messages to, then click **Add** to add each host. Optionally, type a port to which messages addressed to this domain are routed. You can check **MX Lookup** to enable MX lookup for the destination host. You cannot use MX lookup if you specified the host using an IP address. Type a number between 1 and 100, inclusive, under Preference, to indicate the order in which hosts should be used. Lower-numbered hosts are used first. See “Configuring Scanner outbound mail delivery settings” on page 52.

- Click **Directory Data Source** to route messages using directory-based routing for delivery resolution. Choose the LDAP routing source from the accompanying drop-down list.
  
  You must have an LDAP directory data source defined for routing to use this option. See “Creating a data source” on page 496.
  
  See “Creating a routing data source” on page 506.

10 To deliver email to a non-local host using TLS encryption, click **Optional delivery encryption**, then click the radio button that best describes the basis for TLS encryption for this domain.

11 To enable DKIM signing for this domain, use the Domain Key Identified Mail section.
  
  See “Enabling DKIM signing for a domain” on page 123.

12 Click **Save** to add the domain, subdomain, or email address to the list or to confirm your edits.

**Importing a domains list**

You can import a list of domain definitions and email addresses from an ASCII file, similar to the Sendmail `mailertable`. As part of the definition, you can include optional routing information to default local destination hosts.

After import, each domain appears in the list on the **Domains** page. You can then edit any domain as needed. For example, if you want a domain to use TLS encryption or domain key signing, or if you want to use a domain as a non-local domain, you must edit it after you import the domains list.
Note: If you provision content encryption for your messaging system and later add a domain, you must inform your Symantec provisioning representative. For more information, see the Symantec Content Encryption Provisioning page by clicking **Content > Settings > Content Encryption** and then clicking the **Click here**. You may also need to update your certificate to cover the new domains.

See “Encrypting data with Symantec Content Encryption” on page 449.

Note: You can enable directory-based routing for a domain once it has been imported by editing the domain name in the Domains list.

See “Adding or editing domains” on page 82.

You can also enable recipient validation for imported domains. To do this you must also enable Recipient Validation Handling and configure a data source for recipient validation.

See “Setting up invalid recipient handling” on page 99.

See “Creating a recipient validation data source” on page 500.

In the import file, place each domain definition on a line by itself. The domain definition can consist of the following tab-delimited attributes:

- **Domain name**: Can be either a complete domain name, a subdomain name, or an email address. To include all subdomains within a domain, add a period at the beginning of the domain name.

- **Destination**: Consists of destination type and destination host name. Only definitions with a destination type (Mailer) of SMTP or ESMTP are supported, and %backreferences are not supported. After import, ESMTP destination types convert to SMTP. When the host name is enclosed in brackets—smtp:[destination.domain.com]—MX lookup is not performed for the destination host.

- **Validation**: Indicates whether or not recipient validation is enabled for the domain. The value **VALIDATE_RCPTS** in this column enables recipient validation. Any other value or no value will not enable recipient validation. Recipient validation can only be enabled for domains. It cannot be enabled for email addresses.

Here is a sample import file:

```
local1@domain.com    smtp:local1.com
local2@domain.com    smtp:local2.com:20
local3@domain.com    smtp:[local3.com]:30
local4@domain.com    smtp:[local4.com]
.local5.com          smtp:[192.168.248.105]
local6.com           smtp:[192.168.248.106]:60  VALIDATE_RCPTS
```
To import a list of local domains

1. In the Control Center, click Protocols > SMTP > Domains.
2. Click Import.
3. In the Specify the import file text box, enter the filename path or browse to the file containing the list of domain definitions.
4. Click Import.

If entries in the import file do not match the required file format, an error message with a link appears. Click on the link to download a file containing the unprocessed entries.

Deleting domains

You can delete domains to which you no longer want email sent. Deleting a local domain means that the MTA no longer accepts inbound email messages that are addressed to that domain. Deleting a non-local domain means that any routing or TLS options that are configured for that domain no longer operate.

Note: If you delete a local domain, any probe accounts associated with that domain will no longer be valid. Check the active probe accounts before deleting the domain.

See “Adding or editing domains” on page 82.

See “Disabling a probe account” on page 320.

To delete one or more domains

1. In the Control Center, click Protocols > SMTP > Domains.
2. Select one or more domains in the Domains list or click Delete All to delete all listed domains.
3. Click Delete to delete only the domains selected.

About email domain acceptance settings

During site setup, you designate at least one local domain for which Symantec Messaging Gateway accepts inbound email. You also define a single mail host to which the inbound Scanner routes email addressed to local domains. Any domain that is added during site setup is by default a local domain and uses this static route as its default relay to deliver inbound email.

After your site setup is complete, you can further configure inbound email domain acceptance to:

- Reject or drop email addressed invalid recipients at specified local domains.
You must enable recipient validation for any domain for which you want Symantec Messaging Gateway to validate recipients or detect directory harvest attacks.

You configure a domain to validate recipient addresses within a local domain by configuring an LDAP recipient validation profile and enabling recipient validation on a per-domain basis. If recipient validation is enabled for a local domain, Symantec Messaging Gateway checks with the data source to determine that the email address exists in the LDAP directory. If there is no match, any attempted connection is rejected or dropped according to your site’s settings for handling invalid recipients.

Symantec Messaging Gateway accepts all email from internal mail hosts.

**Configuring reverse DNS validation**

You can use reverse DNS as an additional form of sender verification. A reverse DNS lookup finds the domain name based on the IP address. Because a reverse DNS lookup enables anyone to view the source of a connection, many bad senders do not have reverse DNS records, or have false reverse DNS records.

To configure reverse DNS validation

1. In the Control Center, click **Protocols > SMTP > Settings**.
2. On the **SMTP** tab, under **DNS Validation**, check any of the following options:
   - Reject connections where no reverse DNS record exists for the connecting IP address
   - Reject connections where the reverse DNS record exists for the connecting IP address, but the ‘A’ or ‘AAAA’ record of the resulting domain does not match the connecting IP address
   - Reject connections where the domain provided at HELO and EHLO has neither an ‘A’, nor an ‘AAAA’, nor an ‘MX’ record in DNS
   - Reject messages where the domain provided in the MAIL FROM address has neither an ‘A’, nor an ‘AAAA’, nor an ‘MX’ record in DNS
3. Optionally, you can edit the **Reject message** text for any option that you checked.
4. Click **Save**.
Configuring email aliases and address masquerades

You can configure email address aliases, also known as distribution lists, and email address masquerades.

Table 3-3 describes how you can implement address masquerading on inbound mail, outbound mail, or both. You can perform these tasks as needed in any order.

**Table 3-3** Email aliases and address masquerades

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about aliases and address masquerades.</td>
<td>An alias translates an email address into one or more destination addresses. Windows users may understand this concept as a “distribution list.” You can add an alias as a convenient shortcut for typing a long list of recipients. An alias can also translate addresses from one top-level domain to another. Address masquerading is a method of concealing email addresses or domain names behind the mail gateway by assigning replacement values to them. See “About aliases and address masquerades” on page 90.</td>
</tr>
<tr>
<td>Add new aliases or modify existing ones.</td>
<td>Specify one and only one source email address or domain for each alias that you enter. See “Adding or editing aliases” on page 91.</td>
</tr>
<tr>
<td>Import an alias file.</td>
<td>Aliases can be imported from a text file. See “Importing aliases” on page 92.</td>
</tr>
<tr>
<td>Review examples of alias source and destination addresses.</td>
<td>You can enter multiple destination email addresses for each alias that you enter as a source email address. You can only enter a single destination domain, however, for each alias that you enter as a source domain. Alias source addresses must have local domains. Destination domains can be local or non-local domains. See “Alias addresses” on page 92.</td>
</tr>
<tr>
<td>Add a new address masquerade or modify an existing one.</td>
<td>Symantec Messaging Gateway lets you implement address masquerading on inbound mail, outbound mail, or both. See “Adding or editing address masquerades” on page 93.</td>
</tr>
<tr>
<td>Import an address masquerade file.</td>
<td>In addition to creating new masqueraded entries, you can import them from a text file similar to the Sendmail virtusertable. See “Importing an address masquerade list” on page 94.</td>
</tr>
</tbody>
</table>
### About aliases and address masquerades

An alias translates an email address into one or more destination addresses. Windows users may understand this concept as a “distribution list.” You can add an alias as a convenient shortcut for typing a long list of recipients. An alias can also translate addresses from one top-level domain to another. For example, you can create an alias source domain to translate `example.com` to the target domain `example-internetsecurity.com`. Symantec Messaging Gateway then delivers all email that is addressed to `someone@example.com` to `someone@example-internetsecurity.com`.

Address masquerading is a method of concealing email addresses or domain names behind the mail gateway by assigning replacement values to them. Symantec Messaging Gateway lets you implement address masquerading on inbound mail, outbound mail, or both. A typical use of address masquerading is to hide the names of internal mail hosts so that outgoing mail appears to be coming from a different domain than that of the actual host.

Outbound address masquerades change the apparent sender of a message. Inbound address masquerades change the apparent recipient of a message.

Alias translation only applies to inbound or internal messages processed by Symantec Messaging Gateway. Once the gateway allows email to connect to the inbound scanner, it determines whether the address in the SMTP envelope `To:` field is an alias and translates it into any destination addresses during the connection session. Transformed addresses are written back to the SMTP envelope `To:` before the scanner filters the message. The contents of the message `To:` and `Cc:` headers are ignored and not changed.

---

**Note:** If you employ probe accounts along with aliases and address masquerades you may lose one or the other account. Follow the guidelines for creating probe accounts.

See “About creating probe accounts” on page 315.

Inbound address masquerading takes precedence over the alias translation. If the same original email address or domain exists in both the address masquerading list and the aliases list, messages to the source domain are routed to the masqueraded address or domain. Symantec Messaging Gateway does not route the message to the alias address or domain.

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Symantec Messaging Gateway to ignore text casing in addresses.</td>
<td>When you enable this option, the MTA ignores the text case of the local part of addresses for address masquerading, aliases, and probe accounts. See “Ignoring text casing in local addresses” on page 95.</td>
</tr>
</tbody>
</table>
Except where address masquerading applies to a recipient address, you must add the source
domain of an alias to the list of local domains for which Symantec Messaging Gateway accepts
inbound email.

See “Adding or editing domains” on page 82.

Alias translation does not apply to outbound messages that are routed to the Internet.

See “Adding or editing aliases” on page 91.

See “Adding or editing address masquerades” on page 93.

Adding or editing aliases

An alias translates an email address into one or more destination addresses. Specify one and
only one source email address or domain for each alias that you enter. For each destination
address, you can enter a single email address or multiple email addresses separated by
commas, semicolons, or spaces.

See “About aliases and address masquerades” on page 90.

See “Alias addresses” on page 92.

To add an alias
1  In the Control Center, click **Protocols > SMTP > Aliases**.
2  Click Add.
3  On the **Add Aliases** page, type the alias in the **Alias domain or email address** box.
4  Type a domain or one or more destination email addresses in the **Domain or email
addresses for this alias** box.
    You can specify multiple email addresses, or a single domain.
5  Click Save.

To edit an alias
1  In the Control Center, click **Protocols > SMTP > Aliases**.
2  Click an alias.
3  On the **Edit Aliases** page, modify the text in the **Alias domain or email address** box as
desired.
4  Modify the text in the **Domain or email addresses for this alias** box as desired.
5  Click Save.
Importing aliases

Aliases can be imported from a text file. Each address in the text file must be separated with one or more spaces or tabs, or a combination of spaces and tabs. Commas or semicolons are not valid delimiters. In the import file, each line must contain an alias address followed by one or more destination addresses.

Following is a sample import file:

oak@example.com quercus@symantec-internetsecurity.com
ops@example.com tla@example.com bmi@example.com
blockads.com noadsorspam.com

To import aliases:

1. In the Control Center, click **Protocols > SMTP > Aliases**.
2. Click **Import**.
3. In the **Specify the import file** text box, enter or browse to the filename containing the list of aliases.
4. Click **Import**.

If entries in the import file are not specified correctly, do not match the required file format or are duplicates, an error message is displayed. You can click a link to download a file containing the unprocessed entries.

See “About aliases and address masquerades” on page 90.

See “Alias addresses” on page 92.

Click **Cancel** to ignore the unprocessed entries and return to the main Aliases page to review the valid imported entries.

Alias addresses

You can enter multiple destination email addresses for each alias that you enter as a source email address. You can only enter a single destination domain, however, for each alias that you enter as a source domain. Alias source addresses must have local domains. Destination domains can be local or non-local domains.

<table>
<thead>
<tr>
<th>Alias source example</th>
<th>Destination examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:anyone@example.com">anyone@example.com</a></td>
<td><a href="mailto:somebody@example.com">somebody@example.com</a></td>
</tr>
<tr>
<td><a href="mailto:anybody@example.com">anybody@example.com</a></td>
<td><a href="mailto:someone@elsewhere.com">someone@elsewhere.com</a></td>
</tr>
<tr>
<td><a href="mailto:help@example.com">help@example.com</a></td>
<td><a href="mailto:anybody@example.com">anybody@example.com</a>, <a href="mailto:anyone@example.com">anyone@example.com</a>, <a href="mailto:somebody@example.com">somebody@example.com</a></td>
</tr>
</tbody>
</table>
### Alias source example

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>elsewhere.com</td>
</tr>
</tbody>
</table>

**Note:** Except where address masquerading applies to a recipient address, you must add the source domain of an alias to the list of local domains for which Symantec Messaging Gateway accepts inbound email.

See “Adding or editing domains” on page 82.

Aliases are recursive. This means that an alias specified in the destination email address list is expanded as defined in the list of aliases up to 1000 addresses.

In the example shown below, a message addressed to it@example.com would be delivered to the destination addresses for both it@example.com and ops@example.com, because it@example.com includes ops@example.com.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Destination addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:it@example.com">it@example.com</a></td>
<td><a href="mailto:alro@example.com">alro@example.com</a>, <a href="mailto:oak@example.com">oak@example.com</a>, <a href="mailto:ops@example.com">ops@example.com</a></td>
</tr>
<tr>
<td><a href="mailto:ops@example.com">ops@example.com</a></td>
<td><a href="mailto:tla@example.com">tla@example.com</a>, <a href="mailto:bmi@example.com">bmi@example.com</a>, <a href="mailto:map@example.com">map@example.com</a></td>
</tr>
</tbody>
</table>

You cannot add aliases that duplicate aliases already stored. You cannot create an email address alias for a domain. You cannot create a domain alias for an email address. You can only create an email address alias for one or more other email addresses. You can only create a domain alias for one or more other domains.

Both of the aliases shown below are invalid.

<table>
<thead>
<tr>
<th>Alias</th>
<th>Destination addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:it@example.com">it@example.com</a></td>
<td><a href="mailto:alro@example.com">alro@example.com</a>, symantec.com</td>
</tr>
<tr>
<td>example.com</td>
<td><a href="mailto:sample@symantec.com">sample@symantec.com</a></td>
</tr>
</tbody>
</table>

### Adding or editing address masquerades

Address masquerading is a method of concealing email addresses or domain names behind the mail gateway by assigning replacement values to them.

See “About aliases and address masquerades” on page 90.
Warning: If you masquerade a probe address or domain, the probe account will become invalid. Make sure there are no probe accounts associated with an account you masquerade. See “About creating probe accounts” on page 315.

Follow these steps to add or edit masqueraded entries.

To add a masqueraded entry
1 In the Control Center, click Protocols > SMTP > Address Masquerading.
2 Click Add.
3 In the Original address or domain to masquerade box, specify an address or domain to masquerade. The domain name is not case-sensitive.
4 In the New address or domain box, specify a new name for the address or domain name.
5 From the Apply to drop-down list, specify the messages to which this masqueraded name applies: Outbound messages, Inbound messages, or Inbound and outbound messages.
6 Click Save.

To edit a masqueraded entry
1 In the Control Center, click Protocols > SMTP > Address Masquerading.
2 Click the masqueraded address or domain that you want to modify.
3 On the Edit Masqueraded Entry page, modify the masqueraded entry as desired.
4 Click Save.

Importing an address masquerade list
In addition to creating new masqueraded entries, you can import them from a text file similar to the Sendmail virtusertable. In the import file, place each masqueraded address definition on a line by itself. Each address in the file must be separated with one or more spaces or tabs, or a combination of spaces and tabs. Commas or semicolons are not valid delimiters.

Note: You cannot import a file with extended ASCII or non-ASCII characters; you can only import files encoded in US-ASCII format.

The masquerade address definition consists of the following elements:

Original entry  Specifies the original email address or domain name to be masqueraded.
Replacement entry  Specifies the replacement email address or domain name.
Apply to Indicates the direction to which masquerading is applied. Available choices are:
- Inbound messages
- Outbound messages
- Inbound and outbound messages

Following is a sample import file:

```
orig1@domain.com new1@domain.com inbound
orig2@domain.com new2@domain.com outbound
orig3@domain.com new3@domain.com inbound/outbound
orig4@domain.com new4.com inbound
orig5@domain.com new5.com outbound
orig6@domain.com new6.com inbound/outbound
orig7.com new7@domain.com inbound
orig8.com new8@domain.com outbound
orig9.com new9.com inbound/outbound
```

To import a list of masqueraded entries

1. In the Control Center, click **Protocols > SMTP > Address Masquerading**.
2. Click **Import**.
3. In the **Specify the import file** text box, enter or browse to the filename containing the list of masqueraded entries.
4. Click **Import**.

If entries in the import file are not specified correctly, do not match the required file format, or are duplicates, an error message is displayed. You can click a link to download a file containing the unprocessed entries. Click **Cancel** to return to the Address Masquerading page to review the valid imported entries.

Ignoring text casing in local addresses

When you enable this option, the MTA ignores the text case of the local part of addresses for address masquerading, aliases, and probe accounts.

To ignore text casing in local addresses

1. In the Control Center, click **Protocol > SMTP > Settings**.
2. On the **SMTP** tab, under **Address Handling**, check **Ignore the text case of the local part of addresses in Address Masquerading, Aliases, and Domains**.
3. Click **Save**.

See “Configuring email aliases and address masquerades” on page 89.
Specifying SSL restrictions for TLS communications

In Symantec Messaging Gateway version 10.6.5 and later, you can prevent encrypted SMTP communications that use early TLS versions or SSLv3. Some organizations cannot send or accept messages that use SSLv3 or early versions of TLS for encrypted communications. This setting allows SMG to adhere to a higher TLS standard, if needed.

To enable SSL restrictions

1. Select Protocols > SMTP > Settings.
2. On the SMTP tab, in the SSL Restrictions panel, select Disable support for <version> and earlier protocols in all SMTP TLS conversations.
3. From the drop-down menu, select the latest version that you want to disable. For example:
   - Select SSLv3 to disable SSLv3 and limit communications to TLS version 1.0 or later. SSLv3 has serious vulnerabilities, and some organizations do not accept early versions of TLS.
   - To allow encrypted communications that use TLS version 1.1 or later, and disable support for TLS 1.0 or earlier, select TLSv1.0.

4. Click Save.

The following table describes how the SSL Restrictions setting affects different SMG functions. The table also gives the path where you can choose the settings for each function.

Table 3-4 How SSL restrictions affect encryption settings for hosts, domains, and DLP connect

<table>
<thead>
<tr>
<th>Function</th>
<th>Control Center location</th>
</tr>
</thead>
<tbody>
<tr>
<td>The selected Scanner host accepts TLS encrypted connections for inbound mail.</td>
<td>Administration &gt; Hosts &gt; Configuration &gt; Add or Edit Host &gt; SMTP &gt; Inbound &gt; Accept TLS encryption&lt;br&gt;See “Changing Scanner inbound mail settings” on page 46.&lt;br&gt;See “Preparing your system for content encryption” on page 450.</td>
</tr>
<tr>
<td>If a remote MTA offers encryption, the selected Scanner host attempts to send all messages using TLS encryption.</td>
<td>Administration &gt; Hosts &gt; Configuration &gt; Add or Edit Host &gt; SMTP &gt; Advanced Settings &gt; Delivery tab &gt; Attempt TLS encryption for delivery of all messages&lt;br&gt;See “SMTP advanced delivery settings” on page 59.</td>
</tr>
</tbody>
</table>
Table 3-4

How SSL restrictions affect encryption settings for hosts, domains, and DLP connect (continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>Control Center location</th>
</tr>
</thead>
</table>
| The selected Scanner host accepts TLS encrypted connections for outbound mail.                                                              | Administration > Hosts > Configuration > Add or Edit Host > SMTP > Outbound > Accept TLS encryption  
See “Changing Scanner outbound mail settings” on page 50.                                                                                   |
|                                                                                                                                            | See “Preparing your system for content encryption” on page 450.                           |
| The selected Scanner host accepts TLS connections from users who authenticate and connect remotely to use your MTA to send mail.         | Administration > Hosts > Configuration > Add or Edit Host > SMTP > Authentication > Accept TLS encryption  
See “Best practices for using SMTP authentication” on page 110.                                                                               |
|                                                                                                                                            | See “Configuring SMTP authentication mail settings” on page 106.                         |
| Administration > Hosts > Configuration > Add or Edit Host > SMTP > Authentication > Accept TLS encryption gives you the option to require TLS encryption. |                                                                                         |
| ■ If you enable this option and the sender cannot communicate using a TLS version that SMG supports, the message bounces.               |                                                                                         |
| ■ If you disable this option and the sender cannot communicate using a TLS version that SMG supports, SMG accepts an unencrypted connection (not recommended). |                                                                                         |
| The Scanner host attempts or requires TLS encryption for mail that is delivered to the selected domain.                                  | Protocols > SMTP > Domains > Add or Edit Domain > Delivery > TLS Encryption settings > Optional delivery encryption settings  See “Adding or editing domains” on page 82. |
| ■ If you require TLS encryption and the sending server cannot communicate using a TLS version that SMG supports, the message is queued for delivery and may eventually bounce. |                                                                                         |
| ■ If you select Attempt TLS encryption and the sending server cannot communicate using a TLS version that SMG supports, SMG delivers unencrypted messages. |                                                                                         |
| The Scanner host requires TLS encryption for mail that is received from the domain.                                                        | Protocols > SMTP > Domains > Add or Edit Domain > Acceptance > Reject mail from this domain if not sent using TLS  See “Adding or editing domains” on page 82. |
|                                                                                                                                            |                                                                                         |
### About invalid recipients

By default, when an email message arrives addressed to your domain that is not addressed to a valid user, Symantec Messaging Gateway passes the message to the internal mail server. The internal mail server may either accept the message and generate a bounce message, or the internal mail server may reject the message. Upon receiving the bounce message, a legitimate sender can resend the original message with the correct address. However, messages with invalid recipients can also result from a spammer’s directory harvest attack.

**Note:** The **Remove unresolved recipients** action on the Directory Harvest Attacks page only removes unresolved recipients when a directory harvest attack occurs. You can combine this action with your invalid recipient handling setting or enable the two settings individually.

See “Configuring directory harvest attack recognition” on page 149.

You can configure Symantec Messaging Gateway to accept, reject, or drop any messages that are sent to invalid recipients, as follows:

- If you choose to accept all recipients, Symantec Messaging Gateway accepts all messages, whether or not the recipients are valid. However, if the internal mail server rejects a recipient, Symantec Messaging Gateway sends a bounce message. The internal mail server may also send bounce messages if it is configured to send them.

- If you choose to reject invalid recipients, Symantec Messaging Gateway rejects any messages that are addressed to email addresses that do not exist in your LDAP directory. The sending MTA may generate a bounce message to the sender. You must have a data source configured for recipient validation. Recipients are rejected at the initial SMTP conversation with a 5xx SMTP error. See “About using the recipient validation function with your data source” on page 513.

- If you choose to drop invalid recipients, Symantec Messaging Gateway drops from the mail stream any messages that are addressed to email addresses that do not exist in your LDAP directory.
directory. No bounce messages are returned to the sender. You must have a data source configured for recipient validation.

- If you choose to reject or drop invalid recipients, Symantec Messaging Gateway applies your choice to each local domain that you configure to enable recipient validation. If you do not enable recipient validation for any local domains, no messages are dropped or rejected.

See “Adding or editing domains” on page 82.

**Warning:** Dropping messages for invalid recipients is an extreme measure. Enabling this feature may prevent diagnosis of serious problems with your email configuration. Only enable this feature after you are sure that your email system is stable. Also, if enabled, accidentally mis-addressed messages are dropped, and no bounce messages are sent. You can instead reject invalid recipients, which allows the sending MTA to generate a bounce message if so configured.

See “Setting up invalid recipient handling” on page 99.

**Setting up invalid recipient handling**

You can set up invalid recipient handling to accept all recipients, or to drop or reject invalid recipients. If you choose to drop or reject invalid recipients, you then must enable invalid recipient validation on a per-domain basis.

You must configure a directory data source for recipient validation before choosing to reject or drop invalid recipients.

**Note:** If you chose to **Reject** or **Drop** invalid recipient mail, you must enable recipient validation for that domain.

See “Adding or editing domains” on page 82.

**Warning:** Dropping messages for invalid recipients is an extreme measure. Enabling this feature may prevent diagnosis of serious problems with your email configuration. Only enable it after you are sure that your email system is stable. Also, if enabled, accidentally mis-addressed messages are dropped, and no bounce message are sent. You can instead reject invalid recipients, which allows the sending MTA to generate a bounce message if so configured.

**To set up invalid recipient handling**

1. In the Control Center, click **Protocols > SMTP > Invalid Recipients**.
2. Do one of the following:
Click **Accept all recipients** to accept all messages, whether or not the recipients are valid. Bounce messages are sent if your internal mail server is configured to send bounce messages or to reject invalid recipients.

Click **Reject invalid recipients** to reject any messages that are addressed to the user names that do not exist in your LDAP directory. The sending MTA may generate a bounce message to the sender if configured to do so. You must configure a directory data source for recipient validation to reject invalid recipients. Recipients are rejected at the initial SMTP conversation with a 5xx SMTP error.

Click **Drop invalid recipients** to drop any messages that are addressed to the user names that do not exist in your LDAP directory from the mail stream. No bounce messages are returned to the sender. You must have an LDAP source configured for recipient validation to use this setting. This setting is independent of action you specify using the Directory Harvest Attacks page, but it can be used with that action.

3 Click **Save**.

See “Adding a data source” on page 496.

## About email message flow

Understanding exactly what happens to an email message during processing can help you to configure your system optimally and troubleshoot any problems that arise. Symantec Messaging Gateway lets you manage the SMTP (Simple Mail Transfer Protocol). This topic provides an overview of the message flow for SMTP.

Email policies and SMTP settings can apply to both the inbound and outbound message flow. Some policies and settings, such as those covered by Brightmail Adaptive Reputation Management, address issues unique to inbound message flow. Content filtering policies, on the other hand, address the data loss prevention and regulatory compliance issues that most often affect outbound message flow.

---

**Warning:** Symantec Messaging Gateway allows you to configure various MTA configuration parameters to manage your email message flow. If you relay messages to other MTAs, some settings for these MTAs may conflict with Symantec Messaging Gateway settings. For example, you configure maximum message size for 10 MB, and your local relay MTA has a maximum of 1 MB. Such conflicts can result in errors that are difficult to diagnose.

See “About blocking and allowing messages at connection time” on page 141.

See “About content filtering” on page 322.

See “Email message flow phases” on page 101.
Note: You can vary the number of times Symantec Messaging Gateway scans a potentially malformed message. See “Configuring bad message handling” on page 53.

Email message flow phases

Symantec Messaging Gateway processes an email message in the following phases:

- **Phase 1, SMTP connection** – During the connection phase Symantec Messaging Gateway accepts connections from legitimate senders, unless a specific policy or setting requires rejection or deferral. All of the actions that are taken during this phase are based on the IP address alone. Symantec Messaging Gateway rejects connection attempts from any IP addresses that are not permitted by a Scanner’s SMTP settings. For inbound connections from IP addresses that appear in IP-based bad sender groups, Symantec Messaging Gateway rejects the SMTP connection, unless a different action is configured for the group. Based on Connection Classification limits, some connections are deferred. See “Changing Scanner inbound mail settings” on page 46. See “About managing connection load at the gateway” on page 143.

- **Phase 2, SMTP session** – During the SMTP session, Symantec Messaging Gateway accepts, rejects, or defers messages on the basis of the message envelope. It also checks Connection Classification settings and SMTP settings to determine whether accepting the message exceeds the configured limits. See “Changing Scanner inbound mail acceptance settings” on page 47.

- **Phase 3, Message filtering** – After the Scanner accepts a message, Symantec Messaging Gateway evaluates the message content and renders verdicts. It evaluates the message content based on applicable policies and settings, including, if required, content filtering policies. Based on the verdicts, it applies the configured actions. See “How Symantec Messaging Gateway works” on page 27.

- **Phase 4, Message routing** – Symantec Messaging Gateway routes messages that have not been quarantined or held for review to a mail host. The route is determined by Domains Delivery settings and the Scanner’s Local Mail Delivery and Non-local Mail Delivery settings. See “About email domains” on page 80.

- **Phase 5, Message delivery** – Symantec Messaging Gateway enforces limits on the number of connections to internal mail servers. If the address binding settings are configured to specify the IP addresses that deliver email, Symantec Messaging Gateway uses the specified IP addresses. See “Configuring Scanner inbound email delivery settings” on page 48.

Figure 3-1 illustrates the inbound message flow.
Configuring email for SMTP authentication

SMTP authentication allows an MTA to authenticate an email client before you permit it to send messages.
Table 3-5 lists the tasks that can help you configure your SMTP authentication. You can perform any of these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about Symantec Messaging Gateway SMTP authentication.</td>
<td>You can use SMTP authentication to permit remote users to send email through Symantec Messaging Gateway. A typical use of SMTP authentication is to allow authorized users to relay mail. SMTP authentication is a service extension to the ESMTP protocol. This topic also lists the support MUAs for SMTP authentication and MTAs. It also describes the methods that you can use for authenticating user credentials. See “About using SMTP authentication” on page 103.</td>
</tr>
<tr>
<td>Set up the SMTP authentication.</td>
<td>This topic gives you the process to set up your SMTP authentication. See “How to set up SMTP authentication” on page 104.</td>
</tr>
<tr>
<td>Configure the appropriate mail settings.</td>
<td>You can set up SMTP authentication to enable users who connect remotely to send messages from Symantec Messaging Gateway. See “Configuring SMTP authentication mail settings” on page 106.</td>
</tr>
<tr>
<td>Review the best practices for Symantec Messaging Gateway SMTP authentication.</td>
<td>This topic provides Symantec’s recommendations to help ensure your SMTP authentication works properly. See “Best practices for using SMTP authentication” on page 110.</td>
</tr>
</tbody>
</table>

About using SMTP authentication

You can use SMTP authentication to allow remote users to send email via Symantec Messaging Gateway. A typical use of SMTP authentication is to allow authorized users to relay mail.

SMTP authentication is a service extension to the ESMTP protocol. For more information on SMTP authentication, see RFC 4954: https://www.ietf.org/rfc/rfc4954.txt

Many email clients, also known as Mail User Agents (MUAs), support SMTP authentication. Supported clients allow users to provide appropriate credentials to enable SMTP authentication. Symantec Messaging Gateway has been tested against versions of the following MUAs for SMTP authentication:

- Outlook 2013 (March 2013)
- Outlook 2010
- Outlook 2007
Symantec Messaging Gateway provides two methods for authenticating user credentials supplied for SMTP authentication. You can use an LDAP authentication source, or you can forward the credentials supplied by the MUA to another SMTP server for authentication.

Symantec Messaging Gateway supports SMTP authentication via LDAP using simple bind for all supported LDAP directory types. For SMTP authentication via LDAP using password fetching, all supported directory types except Active Directory, Active Directory Global Catalog, and Domino are supported.

**Note:** Symantec Messaging Gateway searches all of your authentication directory data sources for a user attempting to authenticate. If the user exists in more than one authentication directory data source, SMTP authentication fails.

See “About data sources and functions” on page 499.

For SMTP authentication via SMTP forwarding to an SMTP server, Symantec Messaging Gateway has been tested against servers hosting versions of the following MTAs:

- Exchange
- Domino
- Sendmail

**Warning:** If not configured correctly, with appropriate security safeguards, use of SMTP authentication can expose your system to significant security threats. Be sure to take appropriate steps to protect your users, systems, and data when you configure SMTP authentication.

See “Best practices for using SMTP authentication” on page 110.

To use SMTP authentication, follow the set up process. See “How to set up SMTP authentication” on page 104.

**How to set up SMTP authentication**

Table 3-6 describes the process to set up email for SMTP authentication.
### Table 3-6  Setting up email for SMTP authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1**<br>Required | Choose your authentication source. | You can use either an LDAP server or an SMTP server as your authentication source.  
If you choose an LDAP server, you must have or create a directory data source for authentication. See the links in step 5 for more information.  
If you choose SMTP forwarding, you must provide details for an SMTP server that supports SMTP authentication. This server cannot be another Symantec Messaging Gateway appliance. Skip step 2 and see the link in step 3 for more information.  
**Note:** Using SMTP forwarding may have an adverse impact on mail processing performance. |
| **Step 2**<br>Required if you choose LDAP | Choose your authentication method. | You can authenticate user passwords using either simple bind or password fetching.  
If you do not create a custom LDAP query, Symantec Messaging Gateway defaults to using simple bind. If you want to use password fetching you must create a custom LDAP query.  
See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.  
Symantec Messaging Gateway supports SMTP authentication via LDAP using simple bind for all supported LDAP directory types. For SMTP authentication via LDAP using password fetching, all supported directory types except Active Directory, Active Directory Global Catalog, and Domino are supported. |
| **Step 3**<br>Required | Configure SMTP authentication mail settings. | Enable authentication and provide key authentication details, including whether you will authenticate client credentials via LDAP or via SMTP forwarding.  
You must use an IP address/port combination for SMTP authentication that is different from both your inbound and outbound IP address/port combinations.  
See “Configuring SMTP authentication mail settings” on page 106. |
### Configuring SMTP authentication mail settings

You can set up SMTP authentication to enable users who connect remotely to send messages from Symantec Messaging Gateway.

You can also configure alerts for SMTP authentication login failures.

See “Configuring alerts” on page 688.

**To configure SMTP authentication mail settings**

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. Check the Scanner whose settings you want to modify and click **Edit**.
3. On the **Edit Host Configuration** page, click the **SMTP** tab.
To view the Authentication Mail Settings tab, enable either **Outbound mail filtering only** or **Inbound and Outbound mail filtering**.

Click the **Authentication** tab.

Under **Authentication Mail Settings**, click **Enable Authentication**.

In the **Authentication mail IP address** drop-down menu, select the IP address for which you want to authenticate users.

The available choices are the Ethernet interface and virtual interfaces that are available on the selected Scanner.

Either leave the default port assignment of 587, or enter a new port in the **Port** field.

The port you assign here is the port that you either configure mail clients to access or instruct users to configure in their mail clients.

You must use an IP address/port combination for SMTP authentication that is different from both your inbound and outbound IP address/port combinations.

For more information, see the following RFC:

4954

Optionally, select an IPv6 address from the **Optional Authentication mail IPv6 address** drop-down list.

You can select any IPv6 address that is configured for the Ethernet interface on the selected Scanner.

Either leave the default port assignment of 587, or enter a new port in the **Port** field.

The port you assign here is the port that you either configure mail clients to access or instruct users to configure in their mail clients.

You must use an IP address/port combination for SMTP authentication that is different from both your inbound and outbound IP address/port combinations.

Check **Accept TLS encryption** if you want the host to accept connections using TLS encryption.

If you leave this option unchecked, Symantec Messaging Gateway does not advertise support for TLS encryption during the SMTP session.

- You must configure an MTA TLS certificate and assign it to this Scanner before it can accept TLS encrypted outbound mail for filtering.
  
  See “Assigning an MTA TLS certificate to a Scanner” on page 185.

- The **SSL Restrictions** setting on the **Protocols > SMTP > Settings > SMTP** tab affects the TLS versions that Symantec Messaging Gateway accepts.
  
  See “Specifying SSL restrictions for TLS communications” on page 96.
11. Select the name of a certificate from the drop-down menu to authenticate the Scanner as a trusted source to clients sending over TLS-encrypted connections.

See “About certificates” on page 169.

12. Check **Request client certificate** if you want the scanner to request a TLS encryption certificate from a sender before accepting a TLS-encrypted connection.

13. Check **Require TLS encryption** to allow only TLS-encrypted connections.

---

**Warning:** Symantec strongly recommends that you require TLS encryption when enabling SMTP authentication.

See “Best practices for using SMTP authentication” on page 110.

---

14. Under **Authentication Source**, click either **LDAP server** or **SMTP forwarding**.

If you choose **LDAP server** you must have a directory data source defined for authentication.

See “About using SMTP authentication” on page 103.

If you chose **LDAP server**, skip the next step.

If you chose **SMTP forwarding**, you must have a host running an MTA that supports SMTP authentication.

15. If you chose **SMTP forwarding**, specify the following: SMTP server, host, port, and TLS services you want to use.

- Specify the IP address or host name in the **Host** field, and specify a **Port**.

- Optionally for **Binding**, you can either choose **Auto** or choose a specific IP address. Symantec Messaging Gateway sends the message to the SMTP server from the IP address you choose.

- Under **TLS**, select one of the following:

  - **Do not attempt TLS encryption**: Select this option for unencrypted communication with the SMTP server.
  
  - **Attempt TLS encryption**: Select this option to attempt TLS-encrypted communication. If the SMTP server does not support TLS, communication is unencrypted.
  
  - **Require TLS encryption and don't verify certificate**: Select this option to abort communication if the SMTP server does not support TLS, without verifying the SMTP server certificate.
Require TLS encryption and verify certificateSelect this option to abort communication if the SMTP server does not support TLS, or if the SMTP server certificate cannot be successfully verified.

- If you use TLS, optionally check **Offer TLS client certificate** and choose the certificate you want to use.

---

**Warning:** Symantec strongly recommends that you require TLS encryption when using SMTP forwarding.

**Warning:** Do not specify another Symantec Messaging Gateway appliance as the SMTP server for SMTP forwarding.

See “Best practices for using SMTP authentication” on page 110.

**16** Under **Authentication Mail Connections**, select one of the following options:

- **Accept authenticated mail connections from all IP addresses** Select this option if the users who connect through SMTP authentication frequently travel.
  
  Skip to 18.

- **Accept authenticated mail connections from only the following IP addresses** Select this option if users consistently connect from the same IP addresses. This option provides better security.
  
  Then in the list, check the IP addresses from which you want this Scanner to accept authenticated mail.
  
  Proceed to the next step.
17 Optionally, do any of the following tasks:

- **To manually add an IP address**: Click **Add** and type the host name or IP address of a local domain from which you want to accept authenticated mail connections. You can enter a range of IP addresses using the CIDR format.

- **To edit an IP address**: Check the host name or IP address of the email client whose settings you want to change, click **Edit**, then make the necessary changes.

- **To delete one or more IP addresses**: Check the addresses or domains from which you no longer want to accept authenticated mail connections, and click **Delete** to delete them from the list. To delete all of the existing addresses or domains, click **Delete All**.

- **To import IP addresses**: Click **Import**, browse to the file location, and click **Import**. You can import files with comma, semicolon, space, and tab delimiters.

- **To export IP addresses**: Click **Export** and specify the name of the export file and location where you want to save it.

18 Click **Save** or check **Apply above settings to all Scanners** and then click **Save**.

### Best practices for using SMTP authentication

You can use SMTP authentication to allow remote users to send email using your MTA. Using SMTP authentication can introduce increased security risks if appropriate steps are not taken to ensure secure communications.

Symantec strongly recommends that you implement the following best practices if you are using SMTP authentication:

- **Require TLS encryption for SMTP authentication.**
  See “Configuring SMTP authentication mail settings” on page 106.

- **If you use SMTP forwarding, require TLS encryption for SMTP forwarding.**

- **Do not attempt to use another Symantec Messaging Gateway appliance as your SMTP server for SMTP forwarding.** SMTP forwarding is only performed over IPv4 addresses.

- **When configuring SMTP authentication mail settings, do not choose to accept authenticated mail connections from all IP addresses.** Instead, specify a list of IPv4 and/or IPv6 addresses. This best practice may not be feasible for all organizations.

- **Configure and enable outbound filtering policies that protect against spam.**
  See “Creating the policies that detect spam and unwanted email” on page 256.

- **Configure alerts for SMTP authentication login failures.**
  See “Configuring alerts” on page 688.
Specifying address validation criteria

You can specify the criteria that email message addresses should have to be validated. Specifically, you can specify the characters that are permitted in addresses.

To specify address validation criteria

1. In the Control Center, click Protocols > SMTP > Settings.
2. On the SMTP tab, under Address Validation, select the criteria you want to implement as follows:

   - ** Allow email addresses to contain the percent character**
     Permits an email address to contain the percent sign.
     This option is useful for legacy the systems that allow this symbol as a part of an email address.

   - ** Allow email addresses to start with a dash**
     Lets an address to have minus sign as the first character.
     When you select this option, Symantec Messaging Gateway accepts email to any address that starts with the "-" character. When unchecked, Symantec Messaging Gateway rejects email to any recipient address starting with the "-" character.

   - ** Allow 8-bit characters in email addresses**
     Permits an email address that contains 8-bit characters.
     See “Converting 8-bit MIME messages to 7-bit MIME” on page 677.

   - ** Remove subaddress in recipient validation directory query**
     Provides support for subaddressing in recipient validation.
     Subaddressing consists of additional text in the local portion of an email address (the part before the @), that follows a plus sign or a minus sign. When you select this option, Symantec Messaging Gateway removes the +detail or -detail portion of the email address before it completes an LDAP recipient validation query.

     **Note:** If you use plus or minus signs in email addresses for any purpose other than subaddressing, enabling this feature can cause recipient validation errors.

     See “Creating a recipient validation data source” on page 500.

3. Click Save.
Setting up email sender authentication

This chapter includes the following topics:

- How sender authentication works
- Setting up sender authentication for inbound mail
- Setting up sender authentication for outbound mail
- Enabling DKIM signing for a domain

How sender authentication works

Spammers often attempt to forge the mail server name, the sending domain, or other metadata in email messages to evade detection. SMG offers multiple sender authentication options to detect these forgeries. You can enable any of the following options on the Spam > Settings > Sender Authentication page:

- **SPF** checks the domain of the envelope sender against the published DNS record.
- **Sender ID** checks the domain of the message header "From" address against the published DNS record. Sender ID is less effective than SPF because the "From" address is easier to forge than the envelope sender.
- **DKIM** uses a private domain key to sign the domain's outgoing mail headers and message bodies. The sender adds the matching public key to the domain's DNS records. The mail server that receives the message uses the public key to compare the original signatures and received signatures in the email headers and body. If the signatures match, the message passes DKIM authentication.
- **DMARC** uses SPF and DKIM to authenticate email messages, but adds mechanisms for senders and receivers to share information about the results. Domains that send email
messages can publish their DMARC policies in their DNS TXT records. Recipients can check the results of SPF and DKIM authentication against the senders’ published policies. The recipients can then use the published policies to determine what to do with any messages that don't align.

**Note:** If you did not deploy SMG at the gateway, DMARC and DKIM results are useful, there is no result for SPF. SMG does not perform SPF validation when the connecting IP address is internal.

DMARC allows senders to request reports on non-aligned messages and gives a mechanism for receivers to provide the reports. These reports make both parties aware when a domain is spoofed.

**Note:** Symantec Email Fraud Protection is a cloud service that helps customers implement the DMARC standard to prevent attackers from spoofing their domain names. Email Fraud Protection is offered as an add-on for Symantec Messaging Gateway. Customers who purchase the service point their DMARC, SPF, and DKIM records to the Email Fraud Protection platform, which responds to authentication requests in real time and ensures that email sent using the customer’s domain name is authorized. For information about how Email Fraud Protection works, see the service’s online help at [https://help.symantec.com/home/FRAUD_PRO?locale=EN_US](https://help.symantec.com/home/FRAUD_PRO?locale=EN_US).

You can choose to perform sender authentication on inbound mail to all domains. This setting provides the most security, but requires more processing. As an alternative, you can create a list of domains for special treatment. You can then choose to either exclude the listed domains from sender authentication or perform sender authentication only on the listed domains.

When you enable an authentication method, SMG inserts an Authentication-Results header in each inbound message that it scans. This header contains the scan results for that method. The results are based on the published standards for each protocol.

The sender authentication results also appear in the message audit log. For example:

```
DKIM|permfail (body hash did not verify)|newsletters.stream|dkim
```

To process the messages that fail sender authentication, SMG provides default content filtering policies for the most common DKIM, DMARC, Sender ID, and SPF verdicts. These policies are enabled by default, and you can customize them to meet your organization's requirements. You must assign the content filtering policies to policy groups, however, before SMG can use them to process messages.

When a sender authentication result triggers a content filtering policy, the message audit log records a verdict. The log entry includes the violation that triggered the policy and the action that Symantec Messaging Gateway performed on the message. For example:
Setting up email sender authentication

Setting up sender authentication for inbound mail

Inbound sender authentication detects when spammers attempt to forge the mail server name, the sending domain, or other metadata in the email messages your users receive. SMG offers SPF, Sender ID, DKIM, and DMARC sender authentication options to provide comprehensive spam detection.

Note: Symantec Email Fraud Protection is a cloud service that helps customers implement the DMARC standard to prevent attackers from spoofing their domain names. Email Fraud Protection is offered as an add-on for Symantec Messaging Gateway. Customers who purchase the service point their DMARC, SPF, and DKIM records to the Email Fraud Protection platform, which responds to authentication requests in real time and ensures that email sent using the customer’s domain name is authorized. For information about how Email Fraud Protection works, see the service’s online help at https://help.symantec.com/home/FRAUD_PRO?locale=EN_US.

To set up inbound sender authentication

1. Set up the sender authentication methods that you want to use for spam detection.
   
   Table 4-1 summarizes how to set up SPF, Sender ID, DKIM, and DMARC authentication for inbound mail. You enable each authentication method that you want to SMG to use on the Spam > Settings > Sender Authentication page. Then you assign the related content filtering policies to your policy groups. These content filtering policies are located on the Content > Policies > Email > Email Content Filtering Policies page.

   When a message fails sender authentication, SMG process the message according to the policy that matches the authentication method and failure condition.

   See “Content filtering policies for sender authentication” on page 117.

2. Select which external domains to test.

   Sender authentication uses significant processing resources, but it is most effective against spam when SMG authenticates inbound messages from all domains. When you select a Domain Authentication setting, you decide how to balance spam protection against performance for your particular installation.

   See the section called “Selecting domains for sender authentication” on page 116.
### Table 4-1 Inbound sender authentication setup instructions

<table>
<thead>
<tr>
<th>Sender authentication method</th>
<th>Inbound implementation steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SPF</strong></td>
<td>1. On the <strong>Spam &gt; Settings &gt; Sender Authentication</strong> page, in the <strong>Authentication Types</strong> panel, enable SPF.</td>
</tr>
<tr>
<td></td>
<td>2. On the <strong>Content &gt; Policies &gt; Email &gt; Email Content Filtering Policies</strong> page, assign policy groups to the related content filtering policies, to process messages that do not pass SPF validation.</td>
</tr>
<tr>
<td><strong>Sender ID</strong></td>
<td>1. On the <strong>Spam &gt; Settings &gt; Sender Authentication</strong> page, in the <strong>Authentication Types</strong> panel, enable <strong>Sender ID</strong>. When you enable Sender ID, SMG also enables SPF because when SMG authenticates the Sender ID with DNS, the process also provides SPF authentication.</td>
</tr>
<tr>
<td></td>
<td>2. On the <strong>Content &gt; Policies &gt; Email &gt; Email Content Filtering Policies</strong> page, assign policy groups to the related content filtering policies, to process the messages that do not pass Sender ID validation.</td>
</tr>
<tr>
<td><strong>DKIM</strong></td>
<td>1. On the <strong>Spam &gt; Settings &gt; Sender Authentication</strong> page, in the <strong>Authentication Types</strong> panel, enable <strong>DKIM</strong>. 2. You can also change the Maximum number of DKIM signature validations to any number between 1 and 20, inclusive. When the <strong>Maximum number of DKIM signature validations</strong> is exceeded for a single message, Symantec Messaging Gateway stops DKIM validation for that message. Additional signatures are ignored. If any DKIM signature passes, the message passes DKIM validation. If no signature passes when the <strong>Maximum number of DKIM signature validations</strong> is reached, the message fails DKIM validation.</td>
</tr>
<tr>
<td></td>
<td>3. On the <strong>Content &gt; Policies &gt; Email &gt; Email Content Filtering Policies</strong> page, assign policy groups to the related content filtering policies, to process the messages that do not pass DKIM validation.</td>
</tr>
<tr>
<td><strong>DMARC</strong></td>
<td>1. On the <strong>Spam &gt; Settings &gt; Sender Authentication</strong> page, in the <strong>Authentication Types</strong> panel, enable <strong>DMARC</strong>. 2. In the <strong>DMARC Reporting Settings</strong> panel, select DMARC reporting options. See “Enabling DMARC reporting” on page 121.</td>
</tr>
<tr>
<td></td>
<td>3. On the <strong>Content &gt; Policies &gt; Email &gt; Email Content Filtering Policies</strong> page, assign policy groups to the related content filtering policies, to process the messages that do not pass DMARC validation.</td>
</tr>
</tbody>
</table>
Selecting domains for sender authentication

Symantec recommends that you perform sender authentication on all sender domains. However, the **Domain Authentication** settings let you create a list of sending domains and then choose to include or exclude the domains from sender authentication. When SMG receives a message, it checks the domain of the envelope sender against the list to determine whether or not to perform the sender authentication checks that you enabled.

**To select which sender domains to authenticate**

1. In the **Domain Authentication** panel:
   - Select **Authenticate all domains** to perform sender authentication on inbound mail from all domains. Then click **Save**. **Authenticate all domains** provides the most effective spam protection, but has the greatest effect on performance.
   - Select **Authenticate only the following domains** to perform sender authentication on inbound mail that appears to originate from the listed domains. Then go to Step 2 to build the domain list. This option affects performance the least, but provides the least effective spam protection.
   - Select **Authenticate all domains except the following domains** to exclude the listed domains from sender authentication. Then go to Step 2 to build the domain list. When you select this option, SMG does not test any inbound messages that appear to come from these domains. You can use this option to prevent SMG from testing the sending domains that are known to be safe, which may improve performance.

2. Build the domain list to authenticate or exclude domains from authentication. SMG provides a default list of domains.
   - To add a new domain to the list, click **Add**. Type a domain name in the text field and click **Save**.

   **Note:** Symantec Messaging Gateway performs exact matches against the domains that you add. For example, if you add the top domain, SMG does not automatically match the subdomains. You must explicitly add each subdomain that you also want to match. You cannot use wildcards.

   - To edit the spelling of a domain, select the domain and click **Edit**. Make changes and click **Save**.
   - To delete a domain from the list, select the domain and click **Delete**.

3. Click **Save**.
Content filtering policies for sender authentication

Beginning with version 10.6.5, Symantec Messaging Gateway uses content filtering policies to process messages that fail sender authentication. The following table describes the default content filtering policies for sender authentication on the Content > Policies > Email > Email Content Filtering Policies page. These policies are enabled by default and they apply to inbound messages only.

You assign these policies based on which authentication options you enable on the Spam > Settings > Sender Authentication page. You must assign them to your policy groups before SMG can use the policies to process message that fail sender authentication. To process messages based on different failure conditions, SMG provides multiple content filtering policies for each authentication method. The table includes recommendations for when to assign each policy.

---

**Note:** Symantec Email Fraud Protection is a cloud service that helps customers implement the DMARC standard to prevent attackers from spoofing their domain names. Email Fraud Protection is offered as an add-on for Symantec Messaging Gateway. Customers who purchase the service point their DMARC, SPF, and DKIM records to the Email Fraud Protection platform, which responds to authentication requests in real time and ensures that email sent using the customer’s domain name is authorized. For information about how Email Fraud Protection works, see the service’s online help at [https://help.symantec.com/home/FRAUD_PRO?locale=EN_US](https://help.symantec.com/home/FRAUD_PRO?locale=EN_US).
### Table 4-2  Default policies for sender authentication

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Default conditions to trigger the policy</th>
<th>Default actions</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| Sender Authentication: DMARC, SPF, SenderID Failure: Delete | The message header includes one of the following:  
- Authentication Results: DMARC = Fail: reject  
- Authentication Results: SPF = Fail And Authentication Results: DMARC = None  
- Authentication Results: SENDERID = Fail And Authentication Results: DMARC = None | Delete message           | Assign this policy to your policy groups if you enabled DMARC sender authentication. This policy processes messages that:  
- Fail DMARC authentication, and the sender's published policy is to reject these messages (p-reject).  
- Fail SPF authentication, and the sender's published policy is none (p=none).  
- Fail Sender ID authentication, and the sender's published policy is none (p=none).  
By default, the Subsequent Content Filter Handling setting for this policy is Provide Incidents and Notifications Actions Only, because the default action is to delete the message.  
Make sure that you evaluate the effects of the Subsequent Content Filter Handling if you change the policy action or move the policy to a different position in the list. At the default setting, SMG performs only incidents and notifications actions for policies that are lower in the list. |
<table>
<thead>
<tr>
<th>Policy name</th>
<th>Default conditions to trigger the policy</th>
<th>Default actions</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender Authentication: DMARC Failure: Quarantine</td>
<td>The message header includes: Authentication Results: DMARC = Fail: quarantine</td>
<td>Hold message in Spam Quarantine</td>
<td>Assign this policy to your policy groups if you enable DMARC sender authentication. This policy processes messages that fail DMARC authentication, and the sender's published policy is to quarantine these messages (p-quarantine).</td>
</tr>
<tr>
<td>Sender Authentication: DKIM Failure: Modify subject line with &quot;[DKIM Failure]&quot;</td>
<td>The message header includes: Authentication Results: DKIM = Fail</td>
<td>Prepend subject line with &quot;[DKIM Failure] &quot;</td>
<td>Assign this policy to your policy groups if you enable DKIM sender authentication, but you do not enable DMARC. If you enable DMARC and assign DMARC policies to your policy groups, you do not need to assign this policy. A DKIM failure triggers a DMARC failure.</td>
</tr>
<tr>
<td>Sender Authentication: SPF, SenderID Failure: Modify subject line with &quot;[Sender Auth Failure]&quot;</td>
<td>The message header includes one of the following: - Authentication Results: SPF = Fail - Authentication Results: SENDERID = Fail</td>
<td>Prepend subject line with &quot;[Sender Auth Failure] &quot;</td>
<td>Assign this policy to your policy groups if you enable SPF or Sender ID authentication, but you do not enable DMARC. If you enable DMARC and assign DMARC policies to your policy groups, you do not need to assign this policy. An SPF or Sender ID failure triggers a DMARC failure.</td>
</tr>
</tbody>
</table>
Table 4-2  Default policies for sender authentication (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Default conditions to trigger the policy</th>
<th>Default actions</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender Authentication: SPF Softfail:</td>
<td>The message header includes: Authentication Results: SPF = Softfail</td>
<td>Prepend subject line with &quot;[SPF Softfail] &quot;</td>
<td>Assign this policy to your policy groups if you enable SPF authentication, but you do not enable DMARC. If you enable DMARC and assign DMARC policies to your policy groups, you do not need to assign this policy.</td>
</tr>
<tr>
<td>Modify subject line with &quot;[SPF Softfail]&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Authentication: SenderID Softfail:</td>
<td>The message header includes: Authentication Results: SENDERID = Softfail</td>
<td>Prepend subject line with &quot;[SenderID Softfail] &quot;</td>
<td>Assign this policy to your policy groups if you enable Sender ID authentication, but you do not enable DMARC. If you enable DMARC and assign DMARC policies to your policy groups, you do not need to assign this policy.</td>
</tr>
<tr>
<td>Modify subject line with &quot;[SenderID Softfail]&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender Authentication: Validation error:</td>
<td>The message header includes one of the following:</td>
<td>Prepend subject line with &quot;[SenderAuthentication Validation Error] &quot;</td>
<td>Assign this policy to your groups when you enable any sender authentication option. This policy processes messages when SMG encounters a temporary error condition for DMARC, SPF, DKIM or Sender ID. For example, a DNS timeout during the authentication check triggers a <em>temperror</em> condition. This policy also processes authentication failures due to a permanent error. For example, a DNS record with an invalid structure triggers a <em>permerror</em> condition.</td>
</tr>
<tr>
<td>Modify subject line with &quot;[SenderAuthentication Validation Error]&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enabling DMARC reporting

When you set up DMARC sender authentication for inbound mail on the Spam > Settings > Sender Authentication page, you can also enable DMARC failure reports. SMG emails a failure report to the domain of the sender whose message failed DMARC validation.

To enable DMARC reporting

1. In the SMG Control Center, select Spam > Settings > Sender Authentication.

You can also limit the external domains whose messages you want SMG to check, or allow SMG to perform sender authentication for all domains.

See “Setting up sender authentication for inbound mail” on page 114.

3. In the DMARC Reporting Settings panel, select Enable Failure Reports.
4. In the Sender Address field, type the email address from which the failure reports appear to be sent. The Sender Address must be a valid address on your email system.

SMG sends failure reports only to domains that supply an email address in their DMARC DNS records. If a failure report can't be delivered to a domain that supplies an address, your Sender Address mailbox receives a bounceback message.

- If you want to monitor when failure reports can't be delivered, enter an administrator address as the Sender Address.
- If you do not want to monitor these delivery failures, enter the address of an email account that is not monitored.

SMG does not keep copies of the failure reports that it sends.

5. Click Save.

The DMARC DNS record of the sender's domain must request forensic reports and must supply an email address to receive these failure reports.

Refer to Anatomy of a DMARC resource record in the DNS at https://dmarc.org/overview

For more information about DMARC failure reports, visit https://tools.ietf.org/html/rfc7489#section-7.3

Setting up sender authentication for outbound mail

Outbound sender authentication helps mail servers that are outside of your organization to detect when they receive messages that have forged email addresses or header information that appear to come from your domains.
Sender authentication for outbound mail requires changes to your DNS records that are outside the scope of SMG operations. The outbound setups in the following table describe what you need to do to set up sender authentication for outbound messages.

<table>
<thead>
<tr>
<th>Table 4-3</th>
<th>Outbound steps for sender authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sender authentication method</strong></td>
<td>Outbound implementation steps</td>
</tr>
<tr>
<td><strong>(Enable receivers to detect spoofed emails from your domain)</strong></td>
<td></td>
</tr>
<tr>
<td>SPF</td>
<td>Create a DNS record to provide proof of your domain ownership. Refer to resources on the internet such as <a href="http://www.openspf.org/SPF_Record_Syntax">http://www.openspf.org/SPF_Record_Syntax</a> if you need instructions.</td>
</tr>
<tr>
<td>Sender ID</td>
<td>Create a DNS record to provide proof of your domain ownership. Refer to resources on the internet if you need instructions.</td>
</tr>
</tbody>
</table>
| DKIM | 1. On the Administration > Settings > Certificates > Domain Keys tab, add or import a domain key.  
See “Adding a domain key” on page 126.

2. On the Protocols > Domains > Add or Edit Domain > Delivery tab, enable DKIM signing.  
See “Enabling DKIM signing for a domain” on page 123.

3. Also on the Protocols > Domains > Add or Edit Domain > Delivery tab, click Generate to generate a DKIM DNS text record. This operation provides the correct DNS TXT record content and syntax.

4. Manually copy the generated DKIM DNS text record into your DNS records for the domain.
Table 4-3 Outbound steps for sender authentication (continued)

<table>
<thead>
<tr>
<th>Sender authentication method</th>
<th>Outbound implementation steps (Enable receivers to detect spoofed emails from your domain)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMARC</td>
<td>1  Enable DKIM signing for the domain, as described above.</td>
</tr>
<tr>
<td></td>
<td>2  Add the DMARC resource records to your DNS records for the domain.</td>
</tr>
<tr>
<td></td>
<td>For more information, including the DMARC resource record syntax, visit</td>
</tr>
<tr>
<td></td>
<td><a href="https://dmarc.org/resources/specification/">https://dmarc.org/resources/specification/</a>. You can also find a general procedure</td>
</tr>
<tr>
<td></td>
<td>for implementing DMARC in the dmarc.org FAQ &quot;What steps should I follow to implement</td>
</tr>
<tr>
<td></td>
<td>DMARC on my corporate email domain?</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Symantec Email Fraud Protection is a cloud service that helps customers</td>
</tr>
<tr>
<td></td>
<td>implement the DMARC standard to prevent attackers from spoofing their domain names.</td>
</tr>
<tr>
<td></td>
<td>Email Fraud Protection is offered as an add-on for Symantec Messaging Gateway.</td>
</tr>
<tr>
<td></td>
<td>Customers who purchase the service point their DMARC, SPF, and DKIM records to the</td>
</tr>
<tr>
<td></td>
<td>Email Fraud Protection platform, which responds to authentication requests in real time</td>
</tr>
<tr>
<td></td>
<td>and ensures that email sent using the customer’s domain name is authorized. For</td>
</tr>
<tr>
<td></td>
<td>information about how Email Fraud Protection works, see the service’s online help at</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
</tbody>
</table>

Enabling DKIM signing for a domain

You can enable DKIM signing for all outbound messages from a specific domain, using an existing domain key.

**Note:** Although the DKIM standard allows multiple signatures, Symantec Messaging Gateway can add only one DKIM signature to an outbound message.

To enable DKIM signing for a domain

1 In the Control Center, on the **Administration > Settings > Certificates > Domain Keys** tab, make sure that you added or imported a domain key for DKIM signing.
   See “Adding a domain key” on page 126.
2 Click **Protocols > SMTP > Domains**.
3 Click the underlined name of the domain to which you want to add DKIM signing.
4 On the **Edit Domain** page, click the **Delivery** tab.
5 In the DomainKeys Identified Mail panel, click Enable DKIM signing for messages from this domain.

6 In the Base domain field, enter the domain name to be used as part of the DKIM signature, in the form: example.com

---

Note: If you also enable DMARC for outbound mail, the base domain that you enter here impacts the DKIM alignment that you specify in your DMARC record. For instructions on how to create a DMARC record, visit https://dmarc.org/overview/.

---

7 In the Selector box, type a selector string that receiving MTAs can use to perform DNS lookup to retrieve your public key.

The selector identifies the key that SMG uses to sign the messages that are sent from this domain. Enter a string of up to 63 lower case alphanumeric characters (a-z or 0-9). For more information on the use of selectors, see RFC 4871, Section 3.1. https://tools.ietf.org/html/rfc4871#section-3.1

8 From the Signing key drop-down list, choose the domain key that you want to use to sign messages from this domain.

9 In the Signature expiration box, type an integer between 1 and 9999, inclusive, and then click either Hours or Days.

The default value is 30 days.

10 If you want to customize DKIM signing further, click Show Advanced and complete the following optional fields:

Identity An email address, with or without the portion before the @, that includes either the base domain or a subdomain of the base domain. For example, if your base domain is example.com, acceptable identity strings include:

- @example.com
- user@example.com
- @new.example.com
- user@old.example.com
Override default signed headers

Check this box to replace the default signed headers with headers of your own design. Then type one or more headers, separated by colons.

You can append any header with one of the following characters:

- ? - Sign a single copy of the header. Do not assert a non-existent header if the header does not exist.
- * - Sign all existing copies of the header. Assert a non-existent header if the header does not exist.
- + - Sign all existing copies of the header. Do not assert a non-existent header if the header does not exist.
- [No character] - Sign a single copy of the header. Assert a non-existent header if the header does not exist.

Example:

`Received+:X-Example*:From:Subject?:Received`

Whether or not you override the default signed headers, Symantec Messaging Gateway includes the From: header.

Headers

You can choose the method that is used to prepare the signature for the message headers.

- **apply "relaxed" algorithm** creates a signature based on a representation of the headers that includes minor changes, such as changes to white spaces. If minor alterations of the headers occur during transit, relaxed canonicalization in many cases still results in a matching signature.

- **apply "simple" algorithm** bases the signature on the exact content of the headers, including such details as spacing.

The default for message headers is **apply "relaxed" algorithm**.

Body

You can choose the method that SMG uses to prepare the signature for the message body.

- **apply "relaxed" algorithm** creates a signature based on a representation of the message body that includes minor changes, such as changes to white spaces. If minor alterations of the message body occur during transit, relaxed canonicalization in many cases still results in a matching signature.

- **apply "simple" algorithm** bases the signature on the exact content of the message body, including such details as spacing.

The default for the message body is **apply "simple" algorithm**.

For more information on canonicalization, see RFC 4871, Section 3.4.

**RFC 4871, Section 3.4**

11 Click **Generate** to create a DKIM DNS text record. This text record uses the base domain, selector, and signing key details that you specified in the previous steps.
12 Click **Save**.

13 Manually add the public key to your DNS records.

Receiving MTAs access your DNS entry to retrieve your public key when the MTAs perform DKIM validation.

You can use the Linux facility **dig** to confirm that you configured your DNS correctly.

See “Setting up sender authentication for outbound mail” on page 121.

### Adding a domain key

SMG Scanners use domain keys to perform DKIM signing on outbound mail. When you add a domain key, SMG generates an RSA key pair that includes a public key and a private key.

When you enable DKIM signing for a domain from the **Protocols > SMTP > Domains >Add or Edit Domain > Delivery** tab, you select the domain key.

SMG uses the private key to create a signature, which it adds to the header and body of each outbound message. The recipient mail server uses the public key to validate the message.

**To add a domain key**

1. In the Control Center, click **Administration > Settings > Certificates**.
2. Click the **Domain Keys** tab.
3. Click **Add**.
4. In the **Domain key name** field, type a unique name for this domain key.
5. In the **Key length** drop-down list, choose a length, in bits, for the RSA key.

   The default key length is 1024 bits.

   Many DNS servers have a 256 character limitation for DNS records. Records that are longer than 256 characters may fail to load or the DNS server may truncate them. To avoid this issue, use 1024 length DKIM keys. To use a 1536-bit key or 2048-bit key, split the DNS entry into multiple lines of less than 256 characters.

6. Click **Create**.

If you want to use your own private key to create DKIM signatures, you can import it as a domain key instead of adding a domain key.

See “Importing a domain key” on page 127.

See “Enabling DKIM signing for a domain” on page 123.
Importing a domain key

If you have an RSA private key that you want to use to sign outbound messages, you can import it as a domain key and select it for DKIM signing. The domain key that you import must be a private key, in PEM format, and saved in a text file.

See “PEM format requirements for certificates and domain keys” on page 183.

If the domain key is not in PEM format, or is not acceptable to OpenSSL, Symantec Messaging Gateway will attempt to convert the domain key to correct the issue. If the attempt fails, or if the key or file does not comply with the other requirements, import fails.

To import a domain key

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the Domain Keys tab.
3. Click Import.
4. Next to the File name field, click Browse and select a text file containing the domain key you want to add.
5. In the Domain key name field, type a unique name for this domain key.
6. Click Import.

You can now select the imported key when you enable DKIM signing on the Protocols > SMTP > Domains >Add or Edit Domain > Delivery tab. SMG creates the matching public key.

See “Enabling DKIM signing for a domain” on page 123.

See “Adding a domain key” on page 126.
Setting up sender groups

This chapter includes the following topics:

- Enabling or disabling good and bad sender groups
- Choosing actions for good and bad sender groups
- Managing sender group members
- Exporting sender group information
- Supported methods for identifying senders

Enabling or disabling good and bad sender groups

Use the following procedure to enable or disable sender groups. When you disable a sender group, Symantec Messaging Gateway does not use the group during reputation scanning.

To enable or disable good or bad sender groups

1. In the Control Center, click Reputation > Policies > Bad Senders or Reputation > Policies > Good Senders.

   A black hyphen in the Enabled column indicates that the entry is currently disabled. A green check in the Enabled column indicates that the entry is currently enabled.

2. Check or uncheck the boxes next to the groups that you want to enable or disable.

3. Click Enable or Disable.

See “Enabling or disabling good and bad sender group members” on page 132.

See “Editing good and bad sender group members” on page 131.
Choosing actions for good and bad sender groups

All sender groups have default actions. You can choose other actions for any sender group. The following procedure does not apply to Fastpass.

To choose actions for a good or bad senders group
1. In the Control Center, click Reputation > Policies > Bad Senders or Reputation > Policies > Good Senders.
2. Click one of the bad or good sender groups.
4. On the Configure An Action page, click the drop-down list and choose the action that you want to add.
5. Click Add Action.
6. To add more actions, repeat steps 3 through 5.

Symantec Messaging Gateway prevents you from combining contradictory actions. For example, if the action Defer SMTP Connection appears, you cannot add another action because no other action can be taken on a deferred connection. If you want to add a different action, first check the box next to Defer SMTP Connection and click Delete.

See “Policy actions and what they do” on page 333.
7. To delete an action, check an action in the actions list and click Delete.
8. Click Save.

Managing sender group members

Table 5-1 describes the ways that you can manage sender group members. You can perform these tasks as needed in any order.

Note: The following topics do not apply to Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.
### Table 5-1  Manage sender group members

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new senders to groups.</td>
<td>To prevent undesired messages from being delivered to inboxes, you can add specific email addresses, domains, and connections to your bad sender groups. To ensure that messages from specific email addresses, domains, and connections are not treated as spam, you can add them to your good sender groups. See “Adding senders to administrator and third party sender groups” on page 130.</td>
</tr>
<tr>
<td>Edit existing good and bad sender group members.</td>
<td>Follow these steps to change sender information. See “Editing good and bad sender group members” on page 131.</td>
</tr>
<tr>
<td>Delete good and bad sender group members.</td>
<td>You can delete the good or bad sender group members that you no longer need. See “Deleting good and bad sender group members” on page 131.</td>
</tr>
<tr>
<td>Enable or disable good and bad sender group members.</td>
<td>You may need to periodically disable and then re-enable sender group members for troubleshooting or testing purposes. See “Enabling or disabling good and bad sender group members” on page 132.</td>
</tr>
<tr>
<td>Import good and bad sender groups files.</td>
<td>You can import LDIF-formatted text files into good and bad sender groups. See “Importing good and bad sender group entries” on page 132.</td>
</tr>
</tbody>
</table>

### Adding senders to administrator and third party sender groups

To prevent undesired messages from being delivered to inboxes, you can add specific email addresses, domains, and connections to your bad sender groups. To ensure that messages from specific email addresses, domains, and connections are not treated as spam, you can add them to your good sender groups. You cannot add senders to the Symantec Global Good Senders or Symantec Global Bad Senders groups. This procedure does not apply to directory harvest attacks, email virus attacks or Fastpass.

**To add senders to administrator and third party sender groups**

1. In the Control Center, click Reputation > Policies > Bad Senders or Reputation > Policies > Good Senders.
2. Check a good or bad sender group and click Edit.
3. On the Local Good or Bad Sender Domains page, click Add.
4 On the **Add Sender Group Members** page, enter the information appropriate to the sender list to add it to the current sender group.

See “Supported methods for identifying senders” on page 136.

5 Click **Save**.

6 On the **Local Good or Bad Sender Domains** page, modify the default action for messages originating from senders in this sender group, if desired.

7 Click **Save**.

### Editing good and bad sender group members

Follow these steps to change sender information. This procedure does not apply to Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.

See “Enabling or disabling good and bad sender group members” on page 132.

See “About blocking and allowing messages using sender groups” on page 151.

**To edit good and bad sender group members**

1 In the Control Center, click **Reputation > Policies > Bad Senders** or **Reputation > Policies > Good Senders**.

2 Check a sender group from the sender groups list and click **Edit**.

3 To modify the information on a sender, check the sender whose information you want to modify, and click **Edit**.

   You can also click an underlined sender name to automatically jump to the corresponding edit page.

4 On the **Edit Sender Group Member** page, make any changes, and click **Save**.

5 Click **Save** to commit your changes.

### Deleting good and bad sender group members

Follow the steps below to delete senders. This procedure does not apply to Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks or Fastpass.

**To delete senders from a good or bad senders group**

1 In the Control Center, click **Reputation > Policies > Bad Senders** or **Reputation > Policies > Good Senders**.

2 Click one of the bad or good sender groups.
3 In the Members list, check the box next to the sender that you want to remove from your list, and then click Delete.

4 Click Save.

See “Editing good and bad sender group members” on page 131.

See “Exporting sender group information” on page 135.

See “Enabling or disabling good and bad sender group members” on page 132.

---

Enabling or disabling good and bad sender group members

When you add a new sender to a Sender Group, Symantec Messaging Gateway automatically enables the filter and puts it to use when evaluating incoming messages. You may need to periodically disable and then re-enable sender group members for troubleshooting or testing purposes. Symantec Messaging Gateway treats mail from a sender that you have disabled as it would any other message. This procedure does not apply to Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.

To enable or disable good and bad sender group members

1 In the Control Center, click Reputation > Policies > Good Senders or Reputation > Policies > Bad Senders.

2 Click one of the good or bad sender groups.

A black dash in the Enabled column indicates that the entry is currently disabled. A green check in the Enabled column indicates that the entry is currently enabled.

3 In the Members list on the page for that sender group, perform one of the following tasks:

- To reinstate a member that is currently disabled in a sender group, check the box adjacent to the sender information and click Enable.

- To disable a member that is currently enabled in a sender group, check the box adjacent to the sender information and click Disable.

4 Click Save.

See “Enabling or disabling good and bad sender groups” on page 128.

See “Editing good and bad sender group members” on page 131.

---

Importing good and bad sender group entries

Use the following procedure to import LDIF-formatted text files into good and bad sender groups. This procedure does not apply to Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.
Be aware of the following limitations on the number of entries that can be imported into sender groups:

- The maximum number of total senders that can be stored, including good and bad senders, is 650,000.
- The maximum number of lines per file when importing senders is 500,000. To add more, divide senders into multiple files and import each file separately.
- No warning is displayed if you exceed these limits. Sender data is silently dropped.

To import good and bad sender group entries

1. In the Control Center, click **Reputation > Policies > Bad Senders** or **Reputation > Policies > Good Senders**.

2. Check one of the bad or good sender groups and click **Edit**.
   
   You can import entries for all good sender groups, or all bad sender groups in one import action, no matter which group you open. However, you cannot import entries for Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.

3. Click **Import**.

4. In the **Import** dialog box, specify or browse to the location of the text file with the sender information that you want to import.
   
   The sender information must be formatted correctly.
   
   See “Sender group import file formats” on page 133.

5. Click **Import**.

   Symantec Messaging Gateway merges data from the imported list with the existing sender information.

6. Click **Save**.

Sender group import file formats

Use the specifications in this section when importing sender information for your sender groups. You cannot import sender entries for Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.

See “Importing good and bad sender group entries” on page 132.

The file that you import should be line-oriented and use a format similar to the Lightweight Directory Interchange Format (LDIF), which includes the following restrictions and characteristics:

- The file must have the required LDIF header. Do not change the first three uncommented lines from the following:
After the header, each line must contain exactly one attribute, along with a corresponding pattern. Empty lines or white spaces are not allowed. Lines beginning with # are ignored. Entries terminating with the colon-dash pattern (:-) are disabled; entries terminating with the colon-plus pattern (:+) are enabled; entries with neither set of terminating symbols are enabled.

To populate the list, specify an attribute, which is followed by a pattern. In the following example, a list of attributes and patterns follows the LDIF header. See below for an explanation of the attribute codes.

### Permit List

```
# Permit List
#

dn: cn=mailwall, ou=bmi
objectclass: top
objectclass: bmiBlackWhiteList
AC: 65.86.37.45/255.255.255.0
AS: grandma@example.com
RC: 20.45.32.78/255.255.255.255
RS: spammer@example.com
BL: sbl.spamhaus.org
# Example notations for disabled and enabled entries follow
RS: rejectedspammer@example.com:-
RS: rejectedspammer2@example.com:+
```

The following table lists the attributes and the syntax for the values.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| AC:       | Allowed (good) connection or network. Specify a numerical IP address, numerical IP address and network mask, or Classless Inter-Domain Routing (CIDR) IP address. | AC: 76.86.37.45  
            |             | AC: 76.86.37.45/255.255.255.0  
<pre><code>        |             | AC: 76.86.37.00/18 |
</code></pre>
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| RC:       | Rejected or blocked (bad) connection or network. Specify a numerical IP address, numerical IP address and network mask, or CIDR IP address. | RC: 76.86.37.45  
RC: 76.86.37.45/255.255.255.0  
RC: 76.86.37.00/18 |
| AS:       | Allowed (good) sender. Specify an email address or domain using alphanumeric and special characters, except the plus sign (+). | AS: example.com  
AS: spammer@example.org  
AS: john?????@example.com |
| RS:       | Rejected or blocked (bad) sender. Specify an email address or domain using alphanumeric and special characters, except the plus sign (+). | RS: example.com  
RS: spammer@example.org  
RS: john?????@example.com |
| BL:       | Third party blocked (bad) sender list. Use the zone name specified by the list provider. | BL: sbl.spamhaus.org |
| WL:       | Third party allowed (good) sender list. Use the zone name specified by the list provider. | WL: allowed.example.com |

### Exporting sender group information

Occasions can arise when you want to export the data stored in your sender group for use in another application. Use the following procedure to export sender group entries to a text file. This procedure does not apply to Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.

See “Importing good and bad sender group entries” on page 132.
To export sender group information to a text file

1. In the Control Center, click **Reputation > Policies > Bad Senders** or **Reputation > Policies > Good Senders**.

2. Click one of the bad or good sender groups.

   The entries for all good sender groups, or all bad sender groups are exported no matter which list you open. However, you cannot export entries for Symantec Global Good Senders, Symantec Global Bad Senders, directory harvest attacks, email virus attacks, or Fastpass.

3. Click **Export**.

   Your browser will prompt you to open the file from its current location or save it to disk.

---

**Supported methods for identifying senders**

You can use the following methods to identify senders for your good sender groups and bad sender groups:

**IP-based**

Specify IP connections.

Symantec Messaging Gateway checks the IP address of the mail server that initiates the connection to verify if it is in your good sender groups or bad sender groups. You can specify IPv4 addresses or IPv6 addresses.

Wildcards are not supported.

You can use the standard IPv4 format or IPv6 format for a single host or CIDR notation for a range. You can use network masks to indicate a range of addresses, but you cannot use subnet masks that define non-contiguous sets of IP addresses (for example, 69.84.35.0/255.0.255.0).

**Third-party services**

Supply the lookup domain of a third-party sender service. Symantec Messaging Gateway can check the message source against third-party DNS-based lists to which you subscribe—for example, list.example.org.

**Note:** Be sure to confirm the quality of a third-party list before using it. Symantec is unable to resolve false positives that result from use of third-party lists.
Domain-based Specify sender addresses or domain names.
Symantec Messaging Gateway checks the following characteristics of incoming mail against those in your lists:

- **MAIL FROM:** address in the SMTP envelope. Specify a pattern that matches the value for localpart@domain in the address.
- **From:** address in the message headers. Specify a pattern that matches the value for localpart@domain in the FROM: header.

Wild cards can be specified in domain names unless the local part is preceding. For example, localpart@example.com, and localpart*@example.com are both supported, but localpart@*.example.com is not supported.

Table 5-2 provides examples to model entries when you add members to a sender group if you choose to identify senders by address or domain name.

Table 5-2 Examples

<table>
<thead>
<tr>
<th>Example</th>
<th>Sample matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td><a href="mailto:chang@example.com">chang@example.com</a>, <a href="mailto:marta@example.com">marta@example.com</a>, <a href="mailto:john@bank.example.com">john@bank.example.com</a></td>
</tr>
<tr>
<td>*.example.com</td>
<td>server1.example.com, server2.example.com</td>
</tr>
<tr>
<td>example*.com</td>
<td>example1.com, example2.com</td>
</tr>
<tr>
<td><a href="mailto:malcolm@example.net">malcolm@example.net</a></td>
<td><a href="mailto:malcolm@example.net">malcolm@example.net</a></td>
</tr>
<tr>
<td>sara*@example.org</td>
<td><a href="mailto:sara@example.org">sara@example.org</a>, <a href="mailto:sarahjane@example.org">sarahjane@example.org</a></td>
</tr>
<tr>
<td>jo??@example.org</td>
<td><a href="mailto:john@example.org">john@example.org</a>, <a href="mailto:josh@example.org">josh@example.org</a></td>
</tr>
</tbody>
</table>
Enabling reputation filtering

This chapter includes the following topics:

- Enabling reputation-based filtering features
- Managing email traffic at the gateway
- Configuring email virus attack recognition
- Configuring directory harvest attack recognition
- About blocking and allowing messages using sender groups
- About conserving resources using Fastpass
- Defending against bounce attacks
- Researching IP address reputation

Enabling reputation-based filtering features

Table 6-1 describes the process to set up reputation-based filtering.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>Understand Symantec Messaging Gateway’s blocking features and technologies.</td>
<td>See “About blocking and allowing messages at connection time” on page 141.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About managing connection load at the gateway” on page 143.</td>
</tr>
<tr>
<td>Phase 2</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Phase 2</td>
<td>Customize message flow parameters.</td>
<td>Configure Connection Classification to customize the parameters for your message flow. See “Configuring Connection Classification” on page 145. See “Connection class default settings” on page 146.</td>
</tr>
</tbody>
</table>

| Phase 3 | Set up email virus attack recognition and specify actions to take. | Configure your system to recognize and block offenders. See “Configuring email virus attack recognition” on page 147. See “Configuring directory harvest attack recognition” on page 149. Specify filter rules for Bad Sender email. See “About blocking and allowing messages using sender groups” on page 151. Use additional tools for IP analysis to verify sender history. See “Researching IP address reputation” on page 163. |

| Phase 4 | Protect system resources. | Understand how Fastpass can prevent drainage of valuable system resources. See “About conserving resources using Fastpass” on page 154. Configure system to recognize and fast track legitimate senders and reduce processing power. See “Configuring Fastpass” on page 156. |
### Table 6-1  Process for setting up reputation-based filtering features (continued)

<table>
<thead>
<tr>
<th>Phase</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 5</td>
<td>Set up Bounce Attack Prevention.</td>
<td>Understand bounce attacks and non-deliverable receipt (NDR) messages. See “About defending against bounce attacks” on page 160. Provide a Bounce Attack Prevention seed value in your Control Center. See “Configuring the Control Center for Bounce Attack Prevention” on page 161. Determine and configure the groups to which you want the system to apply Bounce Attack Prevention. See “Configuring policy groups for Bounce Attack Prevention” on page 162. Assign a policy (a default policy is provided) to the group that determines the actions to be taken for NDRs that do not pass Bounce Attack Prevention validation. See “Creating an email spam or unwanted email policy for Bounce Attack Prevention” on page 163.</td>
</tr>
</tbody>
</table>

### Managing email traffic at the gateway

You can configure tools available in the Control Center to enable the proprietary technologies that greatly reduce incoming spam before it hits your network.

**Table 6-2** lists topics about these technologies and how they integrate with the gateway.

### Table 6-2  Manage traffic at the gateway

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>See “About blocking and allowing messages at connection time” on page 141.</td>
<td>Symantec Messaging Gateway features Brightmail Adaptive Reputation Management (Brightmail ARM). Brightmail ARM includes features designed to reduce unnecessary incoming email traffic, protect your network from attacks, and optimize the use of your processing resources. Brightmail ARM includes technologies that can reject or defer incoming connection attempts based solely on the incoming IP address.</td>
</tr>
</tbody>
</table>
Table 6-2  Manage traffic at the gateway (continued)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>See “About managing connection load at the gateway” on page 143.</td>
<td>You can reduce the cost of processing by managing connection load and distinguishing between connections from senders that are known to send spam and legitimate senders. The Connection Classification feature dynamically manages connection load based on the local reputation data that is collected automatically.</td>
</tr>
<tr>
<td>See “About blocking and allowing messages using sender groups” on page 151.</td>
<td>When you filter email based on the sender's domain, IP address, or email address, you can reduce spam and malware.</td>
</tr>
<tr>
<td>See “Configuring Connection Classification” on page 145.</td>
<td>These topics explain how to configure the tools that enable these technologies.</td>
</tr>
<tr>
<td>See “Researching IP address reputation” on page 163.</td>
<td></td>
</tr>
</tbody>
</table>

About blocking and allowing messages at connection time

Scanning email for spam, malware, and content filtering is a resource-intensive task. Any email that must be processed past the gateway taxes your mail infrastructure, resource capacity, and system performance. Symantec Messaging Gateway features Brightmail Adaptive Reputation Management (Brightmail ARM). Brightmail ARM includes features designed to reduce unnecessary incoming email traffic, protect your network from attacks, and optimize the use of your processing resources.

Brightmail ARM includes technologies that can reject or defer incoming connection attempts based solely on the incoming IP address. To accomplish this, Brightmail ARM uses dynamic, self-learning local reputation data, global reputation data, and administrator-defined Bad Sender Policies and Good Sender Policies.

Brightmail ARM generates local reputation data based on good and bad verdicts rendered on messages in your mail stream. Brightmail ARM builds global reputation data by leveraging the extensive world-wide data collection capabilities of Brightmail IQ Services. Brightmail IQ Services includes the Probe Network, Symantec's collection of millions of honeypot emails that collect spam throughout the Internet, as well as the Global Intelligence Network. The Global Intelligence Network includes threat detection and response centers around the world, managed by Symantec Security Response.

Brightmail ARM uses these diverse technologies to achieve five goals:
Reduce the volume of incoming email traffic by eliminating most spam messages at the gateway.

Stop virus, malware, and directory harvest attacks at the gateway.

Allow messages from senders with the best local reputation to bypass spam scanning.

Provide uninterrupted connection abilities to your best senders, regardless of the volume of spam or attacks at any moment.

Protect you from denial-of-service attacks by limiting the connection abilities of illegitimate senders.

Symantec Messaging Gateway conserves, protects, and optimizes your physical assets, your message flow, and your vital data. Brightmail ARM is the first stage in the inbound protection process. By examining the incoming IP addresses, and in some cases also the message envelope, Brightmail ARM can take preventive action. By rejecting or deferring undesirable connections, Brightmail ARM restores valuable filtering cycles to the Scanner.

Brightmail ARM employs the following features and technologies to achieve these aims.

**Table 6-3**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Classification</td>
<td>Connection Classification provides the best connection abilities to your best senders, and progressively worse connection abilities to all other senders. Connection Classification ensures that your worst senders cannot degrade the connection experience of your best senders.</td>
</tr>
<tr>
<td></td>
<td>Connection Classification automatically places every incoming sender IP into one of 10 classes based on local reputation. Class membership is determined based on how many legitimate and spam messages each IP has sent to the Scanner, and is constantly updated.</td>
</tr>
<tr>
<td></td>
<td>New IPs are assigned to the Default class. Senders in Good Sender groups always use the best class (Class 1). Senders in Bad Sender groups always use the worst class (Class 9).</td>
</tr>
<tr>
<td></td>
<td>See “About managing connection load at the gateway” on page 143.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring Connection Classification” on page 145.</td>
</tr>
<tr>
<td>Email virus attack prevention</td>
<td>If Symantec Messaging Gateway detects a specified number of infected messages from an IP address, email virus attack prevention can then defer further connections. Or, you can choose other actions.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring email virus attack recognition” on page 147.</td>
</tr>
</tbody>
</table>
About managing connection load at the gateway

Today, in most networks, the majority of email traffic is spam. You can reduce the cost of processing by managing connection load and distinguishing between connections from senders known to send spam and legitimate senders. The Connection Classification feature dynamically manages connection load based on the local reputation data collected automatically. Connection Classification is a self-learning feature. In response to the latest changes in local reputation, Connection Classification updates its management of connection load on a just-in-time basis.
For the purposes of Connection Classification data collection, unwanted messages are not counted as spam.

Spammers routinely leverage vast networks of compromised client machines, known as botnets, to disseminate their attacks. This enables them to generate huge volumes of messages without sending enough messages from any single IP address to merit entry on a global blacklist. Connection Classification supplements global lists from Symantec, third parties and your own administrator-defined lists with an approach that is effective against botnet-driven spam and the huge overall volume of spam.

By reducing the system resources used by senders with poor local reputation, Connection Classification protects your legitimate mail flow from denial-of-service attacks. With Connection Classification enabled, spammers get fewer connections. As a result, more resources are available to your legitimate senders.

To take advantage of Connection Classification, your Symantec Messaging Gateway appliance must be deployed at the gateway.

Connection Classification works by assigning each connecting IP address to one of ten classes, based on the amount of spam sent by that IP address. Connection Classification assigns new IP addresses to the default class. Connection Classification regularly changes the classifications of senders, as it continues to learn more about sender reputation in real time.

Connection Classification allows most connections for the best senders (class 1). As one moves from the best class to the worst class (Class 9), the network resources allowed a sender decrease. For Class 9, Connection Classification defers most connections.

Senders in the Symantec Global Good Senders, Local Good Sender IPs, and Third Party Good Senders groups are always assigned to the best class (Class 1). Senders in the Symantec Global Bad Senders, Local Bad Sender IPs, and Third Party Bad Senders groups are always assigned to the worst class (Class 9).

Symantec Messaging Gateway determines class membership separately for each Scanner in your system. The same sending IP can be in Class 3 on one Scanner and Class 4 on another Scanner. Based on the amount of spam sent from each IP address, the classifications can change constantly, to dynamically reflect the latest local, per-Scanner reputation.

The restrictions placed on a sender’s ability to consume system and network resources correlate directly with the sender’s reputation for spamming your organization. Senders with a clean history are placed in the best class and allowed more frequent connections than those with poor records. Conversely, an IP address with a poor reputation can improve its class over time by sending less spam and more legitimate email.
Connection Classification uses the data collected in the reputation database to determine the probability that a message sent from a given IP is spam. As the appliance collects more data over time, the probabilistic determination yields more accurate results.

The only action Symantec Messaging Gateway takes based on Connection Classification is to defer some SMTP connections. Connection deferral is also known as soft rejection or a 450 SMTP error. Connection Classification defers connections during the connection phase of the inbound message flow and also during the SMTP session phase.

See “About email message flow” on page 100.

Symantec Messaging Gateway does not take any action based on Connection Classification until the appliance has recorded enough data to make accurate predictions. Immediately after the initial installation of a Scanner, Connection Classification is in learning mode. Learning mode ends when 50,000 messages are received and the statistics gathered from them have been added to the database. At that point, if Connection Classification is enabled, connection management begins. If you have multiple Scanners, a newly installed Scanner is initially in learning mode, while your other Scanners may already be managing connection load.

---

**Note:** If you disable Connection Classification, the Scanner continues to record sender reputation information. This means that you can disable this feature temporarily and not miss any sender data during that time.

---

You can edit the connection parameters for each class.

See “Configuring Connection Classification” on page 145.

You can query the status of an IP’s reputation.

See “Researching IP address reputation” on page 163.

---

**Configuring Connection Classification**

Using Connection Classification ensures that the most abusive senders cannot degrade the connection ability of your best senders. Connection Classification automatically classifies every incoming IP address into one of 10 classes. Symantec Messaging Gateway automatically gathers local reputation data to inform the classification. Senders in the best class, because they rarely if ever send spam, benefit from the best connection parameters. Senders in the worst class are subject to the worst connection parameters. New IP addresses are initially placed into the default class.

Upon initial installation, Connection Classification is in learning mode for the first 50,000 messages. During learning mode no messages are deferred based on their connection class. Connection Classification is designed to work without any configuration. However, you can configure Connection Classification to customize the parameters for your message flow. Use the procedures in this section to enable, disable, or configure Connection Classification.
To configure Connection Classification

1. In the Control Center, click Reputation > Policies > Connection Classification.

2. On the Connection Classification page, check Enable Connection Classification.
   To disable Connection Classification, uncheck the box.

3. To configure Connection Classification parameters, click Edit.
   The fields in the table become editable, and the Edit button changes to a Load Defaults button.
   See “Connection class default settings” on page 146.

4. To change the maximum connections for each class, type new values in the 10 fields on the Maximum connections row.
   Each value is the percent of total available connections that are allocated to that class.
   The total of all 10 values must equal 100%. In each field, you can enter a value between 0.1 and 99.1, inclusive. As you edit the fields, the current total of the amounts you entered appears in red below the Maximum connections label on the left.

5. To change the connections that are allowed on a per-IP address basis, type new values in the Maximum Connections per IP fields.

6. To vary the number of messages that are allowed on a per-connection basis, type new values in the Messages per Connection fields.

7. To vary the time, in seconds, before a sender IP is allowed to reconnect, type new values in the Reconnect Timeout fields.

8. To vary the proportion of connections that are deferred for each class, type new values in the Deferred Messages fields.
   Each value on this row represents the percentage of the total messages for sender IP addresses in that class that must be deferred. You can type any integer between 0 and 100, inclusive. The values do not need to add up to 100%.

9. To abandon your changes and return to the default values, click Load Defaults.

10. To commit your changes, click Save.

Connection class default settings

Table 6-4 shows the default values for each connection class. A value of zero (0) indicates that there is no limit.
Table 6-4  Default values for each connection class

<table>
<thead>
<tr>
<th>Connection class</th>
<th>Maximum connections (must total 100%)</th>
<th>Maximum connections per IP</th>
<th>Messages per connection</th>
<th>Reconnect timeout</th>
<th>Deferred messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Class</td>
<td>10.0%</td>
<td>1</td>
<td>1</td>
<td>10 sec</td>
<td>10%</td>
</tr>
<tr>
<td>Class 9 (worst)</td>
<td>0.2%</td>
<td>1</td>
<td>1</td>
<td>60 sec</td>
<td>95%</td>
</tr>
<tr>
<td>Class 8</td>
<td>0.4%</td>
<td>1</td>
<td>1</td>
<td>30 sec</td>
<td>80%</td>
</tr>
<tr>
<td>Class 7</td>
<td>1.0%</td>
<td>1</td>
<td>1</td>
<td>30 sec</td>
<td>60%</td>
</tr>
<tr>
<td>Class 6</td>
<td>5.0%</td>
<td>1</td>
<td>1</td>
<td>15 sec</td>
<td>30%</td>
</tr>
<tr>
<td>Class 5</td>
<td>10.0%</td>
<td>1</td>
<td>5</td>
<td>5 sec</td>
<td>60%</td>
</tr>
<tr>
<td>Class 4</td>
<td>10.0%</td>
<td>25</td>
<td>10</td>
<td>2 sec</td>
<td>5%</td>
</tr>
<tr>
<td>Class 3</td>
<td>10.0%</td>
<td>50</td>
<td>20</td>
<td>1 sec</td>
<td>0%</td>
</tr>
<tr>
<td>Class 2</td>
<td>19.0%</td>
<td>100</td>
<td>40</td>
<td>1 sec</td>
<td>0%</td>
</tr>
<tr>
<td>Class 1 (best)</td>
<td>34.4%</td>
<td>200</td>
<td>0</td>
<td>0 sec</td>
<td>0%</td>
</tr>
</tbody>
</table>

See “About managing connection load at the gateway” on page 143.

Configuring email virus attack recognition

In an email virus attack, a specified quantity of infected email messages has been received from a particular IP address. By default, any connections that are received from violating senders are deferred.

Set up email virus attack recognition as described in the following procedure. Email virus attack recognition is disabled by default, and must be enabled to be activated.

To enable or disable email virus attack recognition

1. In the Control Center, click **Reputation > Policies > Bad Senders**.
2. To enable or disable email virus attack recognition on this page, click **Email Virus Attacks**, then click **Enable** or **Disable**.
   Or, continue with the next step.
3. Click **Email Virus Attacks**.
4. Check **Enable Email Virus Attack detection** to enable email virus attack recognition, or uncheck **Enable Email Virus Attack detection** to disable email virus attack recognition.
To configure email virus attack recognition

1 In the Control Center, click **Reputation > Policies > Bad Senders**.

2 Click **Email Virus Attacks**.

3 Accept the defaults or modify the values under Email Virus Attack Configuration:

- **Minimum percentage of virus messages**: Percentage of virus messages from a single server that must be exceeded to trigger the specified action. The minimum number must also be exceeded.

- **Minimum number of virus messages**: Number of virus messages from a single server that must be exceeded to trigger the specified action. The minimum percentage must also be exceeded.

- **Qualification time window**: Time period in which the specified percentage and number of virus messages must be exceeded to trigger the specified action.

- **Penalty box time**: Period of time during which Symantec Messaging Gateway performs the specified action against all messages from the sending SMTP connection.

4 Under **Actions**, you can:

- Accept the default, recommended action of Defer SMTP Connection with a message of "try again later."

- Edit the action to enter a new message and click **Update Action**.

- Or select another action from the drop-down list under **If an email virus attack occurs**.

Other actions may provide additional options for you to configure. For instance, if you choose the **Archive the message** action, the **Email Virus Attacks** page displays an **Optional archive tag** text box and an **Encoding** drop-down list.

5 Click **Add Action** to add the action to the list of actions Symantec Messaging Gateway takes upon recognizing a virus attack.

Symantec Messaging Gateway prevents you from combining contradictory actions. For example, you cannot add another action to the default action because no other action can be taken on a deferred connection. If you want to add a different action, first check the box next to **Defer SMTP Connection** and click **Delete**.

See “**Policy actions and what they do**” on page 333.
6 To change the settings for an existing action, check the box next to the action and click Edit.

Any available options for that action appear. Click Update Action after configuring the options.

7 Click Save.

Configuring directory harvest attack recognition

Spammers employ directory harvest attacks to find valid email addresses at the target site. A directory harvest attack works by sending a large quantity of possible email addresses to a site. An unprotected mail server rejects any messages that are sent to invalid addresses. This behavior allows spammers to tell which email addresses are valid by checking the rejected messages against the original list.

When directory harvest attack recognition is enabled, any connections that are received from violating senders are deferred by default. Deferring a connection slows down the progress of a possible attack and discourages spammers from maintaining the connection.

Set up directory harvest attack recognition as described in the following procedures. Directory harvest attack recognition is disabled by default. You must enable directory harvest attack recognition to activate it.

---

**Note:** Before enabling directory harvest attack recognition, you must perform the following actions:

- Set up your local domains. Symantec Messaging Gateway accepts inbound messages only for the domains you specify.
  
  See “Adding or editing domains” on page 82.

- Enable invalid recipient handling, configured to reject invalid recipients.
  
  See “Setting up invalid recipient handling” on page 99.

To enable or disable directory harvest attack recognition

1 In the Control Center, click Reputation > Policies > Bad Senders.

2 To enable or disable directory harvest attack recognition on this page, check Directory Harvest Attack and click Enable or Disable.

Or, continue with the next step.

3 Click Directory Harvest Attack.

4 Check Enable DHA detection to enable directory harvest attack recognition, or uncheck Enable DHA detection to disable directory harvest attack recognition.

5 Click Save.
To configure directory harvest attack recognition

1. In the Control Center, click **Reputation > Policies > Bad Senders**.

2. Click **Directory Harvest Attack**.

3. Accept the defaults or modify the values under Directory Harvest Attack Configuration:

   - **Minimum percentage of bad recipients**
     - Percentage of bad recipient messages from a single server that must be exceeded to trigger the specified action. The minimum number must also be exceeded. Bad recipient messages are messages sent to addresses in your local domains that do not exist.

   - **Minimum number of bad recipients**
     - Number of bad recipient messages from a single server that must be exceeded to trigger the specified action. The minimum percentage must also be exceeded.

   - **Qualification time window**
     - Time period in which the specified percentage and number of bad recipient messages must be exceeded to trigger the specified action.

   - **Penalty box time**
     - Period of time during which Symantec Messaging Gateway performs the specified action against all messages from the sending SMTP connection.

4. Under **Actions**, you can:

   - Accept the default, recommended action of Defer SMTP Connection with a message of "try again later."

   - Edit the action to enter a new message and click **Update Action**.

   - Or, select another action from the drop-down list under **If a directory harvest attack occurs**.

   Other actions may provide additional options for you to configure. For instance, if you choose the **Archive the message** action, the **Directory Harvest Attack** page displays an **Optional archive tag** text field and an **Encoding** drop-down list.

5. Click **Add Action** to add the action to the list of actions Symantec Messaging Gateway takes upon recognizing a directory harvest attack.

   Symantec Messaging Gateway prevents you from combining contradictory actions. For example, you cannot add another action to the default action because no other action can be taken on a deferred connection. If you want to add a different action, first check the box next to **Defer SMTP Connection** and click **Delete**.

   See “Policy actions and what they do” on page 333.
6. To change the settings for an existing action, check the box next to the action name and click **Edit**. Any available options for that action appear. Click **Update Action** after configuring the options.

7. Click **Save**.

### About blocking and allowing messages using sender groups

Filtering email based on the sender’s domain, IP address, or email address provides administrators and end users a powerful way to reduce spam and malware.

---

**Note:** This section describes administrator-defined and global sender groups, which are applied at the server level for your organization. To allow end users to maintain individual sender lists, enable personal good and bad sender lists by going to Administration > Users > Groups.

See "Enabling and disabling end user settings for policy groups" on page 201.

---

Symantec Messaging Gateway lets you customize spam detection in the following ways:

**Define good senders**  
Symantec Messaging Gateway treats mail coming from an address or connection in the Local Good Sender Domains and Local Good Sender IPs groups as legitimate mail. The good sender groups reduce the small risk that messages sent from trusted senders will be treated as spam or filtered in any way. By default, messages from these senders are delivered normally.

**Define bad senders**  
Symantec Messaging Gateway supports a number of actions for mail from a sender or connection in the Local Bad Sender Domains and Local Bad Sender IPs groups. By default, messages from senders in the Local Bad Sender Domains group are deleted. By default, SMTP connections from senders in the Local Bad Sender IPs and Third Party Bad Senders groups are rejected. However, you can instead choose other actions.
By default, Symantec Messaging Gateway is configured to use Symantec Global Good Senders and Symantec Global Bad Senders. Symantec monitors hundreds of thousands of email sources to determine how much email sent from these IP addresses is legitimate and how much is spam.

Symantec Global Good Senders consists of IP addresses known as legitimate senders based on reputation data collected by Symantec. Symantec Global Bad Senders consists of IP addresses that have sent large amounts of spam to mail servers protected by Symantec.

Both groups are continuously compiled, updated, and incorporated into Symantec Messaging Gateway filtering processes at your site. No configuration is required for these lists. You can choose to disable either of these lists.

By default, messages from senders in the Symantec Global Good Senders group are delivered normally. By default, SMTP connections from senders in the Symantec Global Bad Senders group are rejected. However, you can instead choose other actions.

Third parties compile and manage lists of desirable or undesirable IP addresses. These lists are queried using DNS lookups. You can add third-party sender lists to your Third Party Bad Senders or Third Party Good Senders groups.

By default, SMTP connections from bad senders in these groups are rejected, and messages from good senders in these groups are delivered normally. However, you can instead choose other actions.

**Note:** Be sure to confirm the quality of a third-party list before using it. Symantec is unable to resolve false positives that result from third-party lists.

Table 6-5 describes why you might want to maintain lists of good or bad senders for your organization and gives examples of patterns that you might use to match the sender.

**Table 6-5**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
<th>Pattern example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail from an end-user's colleague is occasionally flagged as spam.</td>
<td>If personal good and bad sender lists are enabled for end users, the user can add the colleague's email address to their Good Senders list. To enable this capability for an end user, go to <strong>Administration &gt; Users &gt; Policy Groups</strong>, edit the policy group containing the end user, and click on the <strong>End User</strong> tab. The user can then add <a href="mailto:colleague@trustedco.com">colleague@trustedco.com</a> to their Good Senders list. See “Enabling and disabling end user settings for policy groups” on page 201.</td>
<td><a href="mailto:colleague@trustedco.com">colleague@trustedco.com</a></td>
</tr>
<tr>
<td>Problem</td>
<td>Solution</td>
<td>Pattern example</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Desired newsletter from a mailing list is occasionally flagged as spam.</td>
<td>Add newsletter.com to the Local Good Sender Domains group. See “Adding senders to administrator and third party sender groups” on page 130.</td>
<td><a href="mailto:latest@newsletter.com">latest@newsletter.com</a></td>
</tr>
<tr>
<td>An individual is sending unwanted email to people in your organization.</td>
<td>Add <a href="mailto:Joe.unwanted@getmail.com">Joe.unwanted@getmail.com</a> to the Local Bad Sender Domains group. See “Adding senders to administrator and third party sender groups” on page 130.</td>
<td><a href="mailto:Joe.unwanted@getmail.com">Joe.unwanted@getmail.com</a></td>
</tr>
<tr>
<td>Numerous people from a specific range of IP addresses are sending unsolicited mail to people in your organization.</td>
<td>After analyzing the received headers to determine the sender’s network and IP address, add 218.187.0.0/255.255.0.0 to the Local Bad Sender IPs group. See “Adding senders to administrator and third party sender groups” on page 130. See “Supported methods for identifying senders” on page 136.</td>
<td>218.187.0.0/255.255.0.0</td>
</tr>
</tbody>
</table>

When evaluating domain name matches, Symantec Messaging Gateway automatically expands the specified domain to include subdomains. For example, Symantec Messaging Gateway expands example.com to include biz.example.com and jenny@foo.example.com, to ensure that any possible subdomains are allowed or blocked as appropriate. See “Supported methods for identifying senders” on page 136.

You cannot have the exact same entry in both a good sender group and a bad sender group. If an entry already exists in one group, you see an error message when you try to add the same entry to the other group. If you prefer that an entry in one group appear as an entry on the other, first delete the entry from the group where it currently resides, then add it to the other group.

Incorporating third-party lists adds additional steps to the filter process. For example, similar to a typical DNS query, the IP address of the sending mail server for each incoming message is checked against a DNS list maintained in the third-party database. If the sending mail server is on the list, the mail is flagged as spam. If your mail volume is sufficiently high, running incoming mail through a third-party database could hamper performance because of the requisite DNS lookups. Symantec recommends that you use the Symantec Global Good Senders and Symantec Global Bad Senders groups instead of enabling third-party lists.

When deployed at the gateway, Symantec Messaging Gateway obtains the physical or peer IP connection for an incoming message and compares it to entries in the good sender and bad sender groups. If a Scanner is deployed elsewhere in your network, for example, downstream from a gateway MTA that is not identified as an internal mail host, Symantec
Messaging Gateway may identify the IP address of your gateway server as a source of spam. You should accurately identify all internal mail hosts that are upstream relative to inbound mail flow from your Symantec Messaging Gateway appliance.

See “Specifying internal mail hosts for non-gateway deployments” on page 65.

In addition to internal mail hosts you can add, Symantec Messaging Gateway includes a series of IP address ranges in the internal hosts list as follows:

- 0.0.0.0/255.0.0.0
- 10.0.0.0/255.0.0.0
- 127.0.0.0/255.0.0.0
- 169.254.0.0/255.255.0.0
- 172.16.0.0/255.240.0.0
- 192.168.0.0/255.255.0.0

Symantec Messaging Gateway will exclude the IP addresses of internal mail hosts from the following verdicts:

- Local Good Sender IPs
- Local Good Third Party Senders
- Local Bad Sender IPs
- Local Bad Third Party Senders
- Directory Harvest Attacks
- Symantec Global Bad Senders
- Symantec Global Good Senders
- Connection Classification
- Email Virus Attacks
- Fastpass

### About conserving resources using Fastpass

Scanning email messages for spam and unwanted messages is a resource-intensive process. Fastpass conserves resources by providing a temporary exemption from spam scanning for senders with a demonstrated history of sending no spam messages. A "pass" is granted to such a message source if that source has sent a specified number of consecutive legitimate messages, 15 by default.
Note: For the purposes of Fastpass data collection, unwanted messages are counted as spam.

Once a source receives a pass, the amount of antispam processing applied to messages from that source decreases over time. The number of messages that are allowed to bypass antispam filtering, increases as more and more legitimate email comes from the source. This reduces the processing time required for messages from legitimate sources. This may also decrease effectiveness in detecting spam. The Fastpass feature is designed to deliver a significant increase in performance, at the cost of a minimal decrease in effectiveness.

If a message source holding a pass subsequently sends a spam message that is sampled, the pass is immediately revoked from all IP addresses in the /24 range of the offending IP address. Symantec Messaging Gateway performs a full antispam analysis on all messages from sources in that range. The source remains eligible to receive another pass, however, by once again meeting all the configured criteria.

Fastpass uses a database to store and categorize message source IP addresses. The database consists of the following tables:

- **Fastpass trial table**: Contains entries that are being evaluated for possible inclusion in the Fastpass table. A determination is made to move an IP address from the trial table to the pass table based on successful testing for legitimate messages for the IP address. All messages from IP addresses in the Fastpass trial table are scanned for spam and unwanted messages.

- **Fastpass table**: Contains entries that are granted a pass by Fastpass based on no spam coming from the IP address for a specified number of messages.

You can configure any of the following settings:

- **The size of the Fastpass database**: The default size is 250,000 IP addresses; you can change this to any integer between 1,000 and 1,000,000, inclusive. 25% of the database is reserved for the Fastpass table. The remaining 75% reserved for the Fastpass trial table.

- **The rate of growth of the Fastpass trial table**: Specify the probability that an unknown IP address is added to the Fastpass trial table when it sends a legitimate message. You can specify any (integer) probability from a 1/1 probability to a 1/100 probability, inclusive. You only type the denominator of the fraction to indicate the probability. The default value is 3, which indicates a 1/3 or 1 in 3 probability. Note that the number is a probability, not a certainty. For example, if set to 1/3 there may be occasions when five sequential different unknown IPs are not added, or when two IPs in a row are added.
The rate of growth of the Fastpass table | Specify the number of sequential legitimate messages required before an IP address in the Fastpass trial table is added to the Fastpass table. You can specify any integer between 1 and 1,000, inclusive, without commas. The default setting is 15.

The initial probability that a message is scanned for spam after a pass is issued to an IP address | As the IP address continues to send legitimate messages, this sampling rate decreases from this rate. You can specify an integer between 2 and 50, inclusive. You specify only the denominator of the fraction that indicates the probability. The default value is 5, which indicates a 1/5 or 1 in 5 probability.

The list of IP addresses that cannot be granted a pass | You can create this list by adding individual IP addresses or importing a list of IP addresses.

When either table reaches the configured limit, Fastpass discards the least recently used entry to make room for the next entry.

Note that Fastpass only exempts senders from spam scanning. Messages from senders with passes are scanned for viruses and content filtering. However, because these messages are not scanned for spam, they cannot receive Suspected Spam or Spam verdicts.

Senders who are members of the Local Good Sender IPs or Symantec Global Good Senders sender groups cannot receive a pass. However, those senders are already exempted from spam scanning.

The Fastpass database only takes spam, suspected spam, and unwanted message verdicts into account. Virus verdicts, content filtering verdicts, sender authentication verdicts, and sender group verdicts do not affect the granting or revoking of passes.

See “Configuring Fastpass” on page 156.

### Configuring Fastpass

Symantec Messaging Gateway automatically collects data on the level of spam and unwanted messages sent by each IP address, and uses this data to grant or revoke passes. After Symantec Messaging Gateway grants a pass to a sender, it still scans a small sample of the email from that sender for spam and unwanted messages. If Symantec Messaging Gateway identifies a spam or unwanted message, it immediately revokes the pass for that sender.

By default, the Fastpass feature is not enabled. Enabling Fastpass can yield significant savings in processing resources. Fastpass is designed to work without any custom configuration, but you can customize it if needed.

See “About conserving resources using Fastpass” on page 154.
To enable or disable Fastpass

1. In the Control Center, click **Reputation > Policies > Good Senders**.
2. Click **Fastpass**.
3. Check **Enable Fastpass** to enable Fastpass, or uncheck **Enable Fastpass** to disable Fastpass.

To configure Fastpass

1. In the Control Center, click **Reputation > Policies > Good Senders**.
2. Click **Fastpass**.
3. Click **Show Advanced**.
4. In the **Maximum number of sending IPs tracked in the database** field, type an integer between 1,000 and 1,000,000 to change the database size.

   Do not type commas. The database includes two tables. The Fastpass trial table includes sending IPs that are being evaluated for a pass, and is limited to 75% of the maximum database size. The Fastpass table includes sending IPs that currently have a pass, and is limited to 25% of the maximum database size.

   The default value is 250,000.

5. In the **Chance that a new IP will be added to the Fastpass trial table** field, type an integer between 1 and 100, inclusive, to vary the rate of growth of the Fastpass trial table.

   A smaller value results in more frequent sampling. For example, a value of 1 means that every new IP that sends a legitimate message is added to the table. A value of 5 means that a new sending IP, not in the Fastpass trial table has a 20% (1/5 or 1 in 5) chance of being added to the table. All messages from IP addresses in the Fastpass trial table are scanned for spam and unwanted messages. If a spam or unwanted message is received, the entire /24 range of sending IP addresses is removed from both the Fastpass trial table and the Fastpass table.

   The default value is 3, which indicates a 1 in 3 probability.
6 In the **Minimum required legitimate messages before granting fastpass** field, type an integer between 1 and 1,000 to vary the rate of growth of the Fastpass table. Do not type commas. After an IP enters the Fastpass trial table, this value is the number of sequential legitimate messages that must be received from the IP before the IP moves to the Fastpass table. Any spam message received will cause the entire /24 range of IP addresses to be dropped from both tables.

The default value is 15.

7 In the **Initial message sample rate after pass is issued** field, type an integer between 2 and 50, inclusive, to vary the rate at which IPs that have passes and are checked for current behavior.

A smaller value results in more frequent sampling. For example, a value of 2 means that 1 of every 2 messages for an IP just granted a pass is scanned for spam and unwanted messages. A value of 25 means that 1 of every 25 messages is scanned. As additional legitimate messages are received from an IP address, the initial sampling rate is adjusted so that fewer messages are sampled. The sampling rate cannot fall to less than 5 times the initial sampling rate. For example, an initial sampling rate of 8 would gradually decrease as additional legitimate messages are processed, until the sampling rate is 1 message out of 40.

The default value is 5, which indicates a 1 in 5 probability.

**To exclude IPs from receiving Fastpasses**

1 In the Control Center, click **Reputation > Policies > Good Senders**.

2 Click **Fastpass**.

3 Click **Show Advanced**.

4 Under **Fastpass Exclusions**, type the IP addresses you want to exclude from receiving passes in the **IP addresses** field.

You can type multiple IP addresses, separated by commas. You can type fully qualified IP addresses or multiple IP addresses using CIDR notation. Wildcards are not supported. If you specify hostnames, some of the performance benefit of Fastpass is lost, as Symantec Messaging Gateway then needs to look up the hostname of the IP for every sampled message to ensure that it does not match a hostname you have specified to exclude.

5 Click **Import** to import a list of IP addresses.

Imported files must be plain text files containing a single entry per line.

6 Check the box next to the IP address and click **Delete**, to delete and entry from the list.

7 Click **Delete All** to delete all entries on the current page of the list.

8 Click **Export** to export the currently saved list of excluded IPs in a text file.
Defending against bounce attacks

You can enable Symantec Messaging Gateway's Bounce Attack Prevention technology to eliminate non-deliverable receipt (NDR) messages that are a result of redirection techniques commonly used by spammers.

Table 6-6 describes the process to implement Bounce Attack Prevention.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Learn more about bounce attacks and how Symantec Messaging Gateway can help you defend against them.</td>
<td>Bounce attacks can be used to leverage the initial recipient's &quot;good&quot; reputation when sending spam, pollute the initial recipient's IP reputation, or create denial-of-service attacks at the target's server. See “About defending against bounce attacks” on page 160.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure the Control Center settings for Bounce Attack Prevention.</td>
<td>You must configure a seed value in the Control Center. The seed value is used to calculate a tag that is appended to outgoing messages and later used to validate that message if it is returned. See “Configuring the Control Center for Bounce Attack Prevention” on page 161.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure your policy groups to use Bounce Attack Prevention.</td>
<td>Once you configure Bounce Attack Prevention in the Control Center Settings page, you must enable the policy groups to which the system should apply validation and assign a Bounce Attack Prevention policy. See “Configuring policy groups for Bounce Attack Prevention” on page 162.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create policies to prevent bounce attacks.</td>
<td>Lastly, you must enable your policy groups for Bounce Attack Prevention. You assign a spam policy or unwanted mail policy that describes the actions that you want Symantec Messaging Gateway to taken when a message does not pass bounce attack validation. See “Creating an email spam or unwanted email policy for Bounce Attack Prevention” on page 163.</td>
</tr>
</tbody>
</table>
About defending against bounce attacks

A bounce attack occurs when a spammer obscures message origins by using one email server to bounce spam to an address on another server. The spammer does this by inserting a target address into the “Mail From” value in the envelope of their messages then sending those messages to another address.

If the initial recipient finds the message undeliverable, that mail server recognizes the forged "Mail From" value as the original sender, and returns or "bounces" the message to that target. When the targeted system recognizes the server from which the message was bounced as a legitimate sender, it accepts the message as a legitimate non-deliverable receipt (NDR) message.

Bounce attacks can be used to leverage the initial recipient's "good" reputation when sending spam, pollute the initial recipient's IP reputation, or create denial of service attacks at the target's server.

Once your system is configured for Bounce Attack Prevention, Symantec Messaging Gateway calculates a unique tag that uses the provided seed value as well as the current date. Your Scanner attaches this tag to outbound messages sent by users in your defined policy groups.

Note: For successful processing you must also ensure that all of your applicable outbound mail is routed through the appliance.

If the message is then returned as undeliverable, the envelope's return address will contain this tag.

When the system receives a message that appears to be a message returned as undeliverable, the system will compare the inbound message’s recipient with the policy group configuration to see if the user's policy group is configured for Bounce Attack Prevention. If the policy group is configured, the system calculates a new tag that includes the seed value and current date, then uses that new tag to validate the tag in the email.

A valid tag on an inbound NDR will include the following:

■ The correct tag format
■ A seed value that matches the seed value in the new calculated tag
■ A date that falls within a week of the new calculated tag

Based on this evaluation, Symantec Messaging Gateway will do the following:

■ If the system determines that the tag is valid, the system strips the tag from the envelope and sends the message forward for filtering and delivery per your mail filtering configuration.
■ If there is no tag, or the tag content is found to not match the tag that is calculated for validation, the address will be rewritten without tag information then managed per your Bounce Attack Prevention policy configuration. An error will be logged and this message
will be accounted for in your message statistics as a message with a "single threat." The message is also included in your system spam statistics as a "bounce threat."
If your policy defines an action other than "reject" when the message fails validation, the message can acquire more threats and could then be counted in your statistics as a "multiple threat."

- If, due to an unrecognizable format, validation cannot be performed by the system, the system will not strip the tag and will keep the tag as part of the address. The system will then act upon this message based on the actions you define in your spam policy configuration.

**Note:** Bounced messages over 50k are truncated. Attachments in truncated messages may be unreadable.

See “Defending against bounce attacks” on page 159.

**Configuring the Control Center for Bounce Attack Prevention**

You must configure Bounce Attack Prevention in the Control Center by providing a seed value that will be used to calculate a tag that will be appended to outgoing messages and later used to validate that message if it is returned.

See “About defending against bounce attacks” on page 160.

**To create a seed value to be used when creating validation tags for outgoing messages**

1. In the Control Center, select **Administration > Settings > Control Center**.
2. Click the **Certificates** tab.
3. Under **Control Center Certificate**, enter a **Bounce attack prevention seed**.
   This seed value should consist of eight alphanumeric characters.
4. Click **Save**.

**Warning:** If you are running your inbound and outbound messages on different Scanners with different Control Centers, repeat steps 1 through 3 for each Control Center, using the same seed value. This ensures that all inbound and outbound servers are calculating the same tags for validation.

**Note:** For successful processing you must ensure that all of your applicable outbound mail is routed through the appliance.
You must now enable Bounce Attack Prevention for your policy groups and assign a spam policy that describes the actions to be taken when a message does not pass bounce attack validation. If you do not enable at least one policy group for Bounce Attack Prevention, Bounce Attack Prevention will be disabled and your system will not be protected from bounce attacks.

See “Configuring policy groups for Bounce Attack Prevention” on page 162.

A default spam policy is provided, called "Failed Bounce Attack Validation: Reject message". You can use this policy as is, edit it, or create your own policy.

See “Creating an email spam or unwanted email policy for Bounce Attack Prevention” on page 163.

Configuring policy groups for Bounce Attack Prevention

Once you configure Bounce Attack Prevention in the Control Center Settings page, you must enable the policy groups to which the system should apply validation and assign a Bounce Attack Prevention policy.

See “About defending against bounce attacks” on page 160.

To configure policy groups for Bounce Attack Prevention

1. In the Control Center, select Administration > Users > Policy Groups.
2. Select the policy group you want to edit, or create a new one, then select the Spam tab for that policy group.
3. Under Email, check Enable bounce attack prevention for this policy group.
4. For the Bounce attack prevention policy, select the policy you want to apply to bounced messages.

   This policy must contain the condition, "If a message fails bounce attack validation" and actions to be taken should bounce address tag validation fail. Symantec Messaging Gateway provides a default policy: "Failed Bounce Attack Validation: Reject message." This default policy is configured to reject messages that fail tag validation.

   You can also edit this policy or create a new one.

   See “Creating an email spam or unwanted email policy for Bounce Attack Prevention” on page 163.

5. Click Save.

   For successful processing, you must ensure that all of your applicable outbound mail is routed through the appliance.
Creating an email spam or unwanted email policy for Bounce Attack Prevention

To enable Bounce Attack Prevention, you must enable your policy groups for Bounce Attack Prevention and assign a spam policy or unwanted email policy that describes the actions to be taken when a message does not pass bounce attack validation.

See “About defending against bounce attacks” on page 160.

Symantec Messaging Gateway provides you with a default bounce policy called "Failed Bounce Attack Validation: Reject message". This default policy provides one action, which is to reject all messages that fail tag validation. You can edit this policy to change the actions taken, or you can create a new policy to suit your specific needs.

Create an email spam or unwanted email policy for Bounce Attack Prevention conditions

1. In the Control Center, click Spam > Policies > Email.
2. Click Add to create a new policy.
3. Enter a name for the new policy, and for If the following condition is met: select "If a message fails bounce attack validation".
   
   The apply to field will automatically be set to "inbound messages" and disabled. You can only configure an inbound policy for this condition. The outbound policy is static and cannot be modified.
4. Select the actions that should be applied if a bounce message fails validation. An action "Reject messages failing bounce attack validation" is provided, or you can select any other action as desired.
   
   Be sure to consider your existing spam policies and how they might affect your overall email configuration.
5. Under Apply to the following policy groups, select the policy groups to which you want to apply this policy.
6. Click Save.

Researching IP address reputation

Use the IP Reputation Lookup page to research historical and current statistical information about a particular IPv4 address or IPv6 address. You can view the sender groups (if any) that currently include the IP address, add the IP address to your Local Good Sender IPs or Local Bad Sender IPs sender groups, or clear the current sender policy of the IP address. When you clear the sender policy, Symantec Messaging Gateway removes the IP address from the Local Good Sender IPs or Local Bad Sender IPs group.
You can also reset the local reputation of an IP address (thereby clearing the data used to manage the connections given to that IP address). The page displays data collected since the last time the spam reputation was reset for the specified IP address.

The IP reputation functionality is designed to render verdicts when traffic crosses your organization's gateway, before it enters your network. The full benefit of this feature comes from the ability to reject or defer bad connections before the traffic enters your network and consumes resources. This works best when your Symantec Messaging Gateway is deployed at the network edge. However, if you have deployed Symantec Messaging Gateway behind relays or elsewhere within your network, verdicts can still be rendered based on the contents of the received headers.

**Note:** Historical data for this page is not available unless you have configured Symantec Messaging Gateway to store this data on an ongoing basis. You can do this on the Administration > Settings > Reports page. Under Reports Data Storage, check Sender IP connections, and click Save.

To check current and historical information for an IP address

1. In the Control Center, click Reputation > Reputation Tools > IP Reputation Lookup.
2. Specify the IPv4 address or IPv6 address that you want to query.
   You can specify individual IPv6 addresses in any standard IPv6 format.
3. Click Find.

The following information appears for an IP address that you specify:

<table>
<thead>
<tr>
<th>Table 6-7</th>
<th>Reputation Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Add to Local Good Sender IPs</td>
<td>Click to add this IP address to your Local Good Sender IPs group. Connections from IP addresses in Local Good Sender IPs are allowed by default, and the messages bypass spam filtering.</td>
</tr>
<tr>
<td>Add to Local Bad Sender IPs</td>
<td>Click to add this IP address to your Local Bad Sender IPs group. Connections from IP addresses in Local Bad Sender IPs are rejected by default.</td>
</tr>
<tr>
<td>Clear Sender Policy</td>
<td>Click to remove this IP address from either the Local Bad Sender IPs or Local Good Sender IPs group.</td>
</tr>
</tbody>
</table>
### Table 6-7 Reputation Status (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bad Reputation - Global Bad Senders</strong></td>
<td>If this IP address is in the Symantec Global Bad Senders group, a green checkmark appears. If not, a black dash appears. If the Symantec Global Bad Senders group is disabled on the Bad Senders page, this column is grayed out.</td>
</tr>
<tr>
<td><strong>Request Removal</strong></td>
<td>This link appears only if the IP address is in the Symantec Global Bad Senders group. Click the link to request that Symantec remove this IP address from Symantec Global Bad Senders.</td>
</tr>
<tr>
<td><strong>Bad Reputation - Local Bad Sender IPs</strong></td>
<td>If this IP address is in the Local Bad Sender IPs group, a green checkmark appears. If not, a black dash appears. If the Local Bad Sender IPs group is disabled on the Bad Senders page, this column is grayed out.</td>
</tr>
<tr>
<td><strong>Good Reputation - Global Good Senders</strong></td>
<td>If this IP address is in the Symantec Global Good Senders group, a green checkmark appears. If not, a black dash appears. If the Symantec Global Good Senders group is disabled on the Good Senders page, this column is grayed out.</td>
</tr>
<tr>
<td><strong>Good Reputation - Local Good Sender IPs</strong></td>
<td>If this IP address is in the Local Good Sender IPs group, a green checkmark appears. If not, a black dash appears. If the Local Good Sender IPs group is disabled on the Good Senders page, this column is grayed out.</td>
</tr>
</tbody>
</table>

**Note:** An IP address can be in the Local Good Sender IPs group or in the Local Bad Sender IPs group, but not in both. Therefore, if the IP address is currently in one of the two groups, that add button appears grayed out. You can click the button for the other group to switch the IP address from one group to another.
After you click and confirm this action, Symantec Messaging Gateway "forgets" all previous reputation data on this sender. This action clears the **Current Action**, **Message Volume**, and **Total % Spam** columns. However, if the sender is in any of the Local Good Sender IPs, Local Bad Sender IPs, or Fastpass sender groups, the sender remains in those groups. To remove the sender from any of these sender groups, click **Clear Sender Policy**. Clicking **Reset Status** also moves the sender to the default Connection Classification class.

See “About managing connection load at the gateway” on page 143.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset Status</td>
<td>After you click and confirm this action, Symantec Messaging Gateway &quot;forgets&quot; all previous reputation data on this sender. This action clears the <strong>Current Action</strong>, <strong>Message Volume</strong>, and <strong>Total % Spam</strong> columns. However, if the sender is in any of the Local Good Sender IPs, Local Bad Sender IPs, or Fastpass sender groups, the sender remains in those groups. To remove the sender from any of these sender groups, click <strong>Clear Sender Policy</strong>. Clicking <strong>Reset Status</strong> also moves the sender to the default Connection Classification class. See “About managing connection load at the gateway” on page 143.</td>
</tr>
<tr>
<td>Scanners</td>
<td>The Scanners that have seen traffic from this IP address. Each Scanner in your installation has its own line.</td>
</tr>
<tr>
<td>Current Action</td>
<td>This line displays the action that will be taken on connections from this IP address based on the information in the IP Reputation database. Connections from a given IP address can be assigned one of the following actions: 1. Reject: This IP address is in a Bad Sender Group and the action for that group is to reject the SMTP connection. 2. Defer: This IP address is in a Bad Sender Group and the action for that group is to defer the SMTP connection. 3. Skip AS Filtering: This IP address is in a Good Sender Group and the action for that group is to deliver the message normally. Although Symantec Messaging Gateway will not filter messages from this IP address for spam, the messages will undergo all other filtering, including antivirus filtering. 4. Filter Partially: This IP address was granted a pass by the Fastpass feature. In most cases, Symantec Messaging Gateway does not filter messages from this IP address for spam. However, Symantec Messaging Gateway does filter a sample of the messages for spam. All the messages undergo all other filtering, including antivirus filtering. 5. Filter Normally: This IP address has no negative local or global reputation, and has not been granted a pass by the Fastpass feature.</td>
</tr>
<tr>
<td>Message Volume</td>
<td>The quantity of messages from this IP address. One of the following four values appears: 1. None (this is the default value) 2. Low 3. Medium 4. High</td>
</tr>
<tr>
<td>Total % Spam</td>
<td>The percentage of messages from this IP address identified as spam</td>
</tr>
</tbody>
</table>
Table 6-8  Local status (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Class</td>
<td>The connection class (1-9 or Default) assigned to this IP address on this Scanner. Connection Classification defers a higher percentage of connections from IP addresses in higher (worse) classes. For IPv6 addresses, the connection class is always &quot;1&quot;.</td>
</tr>
<tr>
<td>Fastpass</td>
<td>If this IP address currently has a pass granted by the Fastpass feature on this Scanner, a green check appears in this column. If not, a black dash appears. IPv6 addresses are not supported.</td>
</tr>
<tr>
<td>DHA</td>
<td>If this IP address is under DHA restriction based on your settings in Reputation &gt; Bad Senders &gt; Directory Harvest Attack, a green check appears. If not, a black dash appears. IPv6 addresses are not supported.</td>
</tr>
<tr>
<td>Virus Attack</td>
<td>If this IP address is under Virus Attack restriction based on your settings in Reputation &gt; Bad Senders &gt; Email Virus Attacks, a green check appears. If not, a black dash appears. IPv6 addresses are not supported.</td>
</tr>
<tr>
<td>Last Message</td>
<td>The last time traffic was seen from this IP address.</td>
</tr>
</tbody>
</table>

Table 6-9  Local connection history

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time range</td>
<td>Choose the time range for the data displayed in the Local Connection History table. You can choose the past hour, the past day, or the past week.</td>
</tr>
<tr>
<td>Attempted</td>
<td>The number of connections from this IP address attempted within the specified time range.</td>
</tr>
<tr>
<td>Accepted</td>
<td>The number of connections from this IP address accepted within the specified time range.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The number of connections from this IP address rejected within the specified time range.</td>
</tr>
<tr>
<td>Deferred</td>
<td>The number of connections from this IP address deferred within the specified time range.</td>
</tr>
</tbody>
</table>

To check sender group membership for a domain, email address, or IP address

1. In the Control Center, click Reputation > Reputation Tools > Find Sender.
2. Type a domain, email address, or IP address.
3. Click Find Sender.

If the sender is any of the following groups, the name of the group appears:
- Local Bad Sender Domains
- Local Bad Sender IPs
- Third Party Bad Senders
- Local Good Sender Domains
- Local Good Sender IPs
- Third Party Good Senders
Setting up certificates

This chapter includes the following topics:

- About certificates
- Working with certificates
- PEM format requirements for certificates and domain keys
- Viewing an SMTP/TLS or HTTPS certificate
- Exporting a TLS and HTTPS certificate
- Deleting SMTP/TLS or HTTPS certificates
- Assigning an MTA TLS certificate to a Scanner
- Assigning a user interface HTTPS certificate to the Control Center

About certificates

Certificates secure and authenticate communications between client and server IP addresses or domains. You can generate a self-signed certificate or import a signed certificate that a Certificate Authority (CA) issues.

Note the differences between the types of certificates:

- A self-signed certificate has not been signed by a certificate authority.
- A root certificate authority certificate (root CA certificate) is the certificate identifying a specific certificate authority.
- An intermediate certificate authority certificate (intermediate CA certificate) identifies an additional party with responsibility for a certificate, and may be required to provide a complete validation chain for the certificate signature.
A certificate authority-signed certificate has been signed by a certificate authority. In order to ensure that a certificate authority-signed certificate is accepted as valid, make sure that the CA certificate for the certificate authority that signed the certificate appears in the CA Certificates list on the Certificate Authority tab of the Certificate Settings page.

For successful HTTPS authentication using a CA certificate, there must be a complete "path" or "chain" from the client certificate to a CA certificate. Additionally, both participants in the negotiation must recognize the signing authority. Symantec Messaging Gateway includes pre-installed root CA certificates for the most common Certificate Authority vendors. The Certificate Authority tab on the Certificate Settings page lists the pre-installed root CA certificates. You can add additional root or intermediate CA certificates. Some certificate issuers require and provide an intermediate CA certificate for the certificates that they issue for additional security.

For SMTP/TLS authentication using a CA certificate, Symantec Messaging Gateway allows you to use a certificate even if there is not a complete path or chain from the client certificate to a CA certificate.

After you add a certificate, assign it to the Control Center to secure Web-based communications or to a Scanner MTA to support TLS encryption.

MTA TLS certificate

The inbound, outbound, and authentication mail processes in each Scanner use the TLS certificate that is assigned to them to accept messages for scanning and to send TLS-encrypted messages.

See “Assigning an MTA TLS certificate to a Scanner” on page 185.

User interface HTTPS certificate

The Control Center uses the HTTPS certificate to secure communications from Web browsers.

See “Assigning a user interface HTTPS certificate to the Control Center” on page 186.

Note: When you purchase or generate a certificate, you may be able to specify whether you intend to use it for SMTP/TLS or HTTPS. A certificate authority may require you to import an intermediate CA certificate in addition to the certificate itself. Make sure that you install both the certificate and any intermediate certificate that you receive from the certificate authority.

You can add CA-signed certificates to the list of available certificates in one of the following ways:

- Generate a self-signed certificate by completing the Add Certificate page. The self-signed certificate is immediately available as an HTTPS certificate for the Control Center and for Scanner MTAs for accepting TLS encryption.

- Add a certificate authority-signed certificate by submitting a certificate signing request that you generated on the Add Certificate page to a certificate authority. When you receive
the certificate back from the certificate authority, save it locally and import it to the Control Center to add it to the list of available certificates.

- Import a certificate authority-signed certificate that you previously exported from a Symantec Messaging Gateway appliance.
- Update an existing certificate authority-signed certificate with a new certificate that differs only in dates of validity.
- Add a certificate authority-signed certificate without generating a certificate signing request in the Control Center. You must first modify the certificate. The certificate must be in PEM format.

See “Working with certificates” on page 171.

Working with certificates

You can set up certificates through the Control Center.

Table 7-1 describes the tasks that you can perform with certificates. You can perform these tasks as needed in any order.

Table 7-1  Working with certificates

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new self-signed certificate.</td>
<td>A self-signed certificate can be used for either HTTPS communication or SMTP/TLS. Some mail servers may not be able to recognize a self-signed certificate that is used for SMTP/TLS. Many mail servers require a certificate authority-signed certificate. See “Adding a self-signed certificate” on page 173.</td>
</tr>
<tr>
<td>Decide which method you want to use to add a certificate authority-signed certificate.</td>
<td>This topic describes the methods that you can use to add a certificate authority-signed certificate. See &quot;Methods to add a Certificate Authority signed certificate&quot; on page 173.</td>
</tr>
<tr>
<td>Add certificate authority-signed certificates by importing them.</td>
<td>You can add a certificate authority-signed certificate without generating a certificate signing request in the Control Center. See “Modifying a Certificate Authority signed certificate import file” on page 175.</td>
</tr>
</tbody>
</table>
Table 7-1  Working with certificates (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add your own CA or intermediate certificates.</td>
<td>Symantec Messaging Gateway includes preinstalled CA certificates for many common certificate authority vendors. Add a CA certificate if a certificate authority issues you an SMTP/TLS or HTTPS certificate and that certificate authority's CA certificate is not already in the Control Center. Another reason to add a CA certificate is if your certificate requires an intermediate CA certificate. When you add the CA certificate, you complete the certificate chain to permit authentication of a certificate authority-signed certificate. See “Adding a CA or an intermediate certificate” on page 175.</td>
</tr>
<tr>
<td>See an inventory of all of your CA certificates.</td>
<td>You can view a list of the currently installed CA certificates. See “Viewing existing CA certificates” on page 176.</td>
</tr>
<tr>
<td>Request a certificate authority-signed certificate.</td>
<td>A certificate authority-signed certificate is more likely than a self-signed certificate to be effective for SMTP/TLS communication. It can also be used for HTTPS communication. Some possible CAs to use are listed on the Certificate Authority tab in the Control Center. However, other CAs are also supported. See “Requesting a Certificate Authority signed certificate” on page 176.</td>
</tr>
<tr>
<td>Import a certificate authority-signed certificate into the Control Center.</td>
<td>When you receive a certificate from a certificate authority (CA), you must import it to make it available in the Control Center. In addition to the certificate, the CA might have sent you an intermediate CA certificate that you also need to install in the Control Center. See “Importing a Certificate Authority signed certificate” on page 177.</td>
</tr>
<tr>
<td>Export a certificate to import on a different Symantec Messaging Gateway appliance or store as a backup.</td>
<td>You do not need to modify the certificate import file before import. See “Exporting a TLS and HTTPS certificate” on page 184.</td>
</tr>
<tr>
<td>Replace all existing CA certificates in the Control Center with another set of CA certificates.</td>
<td>All existing CA certificates are removed and replaced with the CA certificates in the file that you specify. See “Replacing all existing CA certificates” on page 178.</td>
</tr>
<tr>
<td>Back up CA certificates.</td>
<td>You can back up the CA certificates that are installed in the Control Center. See “Backing up CA certificates” on page 179.</td>
</tr>
</tbody>
</table>
Adding a self-signed certificate

A self-signed certificate can be used for either HTTPS communication or SMTP/TLS. A self-signed certificate used for SMTP/TLS may not be recognized by some email servers. Many email servers require a certificate authority-signed certificate. A self-signed certificate is not recommended for SMTP/TLS.

To add a self-signed certificate

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the TLS & HTTPS Certificates tab.
3. Click Add.
4. In the Certificate name box, type a name for the certificate.
5. In the Certificate type drop-down list, choose Self Signed.
6. Complete the remainder of information on the page.
7. Click Create.

See “Methods to add a Certificate Authority signed certificate” on page 173.

See “About certificates” on page 169.

Methods to add a Certificate Authority signed certificate

Table 7-2 describes the methods that you can use to add a certificate authority-signed certificate.
## Table 7-2  Methods of adding a certificate authority-signed certificate

<table>
<thead>
<tr>
<th>Method</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit a certificate signing request that you generated on the <strong>Add Certificate</strong> page to a certificate authority. When you receive the certificate back from the certificate authority, save it locally and import it to the Control Center to add it to the list of available certificates.</td>
<td>See “Requesting a Certificate Authority signed certificate” on page 176.</td>
</tr>
<tr>
<td>Export a certificate authority-signed certificate or a self-signed certificate from a Symantec Messaging Gateway appliance, then import the certificate.</td>
<td>See “Adding a self-signed certificate” on page 173.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Update an existing TLS &amp; HTTPS certificate authority-signed certificate with a new certificate that differs only in dates of validity. To do this, import the updated certificate into the Control Center, leaving the previous certificate in place.</td>
<td>See “Importing a Certificate Authority signed certificate” on page 177.</td>
</tr>
<tr>
<td>Add a certificate authority-signed certificate without generating a certificate signing request in the Control Center. You must first modify the import file. The certificate must be in PEM format.</td>
<td>See “Modifying a Certificate Authority signed certificate import file” on page 175.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order to ensure that a certificate authority-signed certificate is accepted as valid, make sure that the CA certificate for the certificate authority that signed the certificate appears in the **CA Certificates** list on the **Certificate Authority** tab of the **Certificate Settings** page.

See “Adding a CA or an intermediate certificate” on page 175.

After you add a certificate, you can assign it to the Control Center to secure Web-based communications or to a Scanner MTA to support TLS encryption.

See “Assigning a user interface HTTPS certificate to the Control Center” on page 186.

See “Assigning an MTA TLS certificate to a Scanner” on page 185.

Another reason to add a certificate authority certificate is if your TLS and HTTP certificate requires an intermediate certificate authority certificate. When you add a certificate authority-signed certificate, you complete the certificate chain to permit authentication of the
new certificate. All of your configured Scanners can access the certificate authority-signed certificates in the Control Center for SMTP/TLS and HTTPS authentication.

See “About certificates” on page 169.

Modifying a Certificate Authority signed certificate import file

You can add a Certificate Authority signed certificate without generating a certificate signing request in the Control Center. If you have not exported the certificate from a Symantec Messaging Gateway appliance, you must first modify the certificate import file.

See “Methods to add a Certificate Authority signed certificate” on page 173.

See “About certificates” on page 169.

To modify the certificate import file, remove the passphrase from the key used to generate the certificate signing request. Next, combine first the certificate and then the modified key into a new file. Save the combined file locally, and import it into the Control Center to add it to the list of available certificates. The certificate must be in PEM format.

To modify a Certificate Authority signed certificate import file

1. Delete the passphrase from the key used to generate the certificate signing request.

   You can use the following command:

   ```
   # openssl rsa -in key.pem -out key-nopass.pem
   ```

   where `key.pem` is the input filename of the key, and `key-nopass.pem` is the output filename for the key without the passphrase.

2. Create a new text file.

3. Copy the certificate into the new file.

4. Below the certificate, copy the public key without passphrase into the new file.

5. Save the new file locally.

6. Import the file into the Control Center.

   See “Importing a Certificate Authority signed certificate” on page 177.

Adding a CA or an intermediate certificate

Symantec Messaging Gateway includes pre-installed CA certificates for many common certificate authority vendors. Add a CA certificate if a certificate authority issues you an SMTP/TLS or HTTPS certificate and that certificate authority’s CA certificate is not already in the Control Center.
Another reason to add a CA certificate is if your certificate requires an intermediate CA certificate. When you add the CA certificate, you complete the certificate chain to permit authentication of a certificate authority-signed certificate.

See “About certificates” on page 169.

Ensure that you have the CA certificate before you proceed. The CA certificate may have been included when you received the certificate from the certificate authority. Alternatively, you may be able to download the CA certificate from the certificate authority's website. The file that contains the CA certificate must be in PEM format.

See “PEM format requirements for certificates and domain keys” on page 183.

To add a CA or an intermediate certificate

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the Certificate Authority tab.
3. Click Update.
4. On the Update CA Certificates page, click Browse.
5. Locate and select the file that contains the CA or intermediate certificate.
6. Click Update.

A status message appears at the top of the page to indicate success or failure.

Viewing existing CA certificates

You can view a list of the currently installed CA certificates.

See “About certificates” on page 169.

To view existing CA certificates

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the Certificate Authority tab.

The currently installed CA certificates appear.

Requesting a Certificate Authority signed certificate

A certificate authority signed certificate is more likely than a self-signed certificate to be effective for SMTP/TLS communication, and can also be used for HTTPS communication. Before you proceed, determine the CA from which you want to purchase your certificate. Some possible CAs to use are listed on the Certificate Authority tab in the Control Center. However, other CAs are also supported.
For the common name, use the domain name or the fully qualified domain name of the computer where the certificate will be installed. Some CAs may not support certificates that are created using an IP address instead of a domain name for the common name. Check with your CAs.

See “Viewing existing CA certificates” on page 176.

See “About certificates” on page 169.

Each CA has its own set of procedures to request certificates and issue certificates. Consult your CA for details and follow the instructions that are appropriate for your installation.

Note: If you have a certificate authority signed certificate, you can add that certificate even if you have not submitted a certificate signing request. However, if you did not either generate a new certificate signing request in the Control Center, or export the certificate from a Symantec Messaging Gateway appliance, you must first modify the certificate.

See “Modifying a Certificate Authority signed certificate import file” on page 175.

See “Methods to add a Certificate Authority signed certificate” on page 173.

To request a Certificate Authority signed certificate

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the TLS & HTTPS Certificates tab.
3. Click Add.
4. In the Certificate name box, type a name for this certificate.
5. In the Certificate type drop-down list, click Certification Authority Signed.
6. Fill in the information on the remainder of the page as appropriate.
7. Click Create.
8. Copy the block of text that appears, paste it into a text file, and save it.
   Save the generated text as a text file. You can copy and paste the information from the text file into a CA request form at a later time.
9. Submit the Certificate authority signed Request (CSR) to a CA, using the method that the CA requires.

Importing a Certificate Authority signed certificate

When you receive a certificate from a certificate authority (CA), you must import it to make it available in the Control Center. In addition to the certificate, the CA might have sent you an intermediate CA certificate that you also need to install in the Control Center.
Note: You cannot import a digital signature algorithm (DSA) signed certificate.

You can also update an existing TLS & HTTPS certificate authority signed certificate that differs only in its dates of validity. Follow the procedure below to import the updated certificate, leaving the previous certificate intact.

Note: If you have a Certificate Authority signed certificate, you can import that certificate even if you have not generated a certificate signing request. However, if you did not either generate a new certificate signing request in the Control Center, or export the certificate from a Symantec Messaging Gateway appliance, you must first modify the certificate.

See “Modifying a Certificate Authority signed certificate import file” on page 175.

See “Methods to add a Certificate Authority signed certificate” on page 173.
See “About certificates” on page 169.

To import a Certificate Authority signed certificate

1 When you receive the certificate file from the CA, save the file to a location that you can access from the Control Center.

   In some cases you may need to store more than one file, depending on your certificate authority’s requirements.

2 In the Control Center, click Administration > Settings > Certificates.

3 Click the TLS & HTTPS Certificates tab.

4 Click Import.

5 On the Import Certificate page, type the full path and the file name of the certificate or click Browse and choose the file.

6 Click Import.

Replacing all existing CA certificates

You can replace all existing CA certificates in the Control Center with another set of CA certificates. All existing CA certificates are removed and replaced with the CA certificates in the file that you specify.

Ensure that you have the CA certificates before you proceed. The file that contains the CA certificates must be in PEM format.

See “PEM format requirements for certificates and domain keys” on page 183.
See “About certificates” on page 169.
To replace all existing CA certificates

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the Certificate Authority tab.
3. Click Restore.
4. On the Restore CA Certificates page, click Browse and locate the file that contains the CA certificates.
5. Click Restore.

A status message appears at the top of the page to indicate success or failure.

Backing up CA certificates

You can back up the CA certificates that are installed in the Control Center.

See “About certificates” on page 169.

To back up CA certificates

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the Certificate Authority tab.
3. Click Backup.
4. In the browser File Download dialog box, click Save the file and then specify the file location.

The file may be saved to your default browser download directory or in a location that you specify.

Changing a certificate or domain key name

You can change a certificate or domain key name, but you cannot modify any other part of a certificate. To change another part of a certificate, you must create a new certificate.

See “Adding a self-signed certificate” on page 173.

See “Methods to add a Certificate Authority signed certificate” on page 173.

See “Adding a domain key” on page 126.

To change a self-signed or certificate authority-signed certificate name

1. Click Administration > Settings > Certificates.
2. Click the TLS & HTTPS Certificates tab.
3. Check the box beside the certificate that you want to modify.
4. Click Edit.
5 On the **Edit Certificate** page, type the new name of the certificate in the **Certificate name** field.

Certificate names are limited to a maximum of 255 US-ASCII characters.

6 Click **Save**.

**To change a domain key name**

1 Click **Administration > Settings > Certificates**.

2 Click the **Domain Keys** tab.

3 Check the box beside the domain key that you want to modify.

4 Click **Edit**.

5 On the **Edit Domain Key** page, type the new name of the certificate in the **Domain Key name** field.

6 Click **Save**.

---

**Importing an application certificate**

By importing the application certificate into Symantec Messaging Gateway, Symantec Messaging Gateway can authenticate the connection from the application as a trusted client.

For example, assume that you want to synchronize data between Symantec Messaging Gateway and Data Loss Prevention Enforce. You must first obtain a certificate from the Enforce Server. You then import the certificate in Symantec Messaging Gateway. Symantec Messaging Gateway is then permitted to authenticate with the Enforce Server to perform synchronization.

See “Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway” on page 471.

---

**Note:** Digital signature algorithm (DSA) signed certificates are not supported.

See “Methods to add a Certificate Authority signed certificate” on page 173.

See “About certificates” on page 169.

You must have Full Administration rights or rights to modify Manage Settings to import an application certificate.

**To import an application certificate**

1 When you receive the certificate file from the application, save the file to a location that you can access from the Control Center.

2 In the Control Center, click **Administration > Settings > Certificates**.

3 Click the **Applications** tab.
4 Click **Import**.

5 On the **Import Application Certificate** page, in the **Administrator** field, choose an administrator who has Modify rights to all Content Incident Folders.

---

**Note:** This administrator will be credited in the logs for all future actions in the application interface that use this certificate.

---

6 In the **Certificate name** field, type a descriptive name for the certificate.

7 In the **File Name** field, type the full path and the file name of the certificate or click **Browse** and choose the file.

8 Click **Import**.

### Exporting an application certificate

You can export an application certificate from Symantec Messaging Gateway. When you import this certificate into an application, that application is able to authenticate with Symantec Messaging Gateway.

---

**Warning:** Exporting an application certificate can create significant security risk. The export file contains all the data necessary to authenticate as your server.

---

As a best practice, you may also want to export a certificate for backup or disaster recovery preparation purposes.

See "**Methods to add a Certificate Authority signed certificate**" on page 173.

See "**Importing an application certificate**" on page 180.

You must have Full Administration rights or rights to modify Manage Settings to export an application certificate.

#### To export an application certificate

1 In the Control Center, click **Administration > Settings > Certificates**.

2 Click the **Applications** tab.

3 Check the box beside the certificate that you want to export.

4 Click **Export**.

5 Save the file to a secure location.
Working with application certificates

In addition to the ability to import and export application certificates, you can also perform the following tasks:

**Edit**
- Lets you modify the certificate name and administrator.
- You may want to modify the certificate name to distinguish it from similar certificates.

**Delete**
- Lets you delete one or more certificates that you specify.
- You may want to delete unneeded certificates to keep the list of certificates manageable.

**Warning:** Once a certificate is deleted, it can only be retrieved from a full backup or a custom configuration backup.

See “Restoring an appliance from backups” on page 711.

**View**
- Lets you view the certificate that you specify.
- You can view the details of a certificate to verify its validity.

You must have Full Administration rights or rights to modify Manage Setting to work with application certificates.

To work with application certificates

1. Click **Administration > Settings > Certificates**.
2. Click the **Applications** tab.
3. Check the box beside the certificate that you want to work with.
4. Perform any of the following tasks:

   - **Click Edit.** Click the drop-down menu to change the administrator or modify the certificate name, and then click **Save**.
   - **Click Delete.** In the confirmation dialog box, click **Delete**.
   - **Click View.** After you view the details of the certificate, click **OK** to return to the applications certificates list.

5. Click **Save**.

See “Importing an application certificate” on page 180.

See “Exporting an application certificate” on page 181.
PEM format requirements for certificates and domain keys

When you add a certificate, whether self-generated or Certificate Authority-signed, and when you import a domain key, ensure that the certificate or domain key meets the following requirements:

- The certificate or domain key must be stored in a file in PEM format with the certificate or domain key included as Base64-encoded text between the following markers:
  - For a certificate, \texttt{-----BEGIN CERTIFICATE-----} and \texttt{-----END CERTIFICATE-----}.
  - For a PKCS#8 domain key, \texttt{-----BEGIN PUBLIC KEY-----} and \texttt{-----END PUBLIC KEY-----}.
  - For an OpenSSL domain key, \texttt{-----BEGIN RSA PRIVATE KEY-----} and \texttt{-----END RSA PRIVATE KEY-----}.

  Any text outside of the begin and end markers is ignored.

- The formats for certificates and domain keys are identical, except for the beginning and ending markers.
  - Base64 text consists of only uppercase and lowercase Roman alphabet characters (A–Z, a–z), the numerals (0–9), and the "+" and "/" symbols.

- The file must be encoded as US-ASCII or UTF. The file cannot contain extended ASCII or non-ASCII characters.

- When you add or replace CA certificates (Update or Restore), a file can contain multiple certificates.

- The extension of the file that contains the certificate or domain key does not matter. The .txt or .crt extension are typically used for certificates, and the .key extension is typically used for domain keys.

- The file that contains the certificate or domain key must be accessible from the browser that you use to access the Control Center.

The following is a sample PEM format CA certificate:

\begin{verbatim}
Text before Begin Certificate is ignored.
-----BEGIN CERTIFICATE-----
MIICPTCCAyCEQDun9W8N/kvFT+IqyzcqpVMAoGCSqGSIb3DQEBAgUAMF8xCzAJBgNV
BAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE3MDUGA1UECxMuQ2xhc3Mg
MSBQdWJsaWMgdWJsb2dvCzAJBgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwi
gSW5jLjE3MDUGA1UECxMuQ2xhc3MgMSBQdWJsaWMgdWJsb2dvCzAJBgNVBAYTAlVE
BAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE3MDUGA1UECxMuQ2xhc3MgMSBQ
dWJsaWMgdWJsb2dvCzAJBgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE3
MDUGA1UECxMuQ2xhc3MgMSBQdWJsaWMgdWJsb2dvCzAJBgNVBAYTAlVTMRcwFQYDVQQK
Ew5WZXJpU2lnbiwgSW5jLjE3MDUGA1UECxMuQ2xhc3MgMSBQdWJsaWMgdWJsb2dvCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE3MDUGA1UECxMuQ2xhc3Mg
MSBQdWJsaWMgdWJsb2dvCzAJBgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLj
-----END CERTIFICATE-----
\end{verbatim}
When you add a domain key, Symantec Messaging Gateway generates the domain key in a way that meets PEM format requirements.

See “Adding a CA or an intermediate certificate” on page 175.

See “Adding a self-signed certificate” on page 173.

See “Importing a domain key” on page 127.

See “Adding a domain key” on page 126.

**Viewing an SMTP/TLS or HTTPS certificate**

You can view any of your SMTP/TLS or HTTPS certificates.

See “Viewing existing CA certificates” on page 176.

To view an SMTP/TLS or HTTPS certificate

1. In the Control Center, click **Administration > Settings > Certificates**.
2. Click the **TLS & HTTPS Certificates** tab.
3. Check the box beside the certificate that you want to view.
4. Click **View**.

**Exporting a TLS and HTTPS certificate**

You can export any certificate from a Symantec Messaging Gateway appliance and then import that certificate. You may also want to export a certificate for backup or disaster recovery preparation purposes.

---

**Warning:** Exporting a certificate can create significant security risk. The export file contains all the data necessary to authenticate as your server.

---

**Note:** You cannot export a certificate-signing request.
See “Methods to add a Certificate Authority signed certificate” on page 173.

See “Importing a Certificate Authority signed certificate” on page 177.

To export a TLS and HTTPS certificate

1. In the Control Center, click Administration > Settings > Certificates.
2. Click the TLS & HTTPS Certificates tab.
3. Click the checkbox next to the single certificate you want to export.
4. Click Export.
5. Save the file to a secure location.

Deleting SMTP/TLS or HTTPS certificates

You can view or delete a certificate. You cannot delete a certificate that is in use for SMTP/TLS or HTTPS authentication.

See “Viewing an SMTP/TLS or HTTPS certificate” on page 184.

To delete SMTP/TLS or HTTPS certificates

1. Click Administration > Settings > Certificates.
2. Click the TLS & HTTPS Certificates tab.
3. Check the boxes next to the certificates that you want to delete.
4. Click Delete.

A confirmation window appears.

Assigning an MTA TLS certificate to a Scanner

You can assign an MTA TLS certificate to a Scanner. You need to do this if you want the Scanner to send or accept TLS-encrypted messages for scanning of inbound or outbound mail, or for authentication.

See “About certificates” on page 169.

You can also assign a certificate for SMTP authentication.

See “Configuring SMTP authentication mail settings” on page 106.

You can use a self-signed or Certificate Authority signed certificate. You may also need to install an intermediate or root CA certificate, to ensure that the certificate chain is verifiable. For SMTP/TLS authentication, Symantec Messaging Gateway allows you to use a certificate authority-signed certificate even if there is not a complete path or chain from the client certificate to a certificate authority-signed certificate.
See "Methods to add a Certificate Authority signed certificate" on page 173.

To assign an MTA TLS certificate to a Scanner

1. In the Control Center, click Administration > Hosts > Configuration.
2. Check the box beside the host that you want, and click Edit.
3. Click the SMTP tab.
4. Under either Inbound Mail Settings, Outbound Mail Settings, or Authentication Mail Settings, check Accept TLS encryption if you want this Scanner to scan for inbound or outbound TLS-encrypted email, respectively.
5. In the adjacent drop-down list, choose the MTA TLS certificate that is appropriate to the inbound, outbound, or authentication mail flow.

You can assign the same certificate to both inbound, outbound, and authentication TLS-encrypted email filtering.
6. Check Request client certificate if you want the inbound or authentication connecting client to present its TLS certificate for authentication.

Clients that do not authenticate successfully will not be allowed to send mail to the appliance.

This step is not applicable to outbound mail flow.

You may need to install an intermediate certificate authority-signed certificate or CA certificate to authenticate the connecting client's TLS certificate.
7. For authentication only, you can check Require TLS encryption.

Clients that do not use TLS encryption will not be able to authenticate.
8. Click Save.

Assigning a user interface HTTPS certificate to the Control Center

You can assign a user interface HTTPS certificate to the Control Center. You can use either a self-signed certificate or a certificate authority-signed certificate. If you use a certificate authority-signed certificate, you may need to install an intermediate or root CA certificate, to ensure that the certificate chain is verifiable.

See “About certificates” on page 169.

See “Adding a CA or an intermediate certificate” on page 175.
To assign a user interface HTTPS certificate to the Control Center

1 In the Control Center, click **Administration > Settings > Control Center**.
2 Click the **Certificates** tab.
3 Click the **User interface HTTPS certificate** drop-down list and select a certificate.
4 Click **Save**.
Configuring policy groups

This chapter includes the following topics:

- About policy groups
- Creating policy groups and assigning policies
- About managing policy group members
- Editing, deleting, enabling, or disabling a policy group
- About selecting filtering policies for policy groups
- Enabling and disabling end user settings for policy groups
- Allowing or blocking email based on language
- Setting policy group precedence

About policy groups

Policy groups are sets of users. You apply your spam, malware, threat defense, and content filtering policies to policy groups. You can also enable an Administration Policy, enable end user quarantine or end user setting privileges, or set language restrictions for inbound mail for a policy group.

When a message matches the conditions of a policy, the actions that SMG takes for each sender or recipient can be different, based on the policy group membership. For an inbound message, SMG processes the message for each recipient according to the filtering policies in the recipient's policy group. For an outbound message, the sender's policy group determines how the message is processed.

By default, Symantec Messaging Gateway assigns the default filtering policies for spam, malware, and threat defense to the policy groups that you create. Content filtering does not
have default policies, so no content filtering policies are assigned to new policy groups. After you create your own filter policies, you can edit your policy groups to assign the new policies.

When a recipient or sender is a member of more than one policy group, only the group with the highest group precedence applies. The higher the group appears in the list on the Administration > Users > Policy Groups page, the higher the group’s precedence.

The Default policy group includes all your users. This policy group is always the last group in the list, to ensure that the policies that you assign to custom policy groups work correctly. You cannot change the position of the Default policy group.

From the Administration > Users > Policy Groups page, you can:

- Set policy group precedence, which determines the policies that are applied to each message.
- Edit the policy group membership and actions.
- Enable and disable the policy groups.
- Delete the policy groups.
- View the policy group information for individual users.

See “Creating policy groups and assigning policies” on page 189.

### Creating policy groups and assigning policies

Table 8-1 describes the process to create policy groups and assign policies to those groups.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a policy group and add members.</td>
<td>Create a policy group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a policy group” on page 190.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Add members to the policy group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding members to a policy group” on page 191.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Assign email message <strong>Virus policies</strong> to a policy group.</td>
<td>Symantec pre-installs email virus policies which you can assign to your policy group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Selecting malware policies for a policy group” on page 196.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Default email malware policies” on page 218.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating email malware policies” on page 217.</td>
</tr>
</tbody>
</table>
Table 8-1 Process for creating policy groups and assigning policies (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3| Assign email message **Spam policies** to a policy group. | Symantec pre-installs email spam policies which you can assign to your policy group.  
See “Selecting spam and unwanted email policies for a policy group” on page 198.  
See “Default email spam and unwanted email policies” on page 250.  
If you want to assign custom email spam policies to a policy group, you must first create these; then, return to this step and apply them.  
See “Creating the policies that detect spam and unwanted email” on page 256. |
| Step 4| Assign content filtering policies to a policy group. | There are no default content filtering policies. You must set these up using predefined templates.  
See the process topic for assigning content filtering policies.  
See “Creating a content filtering policy” on page 325. |

Creating a policy group

The Policy Groups page lists each policy group. The Default policy group is always the last group in the list. The Default policy group contains all users and all domains. Although you can add or modify actions for the Default policy group, you cannot add members to the Default policy group. You cannot delete, disable, or change the precedence of the Default policy group.

**Note:** If you enabled probe participation, the **Probe Account** policy group appears in the list of policy groups. If only this list does not have pre-existing custom policy groups, then **Probe Account** policy group is the first group in the list. You can change the precedence of the **Probe Account** policy group. When you edit the **Probe Account** policy group, the **Probe Accounts** page appears.

To create a policy group

1. In the Control Center, click **Administration > Users > Policy Groups**.
2. On the **Policy Groups** page, click **Add**.
3 In the **Policy group name** field, type a name that identifies this group.

4 Click **Save**.

   After you create a policy group, you can add members.

   See “Adding members to a policy group” on page 191.

---

**Adding members to a policy group**

You can assign members to a policy group based on email addresses, domain names, or LDAP groups for the purpose of applying policies. Once you have created your policy group and added members you can select the policies that you want your group to have.

---

**Note:** There is no edit button for editing policy group members. Use the add / remove method for making changes to member names. For example, if you want to correct a typo in a member's name, you must delete the member then add the member again.

---

If you use distribution lists or groups stored in an LDAP directory as part of your policy group membership, and you make changes to the structure of your directory that causes changes to the distinguished name (DN) of any of the LDAP groups, distribution lists or the users that are members of these LDAP entities, do the following to ensure that the policy group is applied consistently:

- If a policy group member is an LDAP DN, update the DN in the policy group if it has changed.
- Clear the cache on the directory data source that is configured to perform address resolution on those LDAP groups and distribution lists and their user members. This step should be taken even if you reference LDAP distribution lists by email address in your policy groups. See “About the directory data cache” on page 562.

To add a member to a policy group

1 In the Control Center, click **Administration > Users > Policy Groups**.

2 Click the Policy Group you want to edit.

3 Ensure that the **Members** tab is displayed, and click **Add**.

4 Specify members using one of the following methods:

   - Type email addresses, domain names, or both in the box. To specify multiple entries, separate each with a comma, semicolon, or space. To add all recipients of a particular domain as members, type the domain in either of the following formats:

     ```
     domain.com
     *@domain.com
     ```

     SMG interprets the asterisk symbol (*) and question mark (?) symbol literally.
Type in the LDAP distinguished name of a group in the field provided, for example:
\texttt{cn=some ldap group,dc=domain,dc=com}.
Any modification that would change the distinguished name string of direct members added this way must be manually updated in the policy group. To protect mailflow behavior, the new distinguished name string membership should be added to the policy prior to modifying the group and the old distinguished name string should be removed after the modifications have been completed.

Check the box next to one or more LDAP groups.
The LDAP groups listed on this page are loaded from your LDAP server. At least one address resolution function must be enabled and group listing query must be configured to use the LDAP groups list.
See “About using the address resolution function with your data source” on page 512.

5 Click \textbf{Add members} to add the new member(s).

6 Click \textbf{Save} on the Edit Policy Group page.

### Deleting members from a policy group

When policy group members are added or removed, the membership for any address resolution source is rebuilt. If your groups are large, it may take a few moments for your changes to be reflected in the system.

To delete a policy group member

1 In the Control Center, click \textbf{Administration > Users > Policy Groups}.

2 Click the policy group that you want to edit.

3 On the \textbf{Members} tab of the Edit Policy Group page, check the box next to one or more email addresses, domains, or LDAP groups, and then click \textbf{Delete}.

4 Click \textbf{Save}.

### About managing policy group members

You manage policy group membership using tools in the Control Center. You can manually add members (during the policy group creation process); or you can import members from an external file.

See “Adding members to a policy group” on page 191.

See “Importing and exporting policy group members” on page 193.

To locate all policy groups to which a member belongs, use the research option that is provided in the Control Center.

See “Researching policy group membership for a user” on page 194.
There is no edit option for editing policy group members. Use the add / remove method for making changes to member names. For example, if you want to correct a typo in a member's name, you must delete the member then add the member to the group again.

**Importing and exporting policy group members**

You can import policy group members from a file, and you can export group members to a file.

---

**Note:** You cannot import or export LDAP group members described by distinguished names.

---

**To import policy group members from a file**

1. In the Control Center, click **Administration > Users > Policy Groups**.
2. Click the underlined name of the Policy Group that you want to edit.
3. On the **Members** tab of the Edit Policy Group page, click **Import**.
4. Enter the appropriate path and filename (or click **Browse** to locate the file on your hard disk), and then click **Import**.

   Separate each domain or email address in the plain text file with a newline. Below is a sample file:

   ```
   ruth@example.com
   rosa@example.com
   ben*@example.com
   example.net
   *.org
   ```

   The email addresses in the samples behave as follows:

   - ruth@example.com and rosa@example.com match those exact email addresses.
   - ben*@example.com matches ben@example.com and benjamin@example.com, etc.
   - example.net matches all email addresses in example.net.
   - *.org matches all email addresses in any domain ending with .org.

5. Click **Save**.

**To export policy group members to a file**

1. In the Control Center, click **Administration > Users > Policy Groups**.
2. Click the underlined name of the policy group you want to edit.
3. In the Members tab of the Edit Policy Group page, click **Export**.
4. Complete your operating system's save file dialog box as appropriate.
Researching policy group membership for a user

You can identify all of the policy groups to which a user is assigned. Table 8-2 provides examples of how SMG matches policy members based on the criteria that you type.

**Table 8-2** Policy group membership search criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name</td>
<td>You can type the domain name in any of the follow manners:</td>
</tr>
<tr>
<td></td>
<td>■ symantecexample.com</td>
</tr>
<tr>
<td></td>
<td>SMG finds the members that have the email domain symantecexample.com</td>
</tr>
<tr>
<td></td>
<td>or any subdomain such as norton.symantecexample.com and</td>
</tr>
<tr>
<td></td>
<td>sep.norton.symantecexample.com.</td>
</tr>
<tr>
<td></td>
<td>■ *symantecexample.com</td>
</tr>
<tr>
<td></td>
<td>SMG finds the members that have the email domain symantecexample.com</td>
</tr>
<tr>
<td></td>
<td>or any sub domain such as norton.symantecexample.com and</td>
</tr>
<tr>
<td></td>
<td>sep.norton.symantecexample.com.</td>
</tr>
<tr>
<td></td>
<td>■ *.symantecexample.com</td>
</tr>
<tr>
<td></td>
<td>SMG finds the members that have the email domain as any sub domain</td>
</tr>
<tr>
<td></td>
<td>of symantecexample.com such as norton.symantecexample.com and</td>
</tr>
<tr>
<td></td>
<td>sep.norton.symantecexample.com.</td>
</tr>
<tr>
<td></td>
<td>However, it does not find symantecexample.com.</td>
</tr>
<tr>
<td></td>
<td>■ .symantecexample*.com</td>
</tr>
<tr>
<td></td>
<td>SMG finds both symantecexample.com and symantecexample.com.</td>
</tr>
<tr>
<td></td>
<td>If you type a question mark (?) in the domain, SMG treats it as wildcard</td>
</tr>
<tr>
<td></td>
<td>for that position. For example, if you type symante?, SMG finds</td>
</tr>
<tr>
<td></td>
<td>symantec.com and symantenm.com.</td>
</tr>
<tr>
<td>Email address</td>
<td>If you type <a href="mailto:sep.1@symantecexample.com">sep.1@symantecexample.com</a>, SMG the finds the members that</td>
</tr>
<tr>
<td></td>
<td>match <a href="mailto:sep.1@symantecexample.com">sep.1@symantecexample.com</a> and <a href="mailto:sep11@symantecexample.com">sep11@symantecexample.com</a>.</td>
</tr>
<tr>
<td>LDAP domain name</td>
<td>If you type a member domain name such as dc=symantec.mail?tail, dc=com,</td>
</tr>
<tr>
<td></td>
<td>any user that is part of this group appears as a match.</td>
</tr>
<tr>
<td></td>
<td>SMG treats metacharacters such as period (.) or question mark (?) as</td>
</tr>
<tr>
<td></td>
<td>literal characters in LDAP domain names.</td>
</tr>
</tbody>
</table>

To research policy group membership for a user

1. Do one of the following:
   - In the Control Center, click **Administration > Users > Policy Groups**, click on the name of a group, and click **Find User**.
In the Control Center, click **Administration > Users > Find User**.

2 In the **Email address** box, type the user's email address.

3 Click **Find User**.

   The Control Center lists the enabled policy groups in which the specified user exists, in order by policy group precedence.

   See “About policy groups” on page 188.

   See “Creating a policy group” on page 190.

   See “Adding members to a policy group” on page 191.

### Editing, deleting, enabling, or disabling a policy group

The following sections describe common administrative tasks for policy groups.

#### To edit an existing policy group

1 In the Control Center, click **Administration > Users > Policy Groups**.

2 Click the policy name or check the box next to a policy group, and then click **Edit**.

   Add or delete members or change filtering actions for this policy group as you did when you created it.

   See “Creating a policy group” on page 190.

#### To enable a policy group

1 In the Control Center, click **Administration > Users > Policy Groups**.

2 Check the box next to a policy group, and then click **Enable**.

#### To disable a policy group

1 In the Control Center, click **Administration > Users > Policy Groups**.

2 Check the box next to a policy group, and then click **Disable**.

---

**Note:** You cannot disable or delete the Default policy group.

#### To delete a policy group

1 In the Control Center, click **Administration > Users > Policy Groups**.

2 On the Policy Groups page, check the box next to a policy group, and then click **Delete**.
About selecting filtering policies for policy groups

By default, the policy groups that you create are assigned the default filter policies for spam, malware, and content filtering.

The following describes how you can assign custom filter policies to your policy groups (you can perform these tasks as needed in any order):

■ Select email malware policies for policy groups.
  See “Selecting malware policies for a policy group” on page 196.
  Use the index of available malware policies to assist you in customizing your policy groups.
  See “Malware categories and default actions” on page 197.

■ Select spam policies for policy groups.
  See “Selecting spam and unwanted email policies for a policy group” on page 198.

■ Select content filtering policies for policy groups.
  See “Selecting content filtering policies for a policy group” on page 200.

For SMG to filter a policy, the policy must be assigned to at least one policy group and the policy must be enabled.

Selecting malware policies for a policy group

For each policy group, you can specify malware policies. SMG comes with preconfigured malware policies that are enabled by default. When you select malware policies for a policy group, you select from these preloaded policies.

See “Default email malware policies” on page 218.

You can, however, also make your own custom malware policies and apply them to your policy groups. Or, you can modify the default malware policies to fine tune them or to expand or reduce their scope.

See “Creating email malware policies” on page 217.
See “Modifying email malware policies” on page 222.

---

**Note:** By default, messages and attachments that contain malware are cleaned. The inbound messages and outbound messages that contain a mass-mailing worm are deleted. Unscannable messages are deleted as well. You may want to change the default setting for unscannable messages if you are concerned about losing important messages. You can apply different actions to messages that are unscannable for different reasons.
To select malware policies for a policy group

1. In the Control Center, click Administration > Users > Policy Groups.
2. On the Policy Groups page, click the group for which you want to select malware policies.
3. Click the Malware tab.
4. Optionally, click View next to any policy to view the details of that policy.
5. If desired, under Email check Enable inbound email virus scanning for this policy group, and then select the desired policy from each of the following drop-down lists:
   - Inbound antivirus policy
   - Inbound mass-mailing worm policy
   - Inbound encrypted attachment policy
   - Inbound Disarm policy
   - Inbound suspicious attachment policy
   - Inbound spyware/adware policy
   - Inbound unscannable due to limits exceeded policy
   - Inbound unscannable due to other policy
   - Inbound unscannable for Disarm policy
6. If desired, under Email check Enable outbound email virus scanning for this policy group, and then select the desired policy from each of the following drop-down lists:
   - Outbound antivirus policy
   - Outbound mass-mailing worm policy
   - Outbound encrypted attachment policy
   - Outbound Disarm policy
   - Outbound suspicious attachment policy
   - Outbound spyware/adware policy
   - Outbound unscannable due to limits exceeded policy
   - Outbound unscannable due to other policy
   - Outbound unscannable for Disarm policy
7. Click Save.

Malware categories and default actions

Table 8-3 describes the default actions for the SMG malware categories.
Selecting spam and unwanted email policies for a policy group

Spam and unwanted email policies determine what to do with inbound email and outbound email for any of the following conditions:

- If email is spam
  Messages that SMG identifies as spam based on the scores that are derived from pattern matching, filters, and heuristic analysis.

- If email is an unwanted message
  Unwanted messages consist of the following:
  
  - Suspected spam
    Messages that SMG identifies can potentially be spam based on the scores that are derived from pattern matching and heuristic analysis.
  
  - Customer-specific spam
    Messages that SMG identifies as spam based on customer-specific rulesets.
  
  - Marketing mail
    Messages that contain the commercial or fund-raising messages that the user may have requested.
  
  - Newsletters
Messages that include content on specific topics on a known periodic basis (often weekly or monthly), which the user may have requested to receive.

- Emails with redirect URLs
  Redirect URLs include free hosting sites, URL shortening services, and URL redirecting services which can potentially be abused to deliver spam or malware payloads.

SMG installs with the preconfigured default email spam policies and unwanted email policies that you can apply to policy groups.

See “Default email spam and unwanted email policies” on page 250.

---

**Note:** You can also apply custom email spam policies and unwanted email policies. You must first create these policies to make them available from the selection menus.

See “Creating the policies that detect spam and unwanted email” on page 256.

---

To select spam and unwanted email policies for a policy group

1. In the Control Center, click Administration > Users > Policy Groups.
2. On the Policy Groups page, click the policy group for which you want to select spam policies or unwanted email policies.
3. Click the Spam tab.
4. Optionally, click View next to any policy to view the details of that policy.
5. To enable inbound spam scanning, check Enable inbound email spam and unwanted email scanning for this policy group, and then select the required policy from the drop-down list.
6. For each item under Enable inbound email spam and unwanted email scanning for this policy group, click the drop-down list beside the item and select the action. Click View to view the policy details.
   
   The customer-specific spam submission feature must be enabled for customer-specific spam filtering policies to appear in the drop-down list.
7. To enable outbound spam scanning, check Enable outbound email spam and unwanted email scanning for this policy group, and then select the required policy from the drop-down list.
   
   No preconfigured unwanted email policies for outbound messages exist. Unless you create policies for unwanted emails, no policies appear in the drop-down list.
8 For each item under **Enable outbound email spam and unwanted email scanning for this policy group**, click the drop-down list beside the item and select the action. Click **View** to view the policy details.

The customer-specific spam submission feature must be enabled for customer-specific spam filtering policies to appear in the drop-down list.

9 Optionally, check **Enable bounce attack prevention for this policy group**, and then select the desired policy from **Bounce attack prevention policy** drop-down list.

SMG provides a default policy: Failed Bounce Attack Validation: Reject message. You can also edit this policy or create a new policy. The new policy must contain the condition **If a message fails bounce attack validation** and actions to be taken should bounce address tag validation fail.

10 Click **Save**.

You cannot change spam policy details from the **Edit Policy Group** page.

### Selecting content filtering policies for a policy group

By associating an appropriate content filtering policy with a group, you can check messages for attachment types, keywords, or match regular expressions. Depending on the message content, you can add annotations, send notifications, or copy messages to an email address. You can also use your content filtering policies to check for content filtering with statutory regulations or organizational policies.

---

**Note:** Because there are no default content filtering policies, the drop-down list on the **Edit Policy Group** page is initially blank. Before you select content filtering policies for a policy group, you must first create at least one content filtering policy.

---

See “Creating a content filtering policy” on page 325.

**To select content filtering policies for a policy group**

1 In the Control Center, click **Administration > Users > Policy Groups**.

2 On the **Policy Groups** page, click the policy group for which you want to select content filtering policies.

3 Click the **Content Filtering** tab.

4 Check **Enable inbound Content Filtering for this policy group**.
5. Select the desired policy from the **Content Filtering Policies** drop-down list.
   You must already have applied the policy to the group on the **Edit Email Content Filtering Policy** page for it to appear in the drop-down list.
   If you want, click **View** to see a summary of the content filtering policy, and then click **OK** to return to the **Edit Policy Group** page. As you add content filtering policies from the drop-down list, they appear in the bottom list and become unavailable in the drop-down list.

6. Click **Add**.

7. If you want, add additional policies from the **Content Filtering Policies** drop-down list.

8. To configure outbound content filtering policies for the group, check **Enable outbound Content Filtering for this policy group** and follow 5 through 7 again.

9. Click **Save**.
   You cannot change content filtering policy details (such as conditions and actions) from the **Edit Policy Group** page. Although you can add existing policies to the lists on this page, you cannot add new content filtering policies from this page.

---

### Enabling and disabling end user settings for policy groups

End-user settings determine whether end users in a policy group can log into the Control Center to perform either of the following tasks:

- Configure personal Good and Bad Senders lists.
- Block or allow email in specified languages.

---

**Note:** You must have a data source configured for address resolution for this page to be enabled, and both authentication and address resolution data sources are required for the system to execute your settings.

See “**About data sources and functions**” on page 499.

See “**Requirements for enabling end user settings for policy groups**” on page 202.

To log in, users access the same URL in their browser as Control Center administrators: https://<hostname>. The login and password for end users is the same as their LDAP login and password.

For information about supported browsers, see the **SMG Installation Guide**.
Note: For the Good Senders and Bad Senders lists, end users are limited to a total of 200 entries in each list.

Note: Although the language identification technology employed by SMG to identify the language of a message has a high rate of accuracy, false language identifications can occur. Note that messages identified to be in a disallowed language are deleted.

To select end user settings for a policy group

1. In the Control Center, click Administration > Users > Policy Groups.
2. On the Policy Groups page, click the group for which you want to select end user policies.
3. Click the End Users tab.
4. Check Enable end user settings for this policy group.
5. If desired, check Create personal Good and Bad Senders Lists.
6. If desired, check Specify language settings.
7. Click Save.

Requirements for enabling end user settings for policy groups

The following requirements must be satisfied before end users can configure their own personal Good and Bad Senders Lists and block or allow email in specified languages:

- At least one data source is enabled for authentication.
- At least one data source is enabled for address resolution.
- End user preference replication frequency must be set.
- End-user preferences must be enabled for the given policy group on the End Users tab on the Edit Policy Group page.
- Members of the policy group can only be LDAP users, not a locally defined user (that is, an email address you typed manually).

See “Configuring end user quarantine” on page 284.

Allowing or blocking email based on language

Using the language identification offered by SMG, you can block or allow messages written in specified languages for a group. For example, you can choose to only allow English and Spanish messages, or block messages in English and Spanish and allow messages in all other languages.
See “Creating a policy group” on page 190.

See “Adding members to a policy group” on page 191.

To allow or block email based on language for a group

1. In the Control Center, click Administration > Users > Policy Groups.
2. On the Policy Groups page, click the group for which you want to select language policies.
3. Click the Language tab.
4. Click the desired setting.
5. If you chose Only receive mail in the following languages or Do not receive mail in the following languages, check the box for each desired language.

   Available language settings are: Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Portuguese, Russian, and Spanish.
6. Click Save.

Although the language identification technology employed by SMG to identify the language of a message has a high rate of accuracy, false language identifications can occur. Note that messages identified to be written in a disallowed language are deleted.

Setting policy group precedence

The Policy Groups page lists policy groups in a specific order. Policy groups higher in the list have a higher precedence. If a user is a member of multiple groups, the policy group with higher precedence applies in determining how messages are processed for that user.

The Default policy group is always the last group in the list. You cannot change the precedence of the Default policy group. If you enabled probe participation, the Probe Account policy group appears in the list of policy groups.

To set policy group precedence

1. In the Control Center, click Administration > Users > Policy Groups.
2. Click on the group that you want to move, and drag it up or down to the location that you want.

See “Enabling probe participation” on page 317.

See “About policy groups” on page 188.
Detected viruses, malware, and malicious attacks

This chapter includes the following topics:

- About detecting viruses, malware, and malicious attacks
- About Disarm
- What you can do with suspicious attachments
- Spyware or adware verdict details
- Detecting viruses, malware, and malicious threats
- Creating email malware policies
- Managing email malware policies
- Using lists to improve virus scanning performance
- Setting limits on nested files
- Keeping virus definitions current
- Modifying the artificial intelligence sensitivity level

About detecting viruses, malware, and malicious attacks

Viruses and other types of malicious attacks can cause mail server crashes, network downtime, and the compromise and destruction of company data. Symantec Messaging Gateway malware scanning provides virus and malicious threat detection in your email stream.

You create malware policies to protect your server from the following types of attacks:
### Detecting viruses, malware, and malicious attacks

#### About detecting viruses, malware, and malicious attacks

<table>
<thead>
<tr>
<th>Viruses</th>
<th>Symantec Messaging Gateway detects viruses, worms, and Trojan horses in all major file types (for example, Microsoft Word files), including compressed file formats. See “Product technologies that detect viruses and malicious attacks” on page 206.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass-mailer worms</td>
<td>Symantec Messaging Gateway detects that an email message is a mass-mailer worm or virus. It can automatically delete the infected email message and any attachments.</td>
</tr>
<tr>
<td>Suspicious attachments</td>
<td>Symantec Messaging Gateway detects the email messages that exhibit virus-like signs. It also detects the messages that contain a suspicious new pattern of message flow that involves email message attachments.</td>
</tr>
<tr>
<td>Encrypted attachments</td>
<td>Infected files can be intentionally encrypted. Encrypted files cannot be decrypted and scanned without the appropriate decryption tool. You can configure how you want Symantec Messaging Gateway to process encrypted container files.</td>
</tr>
<tr>
<td>Potentially malicious content</td>
<td>Symantec Messaging Gateway’s Disarm technology detects and removes potentially malicious content (PMC) from email attachments, including Microsoft Office documents and Adobe PDFs. You can configure the document and the content types to Disarm. You can Disarm macros, JavaScript, Flash, and other exploitable content.</td>
</tr>
</tbody>
</table>
| Adware and spyware | Symantec Messaging Gateway detects the security risks that do any of the following:  
- Provide unauthorized access to computer systems  
- Identity theft or fraud by logging keystrokes  
- Capture email traffic  
- Harvest personal information, such as passwords and logon identifications  
- Present some type of disruption or nuisance  
See “Spyware or adware verdict details” on page 214. |

- Symantec Messaging Gateway must be able to decompose and scan a container file to detect viruses. You can specify the maximum size and scanning depth levels of container files to reduce your exposure to zip bombs or denial-of-service attacks. See “Setting limits on nested files” on page 228.
- When Symantec Messaging Gateway scans a message and detects a malware policy violation, it takes the verdict that you specify in that policy. See “Creating email malware policies” on page 217. See “Selecting malware policies for a policy group” on page 196.
- You must have a valid antivirus license to perform antivirus scanning functions and to obtain updated virus definitions. See “Licensing your product” on page 714.

For additional protection, you can integrate Symantec Messaging Gateway with Symantec Content Analysis to scan files and attachments for advanced threats.
Product technologies that detect viruses and malicious attacks

Table 9-1 describes the technologies that Symantec Messaging Gateway uses to detect viruses, malicious attacks, and potentially malicious content.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus engine</td>
<td>The antivirus engine provides rapid and reliable virus protection through a multi-threaded scanning system. It scans incoming and outgoing email traffic. It identifies and cleans the messages that contain viruses and related malicious executables. It also attempts to repair viruses within email attachments. The antivirus engine itself cannot be modified.</td>
</tr>
<tr>
<td>Artificial intelligence technology</td>
<td>The product uses static and dynamic artificial intelligence technology to detect virus-like behavior to identify unknown viruses. You can adjust artificial intelligence sensitivity settings for more or less aggressive identification of viruses. See &quot;Modifying the artificial intelligence sensitivity level&quot; on page 235.</td>
</tr>
<tr>
<td>Virus definitions</td>
<td>Virus definitions are available every hour to protect against the latest, fast-spreading threats. Symantec LiveUpdate is the process by which the appliance receives current virus definitions. By default, the appliance downloads certified virus definitions. You can configure how and when you want to obtain updated definitions. See &quot;About updating virus definitions&quot; on page 231.</td>
</tr>
<tr>
<td>Antivirus policies</td>
<td>You can create policies to detect viruses or malicious attacks. When you create a policy, you specify the action that you want Symantec Messaging Gateway to take if the policy is violated. For example, you can clean infected attachments, but delete spyware attachments entirely. You can create as many antivirus policies as needed. See “Creating email malware policies” on page 217.</td>
</tr>
</tbody>
</table>
Table 9-1  Technologies that detect viruses and malicious attacks (continued)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day-zero detection</td>
<td>This feature leverages the Symantec view of email threats as well as heuristic analysis to identify a suspicious attachment before antivirus definitions are available. Messages that contain suspicious attachments can be moved to the Suspect Virus Quarantine. Symantec Messaging Gateway holds the message in the quarantine for the period of time that you specify (up to 24 hours). It then releases the message to be scanned again with updated virus definitions. You can create the virus policies that contain verdicts to quarantine suspect message attachments. You can also configure how long an attachment remains in the Suspect Virus Quarantine. See “About quarantining suspected viruses” on page 237.</td>
</tr>
<tr>
<td>Disarm</td>
<td>Disarm scans email attachments for Microsoft Office and PDF documents that may contain potentially malicious content (PMC). This content includes macros, Flash movies, and other exploitable content. Disarm deconstructs attachments that contain potentially malicious content (PMC), removes the PMC, then reconstructs and delivers the cleaned attachments. You can choose the document types and PMC types on which to attempt removal or reconstruction. You can also archive the original unaltered documents for later retrieval. See “About Disarm” on page 207.</td>
</tr>
<tr>
<td>Threat defense</td>
<td>Threat defense integrates Symantec Messaging Gateway with Symantec Content Analysis to detect advanced threats. Symantec Messaging Gateway then applies threat defense policies to the email messages. See “About threat defense scanning” on page 455. When you enable Disarm for content types on the Malware &gt; Settings &gt; Email Scan Settings &gt; Disarm tab, threat defense policies can also Disarm attachments.</td>
</tr>
</tbody>
</table>

About Disarm

Disarm technology in Symantec Messaging Gateway locates and removes potentially malicious content (PMC) from email attachments. You can scan both inbound messages and outbound messages to detect Microsoft Office and Adobe PDF attachments that may contain PMC. PMC types include macros, scripts, Flash content, and other exploitable content.

Note: Disarm does not determine whether the content that it detects and removes is malicious. Rather, it detects the presence of specified content types within specified document types that have the potential to be exploited and removes them.
When Disarm is enabled, it detects the presence of the PMC in the attached document, deconstructs the attachment, removes the PMC, and reconstructs the document. You can choose the document and PMC types for which to attempt removal. You can also choose to archive the original documents for retrieval later.

Disarm is implemented as an extension of Symantec Messaging Gateway’s day-zero detection feature. It extends the functionality of the Symantec Decomposer to:

- Recursively extract embedded objects from container document types.
- Filter out potentially harmful content (macros, scripts, executables, unrecognized content, unreferenced objects).
- Replace potentially harmful objects with benign or reconstructed versions.
- Reconstruct the container documents and reattach them to the email message.

Disarm does not support the scanning of encrypted or password-protected attachments, nor attachments that are compressed using unsupported formats (such as RAR). If a supported container document is nested within other supported documents, Disarm deconstructs documents until it processes the last nested document or reaches the container limit. Disarm then removes the PMC from the supported type, and reconstructs and reattaches the documents.

See “Setting limits on nested files” on page 228.

---

**Note:** PMC removal and reconstruction of documents may affect both visual fidelity and function. Text formatting or images may look different in the reconstructed document. Functionality may be lost if the original documents contain elements such as text input fields that are implemented with macros. Content may be lost as well if you choose to remove embedded files and attachments from a message. Disarm may also have an effect on Symantec Messaging Gateway’s overall throughput speed, especially if you choose to scan all supported attachment and PMC types.

To activate Disarm, you enable settings to specify the types of content to Disarm. You then create a malware or threat defense policy that uses Disarm and apply the policy to a policy group. You can also choose a content filtering action that lets you bypass Disarm.

See “Using Disarm to remove potentially malicious content” on page 208.

---

**Using Disarm to remove potentially malicious content**

Unlike most other email malware policies, the **Disarm: Disarm attachment** policy action is not activated by default, though it is enabled. To activate it, you:

- Configure email scan settings to specify the container document and PMC types to detect.
Configure an email malware policy that detects the specified PMC types within the container documents, and includes the action to Disarm the PMC.

Apply this policy to one or more policy groups.

You can also annotate messages from which PMC was removed, mark up the Subject line, and archive the original messages for later retrieval. Any actions that can be added to other malware policies can also be added to the Disarm: Disarm attachment policy.

**Note:** You can also configure threat defense policies to use Disarm. See “Creating new threat defense policy sets” on page 465.

Table 9-2 describes the tasks that you perform to detect and remove potentially malicious content. You can perform the tasks in any order.

**Table 9-2**  
Disarming potentially malicious content

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure email scan settings to specify the document and PMC types to remove.</td>
<td>On the Malware page, select Email scan settings and then the Disarm tab. Specify which document types to detect, and within each document type, specify which potentially malicious content types to Disarm. You can also enable Preprocess non-conforming PDFs if you find that PDF attachments are negatively affected by Disarm. See “Potentially malicious content details” on page 210. for details about document and PMC types.</td>
</tr>
<tr>
<td>Select default or create new Disarm policies.</td>
<td>Symantec Messaging Gateway comes with a preconfigured default Disarm policy that is enabled but not applied to any group of users. You can use this default policy as-is or modify it to create your own custom policy. You can also choose to add PMC-detection functionality to other existing policies. To use the default PMC policy: On the Email Malware Policies page, select the policy Disarm: Disarm attachment. In the Actions area, select Disarm attachment(s) and click Save. See “Default email malware policies” on page 218. See “Creating email malware policies” on page 217.</td>
</tr>
</tbody>
</table>
### Table 9-2 Disarming potentially malicious content (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the Disarm policy to a policy group.</td>
<td>You can apply the Disarm policy to policy groups in one of two ways:</td>
</tr>
<tr>
<td>■ On the Email Malware Policies page,</td>
<td>select the policy <strong>Disarm: Disarm attachment</strong>. In the Apply to the following policy groups area, select the desired policy groups and click <strong>Save</strong>.</td>
</tr>
<tr>
<td>■ On the Administration tab, under Users,</td>
<td>select <strong>Policy Groups</strong>. Select a policy group from the list, and click the <strong>Malware</strong> tab. Enable the <strong>Disarm: Disarm attachment</strong> policy for malware scanning, and click <strong>Save</strong>. Note that Disarm applies to inbound scanning by default, but you can choose to Disarm outbound attachments as well.</td>
</tr>
<tr>
<td>Specify other actions for Disarm policies.</td>
<td>Any actions that can be added to other malware policies can also be added to the Disarm policy. For example, you can annotate messages from which PMC was removed, quarantine messages with PMC, and archive the original messages for later retrieval.</td>
</tr>
<tr>
<td>Monitor reports.</td>
<td>Examine reports to track PMC detection and policies. Reports also indicate the volume of potential threats that your organization receives. This information can help you fine-tune your threat detection settings.</td>
</tr>
</tbody>
</table>

### Potentially malicious content details

Symantec Messaging Gateway can detect potentially malicious content in several common email attachment types (Word, Excel, PowerPoint, PDF). Table 9-3 lists and describes each type of PMC, and explains the consequences of removing it from a container document.
Malware that is embedded in or attached to another file or document is more complex to detect than malware that is contained directly in an email message. Disarm lets you recursively reconstruct or remove embedded files and attachments not just from the message itself, but also from the message’s attached documents. Each attached or embedded document is opened scanned for attached or embedded objects, up to the limit specified in the SMTP Protocol Settings page’s Container Limits area. An attached or embedded file is reconstructed if its file type is supported. If not, it is removed. Some file types that are not commonly malicious (such as image files) are ignored rather than reconstructed or removed.

**Consequences of removal:**

Removing embedded or attached files can result in content loss. You can archive messages from which embedded files and attachments are removed so that you can recover the content later.

Attached documents sometimes contain icons used to open other documents embedded in them. If the embedded document types are disabled in the Disarm scan settings, then Disarm retains the icons and replaces the disabled document type’s content with text that explains that the content has been intentionally removed. This text is displayed when the icons are clicked.

If you find that PDF attachments become unreadable, enable Preprocess non-conforming PDFs on the Malware > Scan Settings > Disarm tab. This feature identifies and attempts to repair the structure of PDF documents that do not conform to the published PDF standard. This preprocessing helps Disarm to reconstruct these PDFs properly after they are scanned.

**Flash**

Supported file types: Office 2003, Office 2007 and later, and PDF

Flash content (especially if the Flash Player is unpatched) is a common vehicle for malware, both on webpages and in documents.

**Consequences of removal:**

Flash content is removed from attachments and replaced by white rectangles with black borders.

**Macros**

Supported file types: Office 2003 and Office 2007 and later

Macros are used to provide added functionality in documents. They often execute when a document is opened, and are commonly exploited as a vehicle for malware.

**Consequences of removal:**

Loss of macro-based functionality, including custom add-ins, dialog boxes, and data extraction processes.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Embedded files and attachments</strong></td>
<td>Malware that is embedded in or attached to another file or document is more complex to detect than malware that is contained directly in an email message. Disarm lets you recursively reconstruct or remove embedded files and attachments not just from the message itself, but also from the message's attached documents. Each attached or embedded document is opened scanned for attached or embedded objects, up to the limit specified in the SMTP Protocol Settings page's Container Limits area. An attached or embedded file is reconstructed if its file type is supported. If not, it is removed. Some file types that are not commonly malicious (such as image files) are ignored rather than reconstructed or removed. <strong>Consequences of removal:</strong> Removing embedded or attached files can result in content loss. You can archive messages from which embedded files and attachments are removed so that you can recover the content later. Attached documents sometimes contain icons used to open other documents embedded in them. If the embedded document types are disabled in the Disarm scan settings, then Disarm retains the icons and replaces the disabled document type's content with text that explains that the content has been intentionally removed. This text is displayed when the icons are clicked. If you find that PDF attachments become unreadable, enable Preprocess non-conforming PDFs on the Malware &gt; Scan Settings &gt; Disarm tab. This feature identifies and attempts to repair the structure of PDF documents that do not conform to the published PDF standard. This preprocessing helps Disarm to reconstruct these PDFs properly after they are scanned.</td>
</tr>
<tr>
<td><strong>Flash</strong></td>
<td>Flash content (especially if the Flash Player is unpatched) is a common vehicle for malware, both on webpages and in documents. <strong>Consequences of removal:</strong> Flash content is removed from attachments and replaced by white rectangles with black borders.</td>
</tr>
<tr>
<td><strong>Macros</strong></td>
<td>Macros are used to provide added functionality in documents. They often execute when a document is opened, and are commonly exploited as a vehicle for malware. <strong>Consequences of removal:</strong> Loss of macro-based functionality, including custom add-ins, dialog boxes, and data extraction processes.</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3D components</td>
<td>The PDF format supports the inclusion of 3D content using the Universal 3D file format. When you select this option, Disarm strips all 3D components.</td>
</tr>
<tr>
<td>Consequences of removal:</td>
<td>Loss of 3D preview-like functionality.</td>
</tr>
<tr>
<td>Fonts</td>
<td>Fonts that are embedded in PDF files can be used as a vehicle for malware. Disarm strips embedded fonts when this option is selected.</td>
</tr>
<tr>
<td>Consequences of removal:</td>
<td>Visual fidelity can be altered if no substitute font is available on the endpoint. Administrators may choose to distribute known safe replacement fonts to endpoints in their organizations to reduce visual fidelity issues in Disarmed attachments.</td>
</tr>
<tr>
<td>Trailer information</td>
<td>PDF files are comprised of a header, a body, a cross-reference table, and a trailer. The trailer contains information about the root object and the cross-reference table. Trailers can be used maliciously if other objects are added to them.</td>
</tr>
<tr>
<td>Consequences of removal:</td>
<td>None. There is no loss of functionality or fidelity.</td>
</tr>
<tr>
<td>JavaScript</td>
<td>JavaScript in PDFs is most often used to change the document's content in response to some event. For example, JavaScript can be used to hide part of the document before it is printed. It can also be used to pre-fill form fields when the document is opened. JavaScript is also used to restrict the actions of the Acrobat Reader (for example, to validate data that is entered in a PDF form's fields). It can also be used to introduce malicious code in documents.</td>
</tr>
<tr>
<td>Consequences of removal:</td>
<td>Loss of functionality that is provided by the JavaScript.</td>
</tr>
<tr>
<td>Launch</td>
<td>The Launch function is a PDF feature (enabled by default) that lets you launch executables from inside a PDF. Malware creators have exploited this feature for some time. The Launch function is disabled when you select this option.</td>
</tr>
<tr>
<td>Consequences of removal:</td>
<td>The PDF can no longer launch other processes or applications. Add-ins, templates, and tools that rely on launching other documents or processes will no longer work as expected.</td>
</tr>
</tbody>
</table>
Table 9-3 Potentially malicious content container and content type details (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| XFA (and its Javascript) | XFA (XML Forms Architecture) is a group of proprietary XML specifications that are used to enhance the processing of web forms. When you select this option, Disarm removes both the XFA and the JavaScript associated with it.  
**Consequences of removal:**  
Loss of functionality that is provided by XFA. A form’s visual layout is usually unaffected, but its interactive functionality may be lost. |
| Fullscreen | A PDF document's Fullscreen mode can be used maliciously to simulate a GUI or an Internet website to trick users into entering sensitive information. To prevent these exploits, Disarm blocks a PDF attachment's use of Fullscreen functionality.  
**Consequences of removal:**  
Loss of full-screen functionality for legitimate as well as potentially malicious purposes. |

About retrieving Disarmed content

Removal of potentially malicious content (PMC) from email attachments with Disarm may affect both visual fidelity and function in the reconstructed documents. For example, the appearance of a document may change if embedded fonts are removed and replaced with system fonts. Functionality may be lost if the original documents contain elements (such as text input forms) implemented with macros. The input fields may still exist in the reconstructed documents, but may no longer provide input validation or visual feedback after the attachment is Disarmed. Similarly, mouse actions or keyboard input that is controlled by JavaScript may no longer work if JavaScript is removed.

PMC removal can also cause more global losses of functionality in a document, or even loss of content. For example, if you Disarm all macros in Microsoft Office documents, then an Excel spreadsheet that uses macros may no longer work as intended. Similarly, if you choose to reconstruct embedded files and attachments from an email message, then attached or embedded content that Disarm does not support is discarded.

The only way to retain the original content with all of its functionality is to archive all messages with attachments. To archive messages, you first specify the location in which to store the archive. Then you specify "Archive the message" as an action for your Disarm policy or policies. On the **Edit Email Malware Policy** page, in the **Actions** area, click **Add** and select "Archive the message" from the **Configure an action** drop-down list.
What you can do with suspicious attachments

When you create a policy and choose the condition, “If a message contains a suspicious attachment,” additional options become available as follows:

- **Hold message in Suspect Virus Quarantine** Select this option to quarantine the message and all attachments.
- **Strip and Delay in Suspect Virus Quarantine** Select this option to delete the suspicious attachment and quarantine the message. When you select this option, the suspicious attachment cannot be retrieved.

Both of these actions move the message to quarantine. After the amount of time that you specify, the messages are rescanned. This time, however, the messages are scanned with the newest definitions that are available.

See “About quarantining suspected viruses” on page 237.
See “Creating email malware policies” on page 217.

Spyware or adware verdict details

Symantec Messaging Gateway can detect security risks. Security risks are the programs that do any of the following:

- Provide unauthorized access to computer systems
- Compromise data integrity, privacy, confidentiality, or security
- Present some type of disruption or nuisance

Symantec Messaging Gateway applies the spyware or adware verdict to all of the security risks that it detects.

See “About detecting viruses, malware, and malicious attacks” on page 204.

**Table 9-4** lists the categories of security risks that Symantec Messaging Gateway detects.

<table>
<thead>
<tr>
<th>Table 9-4</th>
<th>Security risk categories included in spyware or adware verdict</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Adware</td>
<td>Standalone or the appended programs that gather personal information through the Internet and relay it back to a remote computer without the user's knowledge. Adware might monitor browsing habits for advertising purposes. It can also deliver advertising content.</td>
</tr>
</tbody>
</table>
Table 9-4 Security risk categories included in spyware or adware verdict (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking tools</td>
<td>Programs that are used to gain unauthorized access to a user's computer. For example, a keystroke logger tracks and records individual keystrokes and sends this information to a remote computer. The remote user can perform port scans or vulnerability scans. Hacking tools can also be used to create viruses.</td>
</tr>
<tr>
<td>Dialers</td>
<td>Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. These programs typically to accrue charges.</td>
</tr>
<tr>
<td>Joke programs</td>
<td>Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or bothersome. For example, a joke program might move the Recycling Bin away from the mouse when the user tries to click on it.</td>
</tr>
<tr>
<td>Remote access programs</td>
<td>Programs that let a remote user gain access to a computer over the Internet to gain information, attack, or alter the host computer.</td>
</tr>
<tr>
<td>Spyware</td>
<td>The Standalone programs that can secretly monitor system activity. These programs can and detect passwords and other confidential information and then relay the information back to a remote computer.</td>
</tr>
</tbody>
</table>

Detecting viruses, malware, and malicious threats

Table 9-5 describes the tasks that you can perform to detect viruses and malicious threats. You can perform any or all of the tasks in any order.

Table 9-5 Detecting viruses, malware, and malicious threats

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email virus attack recognition</td>
<td>In an email virus attack, a specified quantity of infected email messages has been received from a particular IP address. By default, any connections that are received from violating senders are deferred. Email virus attack recognition is disabled by default and must be enabled to be activated. See &quot;Configuring email virus attack recognition&quot; on page 147.</td>
</tr>
</tbody>
</table>
Table 9-5  Detecting viruses, malware, and malicious threats *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create and enable email malware policies. | Symantec Messaging Gateway comes with the pre-configured malware policies that are automatically enabled. You can modify these policies and create your own custom policies.  
See “Default email malware policies” on page 218.  
See “Creating email malware policies” on page 217. |
| Set the artificial intelligence sensitivity level. | Symantec Messaging Gateway contains static and dynamic artificial intelligence technology. This technology scans for unusual behaviors (such as self-replication) to target potentially infected message bodies and attachments.  
The default setting is Medium. However, you can modify this setting or turn detection off. Artificial intelligence scanning involve a trade-off between malware-detection rates and false positives. Lower artificial intelligence sensitivity levels may miss more malware but produce fewer false positives. Higher artificial intelligence sensitivity levels may catch more malware but cause more false-positive detections.  
See “Modifying the artificial intelligence sensitivity level” on page 235. |
| Specify the file types that can bypass antivirus scanning. | You can specify the file types that can bypass antivirus scanning. For example, certain file types typically do not contain viruses, such as .mpg files. File types that you feel confident do not contain viruses can bypass virus scanning, which saves system resources.  
Symantec Messaging Gateway provides a default list of file type categories. But you must create Exclude Scanning Lists, select the categories that you want to include, and enable the list. You can also add and remove file types from Exclude Scanning Lists.  
See “Excluding file types from virus scanning” on page 225. |
| Configure the Suspect Virus Quarantine. | You can create virus policies to quarantine suspicious message attachments in the Suspect Virus Quarantine.  
Symantec provides default values for the following Suspect Virus Quarantine settings; however, you can change these settings as needed:  
- Maximum amount of the time that messages are held in the quarantine  
The default setting is 6 hours.  
- Disk space available for the quarantine  
The default setting is 10 GB.  
See “About quarantining suspected viruses” on page 237. |
Table 9-5 Detecting viruses, malware, and malicious threats (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable definition updates.</td>
<td>By default, LiveUpdate is enabled. Platinum definition updates are scheduled to occur every 10 minutes from Monday through Friday. However, you modify when and how you want to obtain updates. See “About updating virus definitions” on page 231.</td>
</tr>
</tbody>
</table>
| Configure outbreak notification alerts.   | Set up alert notifications to let you know any of the following virus-related events occur:  
  ■ An outbreak is detected
  ■ Malware filters are older than the time period that you specify
  ■ New malware filters are available
  ■ The antivirus license has expired
  See “Configuring alerts” on page 688.                                                                                                                                                                                                                                         |
| Monitor reports.                          | Monitor reports to determine how effective virus detection and policies are. Reports also indicate the volume of threats that your organization receives. This information can help you fine-tune your antivirus detection and threat detection settings.                                                                                     |

Creating email malware policies

Symantec Messaging Gateway installs with several preconfigured malware policies that are enabled by default. In addition to these policies, you can create your own custom policies. Content filtering, spam, and malware policy names must be unique. For example, if you have a content filtering policy called XYZ, you cannot have a spam policy or malware policy called XYZ. Email malware policies are enabled by default when you create them.

See “Default email malware policies” on page 218.

To create email malware policies

1. In the Control Center, click **Malware > Policies > Email**.
2. Click **Add**.
3. In the **Policy name** box, type a name for the malware policy.
4. Under **Conditions**, click the **Apply to** drop-down list and choose to which type of message the malware policy should apply:
   - Inbound messages
   - Outbound messages
   - Inbound and Outbound messages
This option specifies where this malware policy is available on the Malware tab when you configure a policy group.
For example, assume that you choose Inbound messages and the If the message contains a mass-mailing worm condition. This malware policy is only available in the Inbound mass-mailing worm policy list when you configure a policy group.

5 Click the If the following condition is met drop-down list to select a condition.
6 Under Actions, click Add.
   On the Configure An Action page, click the drop-down list and select an action.
   For some actions you need to specify additional information in the fields beneath the action.
   For example, assume that you select the action to Forward a copy of the message. A box appears in which you can type the email address of the person to whom you want to forward the message.
   See “Policy actions and what they do” on page 333.
   See “Selecting malware policies for a policy group” on page 196.
7 Click Add Action.
   You can add as many actions as needed, but actions cannot conflict with each other.
8 Under Policy Groups, check one or more groups to which this policy should apply.
9 Click Save.

Default email malware policies

Symantec Messaging Gateway installs with pre-configured malware policies. These policies are enabled by default and can be applied to a policy group. You can disable or modify the policy actions and the policy groups to which the policies apply. The policy name, the type of message that the policy applies to, and the condition that must be met cannot be modified for the pre-configured virus policies that are labeled as default.

See “Creating email malware policies” on page 217.
See “Selecting malware policies for a policy group” on page 196.
Table 9-6  Default email malware policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Applies to the following messages</th>
<th>If the following condition is met</th>
<th>Actions</th>
<th>Applies to the following policy group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus: Clean message (default)</td>
<td>Inbound and outbound messages</td>
<td>Message contains a virus</td>
<td>Clean the message</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Worm: Delete message (default)</td>
<td>Inbound and outbound messages</td>
<td>Message contains a mass-mailing worm</td>
<td>Delete the message</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Unscannable for Disarm: Deliver normally</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for potentially malicious content</td>
<td>Deliver the message normally</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Unscannable for malware and content filtering for any reason: Delete message (default)</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for malware and content filtering</td>
<td>Delete the message</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Encrypted Attachment: Modify subject line with &quot;[WARNING - ENCRYPTED ATTACHMENT NOT VIRUS SCANNED]&quot;</td>
<td>Inbound and outbound messages</td>
<td>Message contains an encrypted attachment</td>
<td>Prepend the subject line with &quot;[WARNING - ENCRYPTED ATTACHMENT NOT VIRUS SCANNED]&quot;</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Virus: Delete message</td>
<td>Inbound and outbound messages</td>
<td>Message contains a virus</td>
<td>Delete the message</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Virus: Modify subject line with &quot;[VIRUS INFECTED]&quot;</td>
<td>Inbound and outbound messages</td>
<td>Message contains a virus</td>
<td>Prepend the subject line with &quot;[VIRUS INFECTED]&quot;</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Virus: Deliver normally</td>
<td>Inbound and outbound messages</td>
<td>Message contains a virus</td>
<td>Deliver the message normally</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Policy name</td>
<td>Applies to the following messages</td>
<td>If the following condition is met</td>
<td>Actions</td>
<td>Applies to the following policy group</td>
<td>Default status</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>----------------------</td>
<td>--------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Worm: Clean message</td>
<td>Inbound and outbound messages</td>
<td>Message contains a mass-mailing worm</td>
<td>Clean the message</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Worm: Modify subject line with &quot;[WORM INFECTED]&quot;</td>
<td>Inbound and outbound messages</td>
<td>Message contains a mass-mailing worm</td>
<td>Prepend the subject line with &quot;[WORM INFECTED]&quot;</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Worm: Deliver normally</td>
<td>Inbound and outbound messages</td>
<td>Message contains a mass-mailing worm</td>
<td>Deliver the message normally</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Unscannable for malware and content filtering for any reason: Modify subject line with &quot;[WARNING -NOT VIRUS SCANNED]&quot;</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for malware and content filtering</td>
<td>Prepend the subject line with &quot;[WARNING -NOT VIRUS SCANNED]&quot;</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Unscannable for malware and content filtering for any reason: Deliver normally</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for malware and content filtering</td>
<td>Deliver the message normally</td>
<td>None</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Policy name</td>
<td>Applies to the following messages</td>
<td>If the following condition is met</td>
<td>Actions</td>
<td>Applies to the following policy group</td>
<td>Default status</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disarm: Disarm attachment</td>
<td>Inbound only by default, but you can choose to apply it to outbound messages as well.</td>
<td>Message contains an attachment with potentially malicious content AND you select container documents and Disarm content types to remove on the Malware &gt; Scan Settings &gt; Email Scan Settings &gt; Disarm tab</td>
<td>Deconstruct the attachment, remove the potentially malicious content, reconstruct the attachment, and deliver normally</td>
<td>None</td>
<td>Enabled by default, but not applied until document and Disarm content types are selected on the Disarm tab and the policy is applied to a group.</td>
</tr>
<tr>
<td>Threat: Modify subject line with &quot;[SPYWARE OR ADWARE INFECTED]&quot; (default)</td>
<td>Inbound and outbound messages</td>
<td>Message contains spyware or adware See “Spyware or adware verdict details” on page 214.</td>
<td>Prepend the subject line with &quot;[SPYWARE OR ADWARE INFECTED]&quot;</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Inbound suspect virus: Strip attachments and hold message in Suspect Virus Quarantine (default)</td>
<td>Inbound messages</td>
<td>Message contains a suspicious attachment</td>
<td>Strip and Delay in Suspect Virus Quarantine with message &quot;Parts of your message have been stripped because they were considered suspect.&quot;</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Outbound suspect virus: Hold message in Suspect Virus Quarantine (default)</td>
<td>Outbound messages</td>
<td>Message contains a suspicious attachment</td>
<td>Hold message in Suspect Virus Quarantine</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
</tbody>
</table>
Managing email malware policies

Table 9-7 describes the ways in which you can manage email malware policies. You can perform these tasks in any order as needed.

### Table 9-7 Manage email malware policies

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify an email malware policy.</td>
<td>You can modify an email malware policy as needed. You can modify default email malware policies or your own custom policies. See “Modifying email malware policies” on page 222.</td>
</tr>
<tr>
<td>Enable or disable an email malware policy.</td>
<td>You must enable a policy for Symantec Messaging Gateway to evaluate it against email. When you create a new policy, it is automatically enabled by default. And Symantec Messaging Gateway preinstalled policies are also automatically enabled by default. See “Enabling or disabling email malware policies” on page 223.</td>
</tr>
<tr>
<td>Delete an email malware policy.</td>
<td>When you no longer need a malware policy, you can delete it. When you delete it, it is permanently removed and cannot be restored. If you are uncertain as to whether you want to permanently delete a policy, consider disabling instead. See “Deleting email malware policies” on page 224.</td>
</tr>
<tr>
<td>Copy an email malware policy.</td>
<td>You may want to create a new policy that is similar an existing policy. Instead of creating the policy from scratch, you can copy it and then modify the newly created policy as needed. See “Copying email malware policies” on page 224.</td>
</tr>
</tbody>
</table>

Modifying email malware policies

You can modify default and custom email malware policies to fine-tune them or to expand or reduce their scope.

Table 9-8 describes the setting that you can modify for default email malware policies and custom email malware policies.

### Table 9-8 Modifiable email malware policy settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Modifiable in default policies</th>
<th>Modifiable in custom policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply to</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 9-8  Modifiable email malware policy settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Modifiable in default policies</th>
<th>Modifiable in custom policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the following condition is met</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Perform the following action</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply to the following groups</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To modify email malware policies

1. In the Control Center, click **Malware > Policies > Email**.
2. Check the box beside the policy that you want to modify, and then click **Edit**.
3. Make the modifications that you want.
4. Click **Save**.

Enabling or disabling email malware policies

Default email malware policies are enabled by default. When you create a new email malware policy, it is enabled by default. You can disable any policy that you do not want Symantec Messaging Gateway to use when it scans email messages.

You can disable a malware policy to troubleshoot email malware scanning issues. You can also create custom email malware policies when an outbreak occurs and then disable the policies when the outbreak ends. You can turn on the policy in the event of another outbreak. You can also disable the policies that you no longer want to use but do not want to delete yet.

To enable or disable email malware policies

1. In the Control Center, click **Malware > Policies > Email**.
2. Check the box beside the policy that you want to enable or disable.
3. Click one of the following options:

   - **Enable**
   - **Disable**

   When you enable a policy, a green check mark appears in the **Enabled** column.
   When you disable a policy, a horizontal line appears in the **Enabled** column.

See "Deleting email malware policies" on page 224.
Deleting email malware policies

You can delete the email malware policies that you no longer need. However, when you delete a policy, the policy cannot be retrieved. If you are unsure if you want to permanently delete a policy, you can disable it instead.

See "Enabling or disabling email malware policies" on page 223.

To delete email malware policies

1. In the Control Center, click **Malware > Policies > Email.**
2. Check the box beside the policy that you want to delete.
3. Click **Delete.**
4. Click **OK** in the confirmation dialog box.

Copying email malware policies

You may have instances in which you create a complicated email malware policy and want to create a similar policy with only a few variances. Symantec Messaging Gateway lets you copy email malware policies.

When you copy an email malware policy, the new policy must have a unique name. For example, if you have a content filtering policy called XYZ, you cannot have a spam policy or malware policy called XYZ. Email malware policies are enabled by default when you create them.

To copy email malware policies

1. In the Control Center, click **Malware > Policies > Email.**
2. Check the box beside the policy that you want to copy.
3. Click **Copy.**
4. On the **Add Email Malware Policies** page, type a new name for the policy.
5. Make any other changes you want.
6. Click **Save.**

Using lists to improve virus scanning performance

You can create lists of file types to exclude from virus scans. Default lists that come installed with the product can be modified to create custom lists.

Table 9-9 describes what you can do with these lists. You can perform these tasks as needed in any order.
Managing lists for virus scanning

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the lists that contain the file types that can bypass antivirus scanning. Multiple lists can help you categorize the file types.</td>
<td>Viruses and malicious threats are typically contained in executable file types. You can improve scanning performance by letting the file types that do not contain executables bypass scanning. See “Excluding file types from virus scanning” on page 225.</td>
</tr>
<tr>
<td>Modify the file types that you want to exclude from scanning as you fine-tune your malware scanning policies.</td>
<td>For example, you may find that some malicious executables can be modified to look like harmless file types. So you want to remove the file types that can be spoofed from the list of files to be excluded from scanning. See “Modifying the file types to exclude from scanning” on page 226.</td>
</tr>
<tr>
<td>Enable and disable lists as needed.</td>
<td>You can have multiple lists of file types to exclude from scanning. However, the file types that are included in the list do not bypass antivirus scanning unless the list is enabled. A list is enabled by default when you create it. Disable any list that you do not want Symantec Messaging Gateway to use when it scans email messages. You can disable a list to troubleshoot email virus scanning issues. You can also create custom a list to use for an outbreak and disable the list when the outbreak ends. You can enable the list again in the event of another outbreak. You can also disable the lists that you no longer want to use but do not want to delete. See “Enabling or disabling the lists of file types to exclude from scanning” on page 227.</td>
</tr>
<tr>
<td>Delete a list of file types to exclude from scanning that you no longer need.</td>
<td>When you delete a list, the contents of the list cannot be retrieved. See “Deleting lists of the file types to exclude from scanning” on page 228.</td>
</tr>
<tr>
<td>Export lists of the file types to exclude from scanning to a text file.</td>
<td>You may want to export file types for any of the following reasons: ■ To have a list that you can distribute throughout your organization to those who need to know the file types that bypass scanning. ■ To have an archive copy of a file type list before you copy the list, modify the list, or delete the list. See “Exporting lists of the file types to exclude from scanning” on page 228.</td>
</tr>
</tbody>
</table>

Excluding file types from virus scanning

Symantec Messaging Gateway lets you create lists of the file types that you want to exclude from virus scanning. You can create a single list or you can create multiple lists to help you categorize the file types.
To help you create your lists, Symantec Messaging Gateway provides file classes that group similar file types. You can choose every file type in a file class, or you can select individual file types to exclude from virus scanning. You can also select All File Classes to create a list of every file class that SMG provides.

To exclude file types from threat defense scanning

1. In the Control Center, click Malware > Settings > Email Scan Settings.
2. On the Exclude Scanning tab, click Add.
3. In the Exclude scanning list name box, type a name for the list.
4. In the File classes list, select the file class that you want to exclude from scanning.
   - To select multiple classes, hold down the Ctrl key while you click the names of file classes.
   - To select every file class in the File classes list, click All File Classes.
5. The File Types list displays all the file types that are associated with your selected file classes.
   - To exclude every file type in the File Types list from virus scanning, click Add File Classes.
   - To remove file types from the exclusion list, hold down the Ctrl key while you deselect the file types. Then click Add File Classes to add the remaining, selected file types.
6. Click Save.
   The names of the file types appear in the Description list.

When you create a new list, it is enabled by default. An exclude scanning list must be enabled if you want SMG to use the list during scans. When a message contains an attachment that matches an excluded file type, SMG does not perform virus scanning on the file. You can edit, delete, disable, enable, or export an exclude scanning list on the Malware > Settings > Email Scan Settings > Exclude Scanning tab.

Modifying the file types to exclude from scanning

You can modify the file types that you want to exclude from scanning as you fine-tune your scanning policies. For example, you may find that some malicious executables can be modified to look like harmless file types. So you want to remove the file types that can be spoofed from the list of files to be excluded from scanning.

See “Excluding file types from virus scanning” on page 225.

To modify the file types to exclude from scanning

1. In the Control Center, click Malware > Settings > Email Scan Settings.
2. Click the Exclude Scanning tab.
As the user checks the box beside the Exclude Scanning List that they want to modify,

1. Click **Edit**.

2. Do any of the following tasks:

   - To add a file type to the list: Under **File classes**, select the file class that you want to exclude from scanning.
     - To select multiple classes, hold down the **Ctrl** key while you click the names of file classes.
     - Click the file classes from which you want to exclude specific file types. Then select the file types from the **File Types** list.
     - Hold down **Ctrl** to select multiple file types.
     - Click **Add File Types**.

   - To remove a file type from the list: Under **Description**, check the box beside the file type that you want to delete, and then click **Delete**.

3. Click **Save**.

See “Enabling or disabling the lists of file types to exclude from scanning” on page 227.

### Enabling or disabling the lists of file types to exclude from scanning

You can have multiple lists of file types to exclude from scanning. However, the file types that are included in the list do not bypass antivirus scanning unless the list is enabled. A list is enabled by default when you create it. Disable any list that you do not want Symantec Messaging Gateway to use when it scans email messages.

You can disable a list to troubleshoot email virus scanning issues. You can also create custom a list to use for an outbreak and disable the list when the outbreak ends. You can enable the list again in the event of another outbreak.

You can also disable the lists that you no longer want to use but do not want to delete yet.

#### To enable or disable the lists of file types to exclude from scanning

1. In the Control Center, click **Malware > Settings > Email Scan Settings**.
2. Click the **Exclude Scanning** tab.
3. Check the box beside the policy that you want to enable or disable.
4. Select one of the following options:

   - **Enable**: When you enable a policy, a green check mark appears in the **Enabled** column.
   - **Disable**: When you disable a policy, a horizontal line appears in the **Enabled** column.
Deleting lists of the file types to exclude from scanning

You can delete a list of file types to exclude from scanning that you no longer need. However, when you delete a list, the contents of the list cannot be retrieved. If you are unsure if you want to permanently delete a list, you can disable it instead. Before you delete the list, you may want to export it and maintain the list for your records.

See “Enabling or disabling the lists of file types to exclude from scanning” on page 227.

To delete lists of file types to exclude from scanning

1. In the Control Center, click Malware > Settings > Email Scan Settings.
2. Click the Exclude Scanning tab.
3. Check the box beside the list that you want to delete.
4. Click Delete.
5. Click Delete in the confirmation dialog box.

Exporting lists of the file types to exclude from scanning

You can export lists of the file types to exclude from scanning to a text file.

You may want to export file types for any of the following reasons:

- To have a list that you can distribute throughout your organization to those who need to know the file types that bypass scanning.
- To have an archive copy of a file type list before you copy the list, modify the list, or delete the list.

To export lists of file types to exclude from scanning

1. In the Control Center, click Malware > Settings > Email Scan Settings.
2. Click the Exclude Scanning tab.
3. Put a check beside the list that contains the file types that you want to export.
4. Click Export.
5. In the confirmation dialog box, specify whether you want to open the file or save it.

Setting limits on nested files

When Symantec Messaging Gateway processes certain compressed files, these files can expand to the point where they deplete system memory. Such container files are often referred to as “zip bombs.” Symantec Messaging Gateway can handle such situations by automatically
sidelining large attachments and stripping the attachments. It assumes that such a file can be a zip bomb and should not be allowed to deplete system resources. Action is taken on the file only because of its size, not because of any indication that it contains a virus or other violation.

You can specify this size threshold and the maximum extraction level that Symantec Messaging Gateway processes in memory. You can also specify a time limit for scanning containers. If a configured limit is reached, Symantec Messaging Gateway performs the action that you specify for the **Unscannable for malware and content filtering** category.

The following table describes at what threshold a container is unscannable for each option that you can configure:

<table>
<thead>
<tr>
<th>Maximum container scan depth</th>
<th>The nested depth in a container file (such as a .zip file or email message) exceeds the number specified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not set this value too high. You can be vulnerable to denial-of-service attacks or zip bombs, which contain many levels of nested files.</td>
<td></td>
</tr>
<tr>
<td>Maximum time to open container</td>
<td>The specified time elapses during a scan of container attachments (such as .zip files).</td>
</tr>
<tr>
<td>Use this setting to detect the containers that do not exceed the other container settings, but include container nesting, many files, large files, or a combination of these.</td>
<td></td>
</tr>
<tr>
<td>Maximum individual file size when opened</td>
<td>Any individual component of the container exceeds the size that is specified when unpacked.</td>
</tr>
<tr>
<td>Maximum accumulated file size when opened</td>
<td>The total size of all the files in a container exceeds the size that is specified when unpacked.</td>
</tr>
</tbody>
</table>

**To set limits on nested files**

1. In the Control Center, click **Protocols > SMTP > Settings** and then click the **Content Scanning** tab.
2. Under **Container Limits**, in the **Maximum container scan depth** box, type the maximum number of container depths.
3. In the **Maximum time to open container** box, type a value, and then click the drop-down menu to specify the **Seconds**, **Minutes**, or **Hours**.
4. In the **Maximum individual file size when opened** box, type the maximum file size, and then click the drop-down menu to select **KB**, **MB**, or **GB**.
5. In the **Maximum accumulated file size when opened** box, type the maximum accumulated file size, and then click the drop-down menu to select **KB**, **MB**, or **GB**.
6. Click **Save**.
## Keeping virus definitions current

Table 9-10 describes all the ways you can keep your virus definitions current. You can perform these tasks as needed in any order.

### Table 9-10 Ways to maintain current virus definitions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about why you should maintain current definitions and how Symantec Messaging Gateway updates definitions.</td>
<td>Symantec Messaging Gateway relies on up-to-date information to detect viruses and threats. One of the most common reasons that problems occur is that virus definition files are not up-to-date. Symantec regularly supplies the updated virus definition files that contain the necessary information about all newly discovered viruses and threats. Regular updates of that information maximize security and guard your organization against infections and the downtime that is associated with an outbreak. See “About updating virus definitions” on page 231.</td>
</tr>
</tbody>
</table>
| Monitor the status of your definition updates.                       | The LiveUpdate status provides the following details:  
  ■ Last LiveUpdate attempt  
  ■ Last virus definitions LiveUpdate status  
  ■ Virus definitions version (revision)  
  ■ Current virus definition manifest  
  See “Viewing the status of your virus definitions” on page 232. |
| Schedule automatic updates to ensure that you are continually protected. | When you schedule automatic virus definition updates, you ensure that you obtain the most current definitions available from Symantec. You can specify how often you want Symantec Messaging Gateway to attempt to obtain virus definitions.  
  See “Scheduling automatic virus definition updates” on page 232. |
| Disable automatic updates as needed.                                | You may want to disable automatic updates. When you disable automatic updates, you must perform on-demand updates to obtain new virus definitions.  
  See “Disabling automatic virus definition updates” on page 233. |
| Perform an on-demand definition update when you need the most current definitions now. | You can initiate a LiveUpdate at any time, even if you schedule automatic updates.  
  See “Initiating virus definition updates on demand” on page 234. |
About updating virus definitions

Symantec Messaging Gateway relies on up-to-date information to detect viruses and threats. One of the most common reasons that problems occur is that virus definition files are not up-to-date. Symantec regularly supplies the updated virus definition files that contain the necessary information about all newly discovered viruses and threats. Regular updates of that information maximize security and guard your organization against infections and the downtime that is associated with an outbreak.

Every 10 minutes, Symantec Messaging Gateway polls Symantec servers to see if updates are available. If they are, that information appears on the Status page. However, updates are only downloaded based on the schedule that you specify. Or you can download definition updates manually.

Table 9-11 lists the methods that you can use to obtain updated virus definitions from Symantec.

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUpdate</td>
<td>You can use LiveUpdate to automatically update your protection. When LiveUpdate runs, it downloads and installs available definitions. You can configure LiveUpdate to run on a scheduled basis, or you can run it on demand. LiveUpdate is enabled by default to update definitions Monday through Friday every 10 minutes. See “Scheduling automatic virus definition updates” on page 232. See “Initiating virus definition updates on demand” on page 234.</td>
</tr>
<tr>
<td>Rapid Response</td>
<td>LiveUpdate Rapid Response updates are now obsolete and are no longer supported. Automatic updates now occur on a more frequent schedule.</td>
</tr>
</tbody>
</table>

You can select the source from where you want to obtain virus definitions. If your organization has several appliances, you can obtain definitions on an internal server. Then you can disseminate the definitions to all of your Symantec Messaging Gateway appliances. This
configuration lets you limit the amount of Internet traffic that accesses Symantec LiveUpdate. In this scenario, you must specify the information for the LAN host and proxy, if required.

See “Specifying from where to obtain virus definitions” on page 234.

You must have a valid content license to install definition files. A content license is a grant by Symantec Corporation for you to update Symantec corporate software with the latest associated content, such as new definitions. When you do not have a content license or your license expires, your product does not receive the most current definitions. Your environment is vulnerable to attacks.

See “Licensing your product” on page 714.

Viewing the status of your virus definitions

Symantec Messaging Gateway provides details about the status of your virus definitions.

The LiveUpdate status provides the following details:

- **Last LiveUpdate attempt**: The day, date, and time that Symantec Messaging Gateway last attempted a virus definition update.
- **Last virus definitions LiveUpdate status**: Whether the last attempted virus definition update was successful.
- **Virus definitions version (revision)**: The version of the current virus definitions.
- **Current virus definition manifest**: A list of virus definitions that are contained in this update.

To view the status of your virus definitions

✦ In the Control Center, click **Malware > Email Scan Settings > LiveUpdate**.

The LiveUpdate status appears under the **LiveUpdate Settings** label.

Scheduling automatic virus definition updates

When you schedule automatic virus definition updates, you ensure that you obtain the most current definitions available from Symantec. You can specify how often you want Symantec Messaging Gateway to attempt to obtain virus definitions.

You can only schedule automatic updates through LiveUpdate.

See “Specifying from where to obtain virus definitions” on page 234.

See “Disabling automatic virus definition updates” on page 233.
To schedule automatic virus definition updates

1 In the Control Center, click Malware > Email Scan Settings > LiveUpdate.

2 Under LiveUpdate Schedule, click Enable automatic updates on the following schedule.

3 Check the appropriate boxes to specify the days of the week at which to begin LiveUpdate. (Recommended: Leave every box checked.)

4 Use the First Attempt controls to specify the time when you want the first LiveUpdate attempt to begin.

5 Choose a Frequency setting to specify how often LiveUpdate runs after the first time. The default value is once every 10 minutes.

6 Choose a Source for the LiveUpdate virus definitions:
   - If you choose Download certified virus definitions from the Symantec website, Symantec Messaging Gateway downloads the virus definitions directly from the internet. This is the default setting.
   - If your organization has a LiveUpdate Administrator server installed on your network, you can choose Download virus definitions from a LAN host. If the LiveUpdate Administrator requires authentication, enter the LAN Host Address, Username and Password that Symantec Messaging Gateway must provide.
     If you also want to use a proxy for communication with the LiveUpdate Administrator, check Use a proxy and enter the Proxy host and Proxy port information that is needed to communicate with the proxy server. If the proxy server requires authentication, enter the Username and Password that Symantec Messaging Gateway must provide.

7 You can enter a value between 3 minutes and 60 minutes. The default is 20 minutes.

8 Click Save.

Disabling automatic virus definition updates

You may want to disable automatic updates. When you disable automatic updates, you must perform on-demand updates to obtain new virus definitions.

---

Warning: When you disable automatic updates, you run the risk of allowing viruses and malicious attacks into your environment. Automatic virus definition updates ensures that your network always has the latest protection available to defend against threats.
To disable automatic virus definition updates

1. In the Control Center, click **Malware > Email Scan Settings > LiveUpdate**.
2. Click **Disable automatic updates**.
3. Click **Save**.

Initiating virus definition updates on demand

You can initiate a LiveUpdate at any time, even if you schedule automatic updates.

To initiate virus definition updates on demand

1. Click **Malware > Email Scan Settings > LiveUpdate**.
2. Click **LiveUpdate Now**.

See “**Viewing the status of your virus definitions**” on page 232.

See “**Specifying from where to obtain virus definitions**” on page 234.

Specifying from where to obtain virus definitions

You can specify the source from where you want to obtain virus definitions as follows:

- **Symantec Web site**  Downloads the virus definitions directly from the Symantec LiveUpdate server.  This option is the default setting.
- **LAN host**  If your organization has several appliances, you can obtain definitions on an internal server. Then you can disseminate the definitions to all of your Symantec Messaging Gateway appliances. This configuration lets you limit the amount of Internet traffic that accesses Symantec LiveUpdate. In this scenario, you must specify the information for the LAN host and proxy, if required.

See “**Scheduling automatic virus definition updates**” on page 232.
See “**Initiating virus definition updates on demand**” on page 234.

To obtain virus definition updates from Symantec LiveUpdate server

1. In the Control Center, click **Malware > Email Scan Settings > LiveUpdate**.
2. Under **Source**, select **Download certified virus definitions from the Symantec website**.
   
   LiveUpdate uses the proxy that is defined on the **Proxy** tab of the **Administration > Hosts > Configuration > Edit** page.
3. Click **Save**.
To obtain virus definition updates from a LAN host

1. In the Control Center, click **Malware > Email Scan Settings > LiveUpdate**.

2. Under **Source**, click **Download virus definitions from a LAN host**.

   If you download virus definitions from a LAN host, LiveUpdate uses a proxy only if you specify one under **Use a proxy**.

   Refer to the *LiveUpdate Administrator's Guide* for more information about how to set up a LAN host.

3. In the **Address** field, type the address of the LAN host.

   Use a URL, not a host name.

4. In the **Username** field and **Password** field, type the user name and password, if required to access the LAN host.

5. If you use a proxy server, check **Use a proxy**.

6. In the **Proxy** host field, type a valid host name.

7. In the **Proxy port** field, type a valid port number.

8. In the **Username** field and **Password** field, type the user name and password if they are required to access the proxy host.

9. Click **Save**.

---

### Modifying the artificial intelligence sensitivity level

By default, Messaging Gateway blocks malicious content using static and dynamic artificial intelligence as well as virus definitions. The sensitivity level determines the way in which the system uses artificial intelligence to detect malware and to scan for threats for which no known definitions exist. In addition to scanning for known threats (static), Messaging Gateway uses artificial intelligence technology to scan for unusual behaviors (dynamic) to target potentially infected message bodies and attachments.

Artificial intelligence scanning involve a trade-off between malware-detection rates and false positives. Lower artificial intelligence sensitivity levels may miss more malware but produce fewer false positives. Higher artificial intelligence sensitivity levels may catch more malware but cause more false-positive detections. For environments where high false positives are acceptable, choose **High Detection Sensitivity** to increase blocking of malicious content. To minimize false positives, choose **Low Detection Sensitivity** to provide the best blocking of malicious content at the lowest false-positive cost.

**To modify the sensitivity level**

1. Click **Malware > Settings > Email Scan Settings**.

2. Click the **General** tab.
3 Under, click the level that you want.
   The default setting is Medium Detection Sensitivity.

4 Click **Save**.

See “Detecting viruses, malware, and malicious threats” on page 215.
Quarantining suspected viruses

This chapter includes the following topics:

■ About quarantining suspected viruses
■ About navigating the Suspect Virus Quarantine
■ Configuring suspect virus message settings
■ Working with suspect viruses messages

About quarantining suspected viruses

When Symantec Messaging Gateway scans a message with a suspicious attachment, it places the message into Suspect Virus Quarantine.

To use Suspect Virus Quarantine, your malware policy must use one of the following actions for suspicious attachments:

■ Hold message in Suspect Virus Quarantine
■ Strip and Delay in Suspect Virus Quarantine

Messages remain in Suspect Virus Quarantine until one of the following conditions occur:
The message is held in quarantine for the specified time. You can specify how long you want to retain messages with suspicious attachments in quarantine. The default value is 6 hours.

You retain messages in quarantine to give Symantec time to release updated virus definitions with which to rescan the message. When the message is rescanned with updated definitions, it will receive a verdict of either clean or infected.

**Note:** Note: If you modify the default value, ensure that you allow adequate time for Symantec Messaging Gateway to download the latest antivirus definitions.

See “Specifying how long suspect virus messages are retained in quarantine” on page 241.

You manually release or delete the message from Suspect Virus Quarantine. See “Deleting suspect virus messages in quarantine” on page 243.

See “Releasing suspect virus messages from quarantine” on page 244.

The Suspect Virus Quarantine's maximum size limit is exceeded. If the quarantine exceeds the maximum size, messages in the quarantine are automatically deleted to make room for new messages.

You can specify the maximum limit.

See “Modifying the disk space allotted for Suspect Virus Quarantine” on page 241.

The existing policy is evaluated and acted upon. Symantec Messaging Gateway evaluates your policy and performs the actions that you specified for the messages with suspicious attachments.

See “What you can do with suspicious attachments” on page 214.

---

**About navigating the Suspect Virus Quarantine**

The following navigation icons help you navigate through messages on the Suspect Virus Message Quarantine page as follows:

- **Go to beginning of messages.**
- **Navigate to last page of messages or 50 pages ahead if there are more than 50 pages.**
- **Go to previous page of messages.**
- **Go to next page of messages.**
Choose up to 500 pages before or after the current page of messages.

When you navigate to a different page of messages, the status of the check boxes in the original page is not preserved. For example, assume that you select three messages on the first page of messages and then move to the next page. When you return to the first page, all of the message check boxes are cleared.

See “ Viewing suspect virus messages in quarantine” on page 243.

See “ Specifying the number of suspect virus message entries to view per page” on page 240.

See “ Sorting suspect virus messages in quarantine” on page 243.

See “ Searching quarantined virus messages” on page 245.

Configuring suspect virus message settings

Table 10-1 describes all the ways you can configure suspect virus message settings. You can perform these tasks as needed in any order.

Table 10-1  Virus message settings

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the language encoding when necessary.</td>
<td>In most cases, the Auto-detect setting properly determines the language encoding for a message in Suspect Virus Quarantine. However, the Control Center may not be able to determine the proper language encoding for some messages. If the message is garbled, select the language encoding most likely to match the encoding that is used in the message.</td>
</tr>
<tr>
<td></td>
<td>See “ Choosing the language encoding for suspect virus messages” on page 240.</td>
</tr>
<tr>
<td>Customize the quarantine view.</td>
<td>You can specify how many quarantined message entries appear per page.</td>
</tr>
<tr>
<td></td>
<td>See “ Specifying the number of suspect virus message entries to view per page” on page 240.</td>
</tr>
<tr>
<td>Schedule when Symantec Messaging Gateway should automatically release messages in the Suspect Virus Quarantine.</td>
<td>You can choose the maximum amount of time a message can be held in Suspect Virus Quarantine. After the period of time that you specify, messages are automatically released from Suspect Virus Quarantine and rescanned with updated virus definitions.</td>
</tr>
<tr>
<td></td>
<td>See “ Specifying how long suspect virus messages are retained in quarantine” on page 241.</td>
</tr>
</tbody>
</table>
Choosing the language encoding for suspect virus messages

In most cases, the Auto-detect setting properly determines the language encoding for a message in Suspect Virus Quarantine. However, the Control Center may not be able to determine the proper language encoding for some messages. If the message is garbled, select the language encoding most likely to match the encoding that is used in the message.

See “Viewing suspect virus messages in quarantine” on page 243.

See “About navigating the Suspect Virus Quarantine” on page 238.

Only the administrators that have Full Administration rights or Manage Quarantine modify rights can choose language encoding for messages in quarantine.

To choose the language encoding for suspect virus messages

1. In the Control Center, click Malware > Quarantine > Email Suspect Virus.
2. Click on the subject line of the message that you want to view.
3. On the message details page, select the language encoding in the drop-down list.

Specifying the number of suspect virus message entries to view per page

You can specify how many quarantined message entries appear per page.

You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Suspect Virus Quarantine.

To specify the number of suspect virus message entries to view per page

1. From the Control Center, click Malware > Quarantine > Email Suspect Virus.
2. Click the Entries per page drop-down list, and select a number.

See “Viewing suspect virus messages in quarantine” on page 243.

See “About navigating the Suspect Virus Quarantine” on page 238.

See “Sorting suspect virus messages in quarantine” on page 243.

---

Table 10-1  
Virus message settings (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can specify the amount of disk space that Suspect Virus Quarantine uses. See “Modifying the disk space allotted for Suspect Virus Quarantine” on page 241.</td>
<td></td>
</tr>
</tbody>
</table>

To optimize your system's resources, you can specify the maximum disk space the quarantine uses.
Specifying how long suspect virus messages are retained in quarantine

You can choose the maximum amount of time a message can be held in Suspect Virus Quarantine, up to 24 hours. After the period of time that you specify, messages are automatically released from Suspect Virus Quarantine and rescanned with updated virus definitions.

You can check the status of your scheduled task from the **Status > Scheduled Tasks** page.

You can also delete messages manually from Suspect Virus Quarantine.

You must have Full Administration or Modify rights to change Suspect Virus Quarantine settings.

**To specify how long suspect virus messages are held in quarantine**

1. On the Control Center, click **Malware > Settings > Suspect Virus Settings**.
2. Under **Message Release**, click the **Automatically release messages older than** drop-down list and select the number of hours to hold messages in quarantine.
   - The default is six hours. The maximum setting is 24 hours.
3. Click **Save**.

Modifying the disk space allotted for Suspect Virus Quarantine

You can specify the amount of disk space that Suspect Virus Quarantine uses. The default disk space is 10 GB.

Only administrators with Full Administration rights or Manage Settings modify rights can modify Suspect Virus Quarantine settings.

**To modify the disk space allotted for Suspect Virus Quarantine**

1. Click **Malware > Settings > Suspect Virus Settings**.
2. Check **Maximum size of the Suspect Virus Quarantine** to enable the threshold.
3. Specify the amount of disk space you want to allot for Suspect Virus Quarantine.
   - The default is 10 GB.
4. Click **Save**.

See “**Specifying how long suspect virus messages are retained in quarantine**” on page 241.
Working with suspect viruses messages

Table 10-2 describes what you can do with messages in Suspect Virus Quarantine. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the messages in the quarantine to determine what action you should take.</td>
<td>You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Suspect Virus Quarantine. See “Viewing suspect virus messages in quarantine” on page 243.</td>
</tr>
<tr>
<td>Sort messages in the quarantine.</td>
<td>You can sort messages in Suspect Virus Quarantine by date to make it easier to categorize the messages or locate a specific message. By default, messages appear in date descending order. The newest messages are listed at the top of the page. See “Sorting suspect virus messages in quarantine” on page 243.</td>
</tr>
<tr>
<td>Search for a specific message.</td>
<td>The ability to search messages lets you more easily find a specific message that you want to view, delete, or release. See “Searching quarantined virus messages” on page 245. See “Suspect virus message search criteria and tips” on page 246.</td>
</tr>
<tr>
<td>Completely delete messages from the quarantine.</td>
<td>You can delete messages in Suspect Virus Quarantine one at a time, or you can delete several messages at once. When you delete a message, it is no longer accessible. See “Deleting suspect virus messages in quarantine” on page 243.</td>
</tr>
<tr>
<td>Release messages from the quarantine to the intended recipients.</td>
<td>You can release messages from the Suspect Virus Quarantine to be rescanned with the latest virus definitions. If Symantec Messaging Gateway is unable to repair the virus and your policy is to quarantine suspect viruses, Symantec Messaging Gateway returns the message to the quarantine. You can release one message at a time, or you can release all messages at once. You can also set up automatic releases and rescanning of suspect virus messages. See “Releasing suspect virus messages from quarantine” on page 244. See “Specifying how long suspect virus messages are retained in quarantine” on page 241.</td>
</tr>
</tbody>
</table>
Viewing suspect virus messages in quarantine

You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Suspect Virus Quarantine.

To view suspect virus messages in quarantine

- Do one of the following:

  If you are not on the Suspect Virus Message Quarantine page
  
  In the Control Center, click Virus > Quarantine > Email Suspect Virus.

  If you are on the Suspect Virus Message Quarantine page and want to see the newly arrived messages
  
  On the Virus > Quarantine > Email Suspect Virus page, if the Display All icon is not visible, click Show Filters, and then click Display All.

Sorting suspect virus messages in quarantine

You can sort messages in Suspect Virus Quarantine by date to make it easier to categorize the messages or locate a specific message. By default, messages appear in date descending order. The newest messages are listed at the top of the page.

You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Suspect Virus Quarantine.

To sort suspect virus messages in quarantine

1. From the Control Center, click Malware > Quarantine > Email Suspect Virus.

2. Click on the Date column heading to sort by ascending order or descending order.

See “Viewing suspect virus messages in quarantine” on page 243.

See “Specifying the number of suspect virus message entries to view per page” on page 240.

See “About navigating the Suspect Virus Quarantine” on page 238.

See “Searching quarantined virus messages” on page 245.

Deleting suspect virus messages in quarantine

You can delete messages in Suspect Virus Quarantine one at a time, or you can delete several messages at once. When you delete a message, it is no longer accessible. Only the administrators that have Full Administration rights or Manage Quarantine Modify rights can delete messages in quarantine.

See “Viewing suspect virus messages in quarantine” on page 243.
You can also use a purge utility to automatically delete messages from Suspect Virus Quarantine. This utility frees you from having to manually delete messages from the quarantine to free up space. The utility purges messages based on the schedule that you specify.

See “Specifying how long suspect virus messages are retained in quarantine” on page 241.

**To delete individual messages in quarantine**

1. From the Control Center, click **Malware > Quarantine > Email Suspect Virus**.
2. Click on the check box beside each message that you want to delete.
3. Click **Delete**.

**To delete all messages in quarantine**

1. From the Control Center, click **Malware > Quarantine > Email Suspect Virus**.
2. Click **Delete All** to delete all of the messages in Suspect Virus Quarantine, including those on other pages.

---

**Releasing suspect virus messages from quarantine**

You can release messages from the Suspect Virus Quarantine to be rescanned with the latest virus definitions. If Symantec Messaging Gateway is unable to repair the virus and your policy is to quarantine suspect viruses, the message is returned to the Suspect Virus Quarantine.

You can release one message at a time, or you can release all messages at once. You can also set up automatic releases and rescanning of suspect virus messages.

See “Specifying how long suspect virus messages are retained in quarantine” on page 241.

Releasing messages requires access to the IP address of the Control Center. If you limit inbound or outbound SMTP access, check the Inbound Mail Settings and Outbound Mail Settings.

Only administrators with Full Administration rights or Manage Quarantine modify rights can release messages from the quarantine.

See “Deleting suspect virus messages in quarantine” on page 243.

See “About Scanner email settings” on page 43.

**To release individual messages from quarantine**

1. From the Control Center, click **Malware > Quarantine > Email Suspect Virus**.
2. Check the box beside each message that you want to release.
3. Click **Release**.
To release all messages from quarantine

1. From the Control Center, click **Malware > Quarantine > Email Suspect Virus**.
2. Click **Release All** to release all the messages in Suspect Virus Quarantine, including those on other pages.

Searching quarantined virus messages

You can search for messages in Suspect Virus Quarantine. The ability to search messages lets you more easily find a specific message that you want to view, delete, or release. You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Suspect Virus Quarantine.

To search quarantined virus messages

1. In the Control Center, click **Malware > Quarantine > Email Suspect Virus**.
2. On the message list page, click **Show Filters**.
3  Do any of the following to perform a search:

To search message envelope "To" recipient
Type a name or address in the To box to search the message envelope RCPT TO: header.

You can search for a display name, the user name portion of an email address, or any part of a display name or email user name. If you type a full email address in the To box, Symantec Messaging Gateway searches only for the user name portion of user_name@example.com.
The search is limited to the envelope To:, which may contain different information than the header To: that appears on the message details page.

To search "From" headers
Type a name or address in the From box to search the From: header in all messages for a particular sender.

You can search for a display name, email address, or any part of a display name or email address. The search is limited to the visible message From: header, which is usually forged in spam messages. The visible message From: header may contain different information than the message envelope.

To search subject headers
Type in the Subject box to search the Subject: header for all messages about a specific topic.

To search a time range
Click the Time range drop-down list to display all of the messages that were received during the time range that you specify.

4  Click Display Filtered.

See “Viewing suspect virus messages in quarantine” on page 243.
See “Specifying the number of suspect virus message entries to view per page” on page 240.
See “About navigating the Suspect Virus Quarantine” on page 238.
See “Sorting suspect virus messages in quarantine” on page 243.

Suspect virus message search criteria and tips
The search function is optimized for searching a large number of messages. However, this can lead to unexpected search results.
Consider the following tips and information to help you conduct searches in Suspect Virus Quarantine:

<table>
<thead>
<tr>
<th>Tokens</th>
<th>Tokens are matched with substring semantics. Searching for a subject with the search target <code>&lt;in&gt;</code> will match &quot;Lowest rate in 45 years,&quot; &quot;RE: re: Sublime Bulletin (verification),&quot; &quot;Up to 85% off Ink Cartridges + no shipping!,&quot; and &quot;Re-finance at todays super low rate.&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple word searches</td>
<td>If any word in a multiple word search is found in a message, that message is considered a match. For example, searching for red carpet match &quot;red carpet,&quot; &quot;red wine,&quot; and &quot;flying carpet.&quot;</td>
</tr>
<tr>
<td>Case sensitivity</td>
<td>All text searches are case-insensitive. For example, assume you type emerson in the From box. Messages with a From header that contains emerson, Emerson, and eMERSOn all appear in the search results.</td>
</tr>
<tr>
<td>Exact phrases</td>
<td>To search for an exact phrase, enclose the phrase in &quot; &quot; (double quotes).</td>
</tr>
<tr>
<td>Wildcards</td>
<td>You can use * (asterisk) to perform wildcard searches. It also functions as a logical AND character. In addition, you can search on special characters such as &amp; (ampersand), ! (exclamation point), $ (dollar sign), and # (pound sign).</td>
</tr>
<tr>
<td>Single characters</td>
<td>Even a single character is treated as a substring target.</td>
</tr>
<tr>
<td>Special characters</td>
<td>You can search on special characters such as &amp; (ampersand), ! (exclamation point), $ (dollar sign), and # (pound sign).</td>
</tr>
<tr>
<td>Multiple characteristics</td>
<td>If you search for multiple characteristics, only the messages that match the combination of characteristics are listed in the search results. For example, assume you type LPQTech in the From box and Inkjet in the Subject box. Only the messages that contain LPQTech in the From: header and Inkjet in the Subject: header appear in the search results.</td>
</tr>
<tr>
<td>Forged header information</td>
<td>Spammers usually &quot;spoof&quot; or forge some of the visible messages headers such as From and To and the invisible envelope information. Sometimes they forge header information using the actual email addresses or domains of innocent people or companies.</td>
</tr>
<tr>
<td>Time to perform a search</td>
<td>The amount of time it takes to perform the search depends on how many search boxes you use and the number of messages in the mailbox. Searching in the administrator mailbox takes longer than searching in a user's mailbox.</td>
</tr>
</tbody>
</table>

See “Searching quarantined virus messages” on page 245.
Filtering spam

This chapter includes the following topics:

- About filtering email spam and unwanted messages
- Configuring spam and unwanted email detection
- Scanning text-based attachments
- Creating the policies that detect spam and unwanted email
- Reducing false positives from unwanted email filtering
- Enabling and disabling spam and unwanted email policies
- Modifying spam and unwanted email policies
- Copying spam policies
- Deleting spam policies
- Configuring the threshold for suspected spam identification
- Enabling or disabling URI reporting to Symantec
- Enabling or disabling URL reputation filtering
- About submitting messages for customer-specific spam rules

About filtering email spam and unwanted messages

Symantec Messaging Gateway provides a set of default spam and unwanted email policies. For a new install, the unwanted email policies are not assigned to any group. If you upgrade from a previous release, the unwanted email policies are disabled and not assigned to any group. You can modify the actions in these policies or create your own policies.

See “Default email spam and unwanted email policies” on page 250.
You can modify the policy settings for spam, suspected spam, marketing emails, newsletters, and redirect URLs.

Table 11-1 describes the categories of unwanted emails.

<table>
<thead>
<tr>
<th>Unwanted email category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing mail</td>
<td>Email messages that contain commercial or fund-raising messages, that may have been requested by the user. These messages often do not include a functional opt-out facility.</td>
</tr>
<tr>
<td>Newsletter</td>
<td>Email messages that include content on specific topics, on a known periodic basis, often weekly or monthly. The user may have requested to receive these publications. A functional opt-out facility is generally available.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Redirect URLs include free hosting sites, URL shortening services, and URL redirecting services which can potentially be abused to deliver spam or malware payloads. Symantec Messaging Gateway can filter against email messages that contain one or more redirect URLs.</td>
</tr>
</tbody>
</table>

Symantec Messaging Gateway supports the false positive and false negative submissions that are related to the following unwanted email verdicts:

- Marketing mail
- Newsletter
- Redirect URL

You can specify how you want spam, suspected spam, or unwanted emails handled. For example, you can send suspected spam messages to the Spam Quarantine. You can also prepend the subject line to let users know that the message is suspected spam.

**Note:** Filtering for unwanted emails can result in legitimate messages being filtered. Symantec recommends starting with an action such as subject line markup or quarantining.

See “About quarantining spam” on page 280.

See “Creating the policies that detect spam and unwanted email” on page 256.

See “Configuring the threshold for suspected spam identification” on page 262.
Default email spam and unwanted email policies

Symantec Messaging Gateway installs with a set of default spam and unwanted email policies. The default spam policies are automatically enabled and assigned to the default policy group. For a new install, the unwanted email policies are not assigned to any group. If you upgrade from a previous release, the unwanted email policies are disabled and not assigned to any group.

If you create a custom email spam or unwanted email policy and apply it to the default policy group, that policy overrides the default policy.

Table 11-2 Preconfigured spam policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Applies to the following messages</th>
<th>If the following condition is met</th>
<th>Actions</th>
<th>Applies to the following policy group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam: Modify subject line with &quot;[Spam]&quot; (default)</td>
<td>Inbound and outbound</td>
<td>If a message is spam</td>
<td>Prepends the subject line with &quot;[Spam]&quot;</td>
<td>Default group</td>
<td>Enabled</td>
</tr>
<tr>
<td>Suspected Spam: Modify subject line with &quot;[Suspected Spam]&quot; (default)</td>
<td>Inbound and outbound</td>
<td>If a message is suspected spam</td>
<td>Prepends the subject line with &quot;[Suspected Spam]&quot;</td>
<td>Default group</td>
<td>Enabled</td>
</tr>
<tr>
<td>Spam or Suspected Spam: Delete message</td>
<td>Inbound and outbound</td>
<td>If a message is spam or suspected spam</td>
<td>Delete message</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Spam or Suspected Spam: Quarantine message</td>
<td>Inbound and outbound</td>
<td>If a message is spam or suspected spam</td>
<td>Hold message in Spam Quarantine</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Spam or Suspected Spam: Deliver normally</td>
<td>Inbound and outbound</td>
<td>If a message is spam or suspected spam</td>
<td>Deliver message normally</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Policy name</td>
<td>Applies to the following messages</td>
<td>If the following condition is met</td>
<td>Actions</td>
<td>Applies to the following policy group</td>
<td>Default status</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Spam or Suspected Spam: Add X-header</td>
<td>Inbound and outbound</td>
<td>If a message is spam or suspected spam</td>
<td>Add an X-header to the spam message</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer-specific Spam: Modify subject line with &quot;[Customer-specific Spam]&quot;</td>
<td>Inbound</td>
<td>If a message is customer-specific spam</td>
<td>Prepend subject line with &quot;[Customer-specific Spam]&quot;</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer-specific Spam: Delete message</td>
<td>Inbound</td>
<td>If a message is customer-specific spam</td>
<td>Delete message</td>
<td>None</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

This policy is available for the versions that are migrated to version 9.5.

This policy is not available as a preconfigured policy on new installations of version 9.5 or later.

This policy cannot be enabled or modified until you enable the customer-specific spam submissions feature.
## Table 11-2  Preconfigured spam policies (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Applies to the following messages</th>
<th>If the following condition is met</th>
<th>Actions</th>
<th>Applies to the following policy group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer-specific Spam: Quarantine message</td>
<td>Inbound</td>
<td>If a message is customer-specific spam</td>
<td>Quarantine message</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This policy cannot be enabled or modified until you enable the customer-specific spam submissions feature.</td>
</tr>
<tr>
<td>Customer-specific Spam: Deliver normally</td>
<td>Inbound</td>
<td>If a message is customer-specific spam</td>
<td>Deliver message normally</td>
<td>None</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This policy cannot be enabled or modified until you enable the customer-specific spam submissions feature.</td>
</tr>
<tr>
<td>Failed Bounce Attack Validation: Reject message (default)</td>
<td>Inbound only</td>
<td>If a message fails bounce attack validation</td>
<td>Reject messages failing bounce attack validation</td>
<td>Default group</td>
<td>Enabled</td>
</tr>
<tr>
<td>Marketing Mail: Modify subject line with &quot;[Marketing Mail]&quot;</td>
<td>Inbound only</td>
<td>If a message is a marketing email</td>
<td>Prepends the subject line with &quot;[Marketing Mail]&quot;</td>
<td>None</td>
<td>Enabled</td>
</tr>
<tr>
<td>Newsletter: Modify subject line with &quot;[Newsletter]&quot;</td>
<td>Inbound only</td>
<td>If a message is a newsletter</td>
<td>Prepends the subject line with &quot;[Newsletter]&quot;</td>
<td>None</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Table 11-2  Preconfigured spam policies (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Applies to the following messages</th>
<th>If the following condition is met</th>
<th>Actions</th>
<th>Applies to the following policy group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect URL Content: Modify subject line with &quot;[Caution: Message contains Redirect URL content]&quot;</td>
<td>Inbound only</td>
<td>If a message contains redirect URL content</td>
<td>Prepends the subject line with &quot;[Caution: Message contains Redirect URL content]&quot;</td>
<td>None</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Configuring spam and unwanted email detection

Table 11-3 describes the tasks that you can perform to detect and enhance spam and unwanted email detection capabilities.

Table 11-3  Configure spam and unwanted email detection

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and enable email spam and unwanted email policies.</td>
<td>Symantec Messaging Gateway installs with a set of default spam and unwanted email policies. For a new installation or upgrade, the default spam policies are automatically enabled and assigned to the default policy group. For a new install, the preconfigured unwanted email policies are enabled but not assigned to any group. If you upgrade from a previous release, the preconfigured unwanted email policies are disabled and not assigned to any group. You can modify these policies or create your own custom policies. See “Default email spam and unwanted email policies” on page 250. See “Creating the policies that detect spam and unwanted email” on page 256. See “Modifying spam and unwanted email policies” on page 260. See “Configuring spam and unwanted email detection” on page 253.</td>
</tr>
</tbody>
</table>
When Symantec Messaging Gateway evaluates whether messages are spam, it calculates a spam score from 1 to 100 for each message. This score is based on the results of a wide variety of antispam technologies. You can define a range of scores from 25 to 89 that constitutes "suspected spam." Through policies, you can specify different actions for the messages that are identified as suspected spam and messages that are identified as spam.

Symantec recommends that you not adjust the spam threshold until you have some exposure into the filtering patterns at your site. Gradually move the threshold setting down 1 point to 5 points per week until the number of false positives is at an acceptable level.

See "Configuring the threshold for suspected spam identification" on page 262.

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the suspected spam level.</td>
<td>When Symantec Messaging Gateway evaluates whether messages are spam, it calculates a spam score from 1 to 100 for each message. This score is based on the results of a wide variety of antispam technologies. You can define a range of scores from 25 to 89 that constitutes “suspected spam.” Through policies, you can specify different actions for the messages that are identified as suspected spam and messages that are identified as spam. Symantec recommends that you not adjust the spam threshold until you have some exposure into the filtering patterns at your site. Gradually move the threshold setting down 1 point to 5 points per week until the number of false positives is at an acceptable level. See &quot;Configuring the threshold for suspected spam identification&quot; on page 262.</td>
</tr>
</tbody>
</table>
| Enable the features that provide Symantec with information that helps us create better spam filters. | You can help Symantec create better spam filters when you enable the following features:  
- Uniform Resource Identifiers (URI) reporting  
  When you enable URI reporting, Symantec Messaging Gateway sends a report to Symantec Security Response. The report contains URIs that appear in the messages that Symantec Messaging Gateway scans for spam. Symantec uses this information to develop new URI-based filters. See “Enabling or disabling URI reporting to Symantec” on page 263.  
- Probe accounts  
  You can forward unused email addresses or invalid email addresses to the Symantec Probe Network. Symantec uses these email addresses to attract spammers. Then Symantec uses the spam messages it receives at these addresses to create better spam filters. See “Enabling probe participation” on page 317. See “Creating probe accounts from invalid recipient email addresses” on page 318. See “Enabling probe accounts” on page 320. |
### Table 11-3  Configure spam and unwanted email detection (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Configure the Spam Quarantine.**      | You can route spam, suspected spam, or unwanted emails to Spam Quarantine. Users access Spam Quarantine to determine if messages in the quarantine are false positives. If a message is stored in the spam quarantine, but is legitimate, users can release the messages to their inboxes. Users can notify you of false positives so that you can continue to adjust your spam settings and spam and unwanted email policies accordingly. You can also set up summary notifications to be delivered to users' inboxes.  
See “Before you use Spam Quarantine” on page 281.  
See “Configuring end user quarantine” on page 284.  
See “Specifying who to notify of false positive messages” on page 290.  
See “About configuring the user and distribution list notification digests” on page 303.  
You can configure thresholds to control the space that is allocated for Spam Quarantine.  
See “Modifying Spam Quarantine thresholds” on page 287.  
See “Specifying when and how often Spam Quarantine is expunged” on page 289. |
| **Monitor reports.**                    | Monitor reports to determine how effective spam policies are. Reports also indicate the volume of spam that your organization receives. This information can help you fine-tune your spam detection settings. |
| **Text-based attachment scanning.**    | Symantec Messaging Gateway can scan email attachments with the following extensions for spam:  
■ .doc  
■ .htm  
■ .html  
■ .rtf  
■ .txt  
■ .wps  
■ .xml  
By default, this option is enabled for a new installation and disabled for upgrades. Enabling this option may result in slower performance of Symantec Messaging Gateway. When this option is disabled, Symantec Messaging Gateway does not use all scanning technologies for evaluating the attachments for spam.  
See “Scanning text-based attachments” on page 256. |
See “About filtering email spam and unwanted messages” on page 248.

Scanning text-based attachments

Symantec Messaging Gateway can scan email attachments with the following extensions for spam:

- .doc
- .htm
- .html
- .rtf
- .txt
- .wps
- .xml

To scan text-based attachments

1. In the Control Center, click **Spam > Settings > Scan Settings**.
2. Under **Text-based Attachment Scanning**, click **Scan text-based attachments**.

By default, this option is enabled for a new installation and disabled for upgrade. Enabling this option may result in slower performance of Symantec Messaging Gateway. When this option is disabled, Symantec Messaging Gateway does not use all scanning technologies for evaluating the attachments for spam.

See “Configuring spam and unwanted email detection” on page 253.

Creating the policies that detect spam and unwanted email

You can create the email spam policies that determine the actions to be taken for specific spam conditions.

Symantec Messaging Gateway installs with several preconfigured policies. You can use these policies as is, edit them to suit your needs, or create your own custom policies.

See “Default email spam and unwanted email policies” on page 250.

When you create a new spam policy, it is enabled by default.
To create the policies that detect spam and unwanted email

1. In the Control Center, click **Spam > Policies > Email**.
2. Click **Add**.
3. On the **Email Spam Policy** page, in the **Policy name** box type a name for the spam policy.

   Content filtering, spam, and malware policy names must be unique. For example, if you have a content filtering policy called "XYZ," you cannot have a spam policy or malware policy called "XYZ."

4. Under **Conditions** click the **Apply to** drop-down list and choose whether the policy is applied to inbound messages only, outbound messages only, or both.

5. Click the **If the following condition is met** drop-down list and select one of the following options:

   - **If a message contains redirect URL content**: Performs the specified action if a message contains redirect URL content.
   - **If a message fails bounce attack validation**: Performs the specified action if a message is a Non-Delivery Receipt message that does not pass validation. This condition is only available for Inbound messages.
   - **If a message is a marketing mail**: Performs the specified action if a message is a marketing email.
   - **If a message is a newsletter**: Performs the specified action if a message is a newsletter.
   - **If a message is customer-specific spam**: Performs the specified action if a message is identified as spam based on a customer-specific spam rule.
   - **If a message is spam**: Performs the specified action if a message is spam.
   - **If a message is spam or suspected spam**: Perform the specified action if a message is either spam or suspected spam.
   - **If a message is suspected spam**: Perform the specified action if a message might be spam. The suspected spam level is adjustable on the **Spam > Settings > Scan Settings** page.

6. Under **Actions**, click **Add**.
On the **Configure An Action** page, click the drop-down list and select the action to take on a message that meets the specified spam condition.

For some actions, you need to specify additional information.

See "Policy actions and what they do" on page 333.

On the **Configure An Action** page, click **Add Action**. You can add additional actions as needed.

Under **Apply to the following groups**, check one or more policy groups to which this policy should apply.

Click **Save**.

---

**Reducing false positives from unwanted email filtering**

You may need to fine-tune your settings to reduce incidents of false positives.

Table 11-4 describes how you can fine-tune settings when users do not receive expected email. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable, enable or reenable, and modify the filtering policy.</td>
<td>To troubleshoot incidents of false positives, disable the policy that you believe might have created the issue. One-by-one you can disable and re-enable policies until you identify the one that needs to be modified. When you identify the policy that you need to modify, edit it and re-enable it. See “Editing, deleting, enabling, or disabling a policy group” on page 195.</td>
</tr>
<tr>
<td>Change the action that is specified in the filtering policy to something less severe.</td>
<td>For example, instead of deleting the message, you can send the message to Spam Quarantine or use subject line markup. See “Creating the policies that detect spam and unwanted email” on page 256.</td>
</tr>
<tr>
<td>Change the policy groups that use the filtering policy.</td>
<td>Another possible solution is to turn off filtering for a subset of users. See “Selecting spam and unwanted email policies for a policy group” on page 198.</td>
</tr>
</tbody>
</table>
Table 11-4 Ways to reduce false positives (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add the sender to the Third Party Good Senders group.</td>
<td>If you are certain of the senders reputation, you can add the sender to the Third Party Good Senders group. Messages from senders in this group automatically bypass spam filtering. See “Adding senders to administrator and third party sender groups” on page 130.</td>
</tr>
<tr>
<td>Add a content filtering policy.</td>
<td>The policy should have a condition that finds the particular messages that were erroneously filtered. You can then specify the <strong>Bypass spam scanning</strong> action. See “Creating a content filtering policy” on page 325.</td>
</tr>
</tbody>
</table>

Enabling and disabling spam and unwanted email policies

New spam and unwanted email policies are enabled by default. For a new installation or upgrade, the default spam policies are automatically enabled and assigned to the default policy group. For a new install, the preconfigured unwanted email policies are enabled but not assigned to any group. If you upgrade from a previous release, the preconfigured unwanted email policies are disabled and not assigned to any group. You can disable any policy that you do not want Symantec Messaging Gateway to use when it scans email messages.

You can disable a spam policy to troubleshoot antispam scanning issues. For example, you can disable the policies that you no longer want to use but do not want to delete yet.

Unwanted email is defined as follows:

- Suspected spam
- Marketing mail
- Newsletters
- Email messages that contain one or more redirect URLs
To enable or disable spam or unwanted email policies

1. In the Control Center, click **Spam > Policies > Email**.
2. Check the box beside the policy that you want to enable to disable.
3. Select one of the following options:

   - **Enable**: When you enable a policy, a green check mark appears in the **Enabled** column.
   - **Disable**: When you disable a policy, a horizontal line appears in the **Enabled** column.

See “About filtering email spam and unwanted messages” on page 248.
See “Creating the policies that detect spam and unwanted email” on page 256.
See “Modifying spam and unwanted email policies” on page 260.
See “Copying spam policies” on page 261.
See “Deleting spam policies” on page 262.

## Modifying spam and unwanted email policies

You can modify spam and unwanted email policies to fine-tune them or to expand or reduce their scope.

Table 11-5 describes the setting that you can modify for default spam policies and custom spam policies.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Modifiable in default policies</th>
<th>Modifiable in custom policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply to</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>If the following condition is met</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Perform the following action</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply to the following policy groups</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
To modify spam and unwanted email policies
1. In the Control Center, click **Spam > Policies > Email**.
2. Check the box beside the policy that you want to modify, and then click **Edit**.
3. Make the modifications that you want.
4. Click **Save**.

See “About filtering email spam and unwanted messages” on page 248.
See “Creating the policies that detect spam and unwanted email” on page 256.
See “Enabling and disabling spam and unwanted email policies” on page 259.
See “Copying spam policies” on page 261.
See “Deleting spam policies” on page 262.

Copying spam policies

You may have instances in which you create a complicated spam policy and want to create a similar policy with only a few variances. Symantec Messaging Gateway lets you copy spam policies.

When you copy a spam policy, the new policy must have a unique name. For example, if you have a content filtering policy called XYZ, you cannot have a spam policy or malware policy called XYZ. Spam policies are enabled by default when you create them.

See “About filtering email spam and unwanted messages” on page 248.
See “Creating the policies that detect spam and unwanted email” on page 256.
See “Enabling and disabling spam and unwanted email policies” on page 259.
See “Modifying spam and unwanted email policies” on page 260.
See “Deleting spam policies” on page 262.

To copy spam policies
1. In the Control Center, click **Spam > Policies > Email**.
2. Check the box beside the policy that you want to copy.
3. Click **Copy**.
4. On the **Email Spam Policies** page, type a new name for the policy.
5. Make any other changes you want.
6. Click **Save**.
Deleting spam policies

You can delete the spam policies that you no longer need. However, when you delete a policy, the policy cannot be retrieved. If you are unsure if you want to permanently delete a policy, you can disable it instead.

See “Enabling and disabling spam and unwanted email policies” on page 259.
See “Copying spam policies” on page 261.
See “Modifying spam and unwanted email policies” on page 260.

To delete spam policies
1 In the Control Center, click Spam > Policies > Email.
2 Check the box beside the policy that you want to delete.
3 Click Delete.
4 Click Delete in the confirmation dialog box.

Configuring the threshold for suspected spam identification

When Symantec Messaging Gateway evaluates whether messages are spam, it calculates a spam score from 1 to 100 for each message. This score is based on techniques such as pattern matching and heuristic analysis.

Symantec Messaging Gateway categorizes the spam scores as follows:

<table>
<thead>
<tr>
<th>Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>90 - 100</td>
<td>If an email receives a score in the range of 90 to 100, it is defined as spam. Symantec determines which messages are spam. This determination cannot be adjusted.</td>
</tr>
<tr>
<td>89 - 25 suspected spam threshold</td>
<td>You can define a range of scores from 25 to 89. The messages that score within this range are considered “suspected spam.” Through policies, you can specify different actions for the messages that are identified as suspected spam and messages that are identified as spam.</td>
</tr>
<tr>
<td>75 by default</td>
<td>For example, assume that you configure your suspected spam scoring range to encompass scores from 80 through 89. If an incoming message receives a spam score of 83, Symantec Messaging Gateway considers this message to be suspected spam. It applies the action you specify for suspected spam messages, such as Modify the Message (tagging the subject line).</td>
</tr>
<tr>
<td>Less than the suspected spam threshold</td>
<td>If a message receives a score that is less than the suspected spam threshold, Symantec Messaging Gateway considers it to be non-spam email.</td>
</tr>
</tbody>
</table>
Symantec recommends that you not adjust the spam threshold until you have some exposure into the filtering patterns at your site. Gradually move the threshold setting down 1 point to 5 points per week until the number of false positives is at an acceptable level. One way to test the effects of spam scoring is to configure your spam policy to hold suspected spam in Spam Quarantine. Then set up a designated mailbox to receive false positives complaints and monitor their numbers as you change the spam-score threshold.

**Note:** Symantec does not consider the legitimate messages that receive a suspected spam verdict to be false positives. Messages that are submitted to Symantec Security Response that receive suspected spam verdicts are not reviewed. The reason is that Symantec cannot control how organizations configure the Suspect Spam threshold value. So Symantec does not create filters or modify filters based on suspected spam verdicts. Filters that are created based on the suspected spam threshold values that are set too low can impact spam effectiveness for all Symantec customers.

See “About filtering email spam and unwanted messages” on page 248.

**To configure the threshold for suspected spam identification**

1. In the Control Center, click **Spam > Settings > Scan Settings**.
2. Under **Do you want messages to be flagged as suspected spam**, click **Yes** or **No**.
3. Under **Select a Suspected Spam Threshold between 25 and 89**, click and drag the slider to increase or decrease the lower limit of the range for suspected spam. You can also type a value in the box.
4. Click **Save**.

### Enabling or disabling URI reporting to Symantec

You can help Symantec create better spam filters that block messages based on Uniform Resource Identifiers (URI). When you enable URI reporting, Symantec Messaging Gateway sends a report to Symantec Security Response. The report contains URIs that appear in the messages that Symantec Messaging Gateway scans for spam. Symantec uses this information to develop new URI-based filters. You receive these updated filters through the Conduit.

See “**Scanner Services**” on page 73.

The URI reporting feature has no measurable impact on product performance.
To enable or disable URI reporting to Symantec

1. In the Control Center, click Spam > Settings > Scan Settings.

2. Under Uniform Resource Identifier Reporting, do either of the following tasks:

   - To enable URI reporting: Check Report URIs to Symantec Security Response. This feature is enabled by default for new installations.
   - To disable URI reporting: Uncheck Report URIs to Symantec Security Response. This feature is disabled by default for migrated installations.

3. Click Save.

Enabling or disabling URL reputation filtering

When you enable URL reputation filtering, Symantec Messaging Gateway scans emails for URLs and sends DNS queries to Symantec for reputation lookup. This ability to check URLs against a large, worldwide pool of reputation data increases the effectiveness of your rules against URL-based spam.

To enable or disable URL reputation filtering

1. In the Control Center, click Spam > Settings > Scan Settings.

2. Under Enable URL reputation filtering, do either of the following tasks:

   - To enable URL reputation filtering: Check Enable URL reputation filtering. For new installations, URL reputation filtering is enabled by default. If you upgraded, and you did not disable the Uniform Resource Identifier Reporting feature on the Spam > Scan Settings page in the previous release, URL reputation filtering is enabled by default.

   - To disable URL reputation filtering: Uncheck Enable URL reputation filtering. If you upgraded, and you disabled Uniform Resource Identifier Reporting in the previous release, Enable URL reputation filtering is disabled by default.

3. Click Save.

See "Enabling or disabling URI reporting to Symantec" on page 263.
About submitting messages for customer-specific spam rules

You can obtain custom spam rules specifically for your organization based on the missed spam messages and false positive messages that administrators and end users submit. This feature provides the following benefits:

- It improves Symantec Messaging Gateway's ability to detect spam and helps administrators control false positive incidents.
- It makes it easier to submit missed spam messages or false positive messages to Symantec for analysis and ruleset creation.
- It provides visibility into the submission status and ruleset creation.

See “How rules are created and why messages may not result in custom rules” on page 267.

When you configure this feature, administrators and end users can submit email messages to Symantec as missed spam or false positives. Within minutes, Symantec creates a custom ruleset. The conduit obtains the ruleset, which is then applied to each configured Scanner.

See “Setting up customer-specific spam submissions” on page 268.

If you want to use the customer-specific spam submission feature, you must obtain a submitter ID. The submitter ID ensures that custom rules are available only to those Scanners that a given Control Center manages.

See “Provisioning the submitter ID for customer-specific spam submissions” on page 270.

Symantec Messaging Gateway lets you specify who can submit messages for custom rules. Alternatively, you can specify who cannot submit messages. Restricted users' messages are submitted, but their messages are not considered for custom rules. Restricted users' submissions appear in reports as Blocked.

See “Specifying who can submit messages for customer-specific rules” on page 273.

You can create the spam policies that take the action that you specify on messages Symantec Messaging Gateway detects based on custom rules. For example, you can create a spam policy in which the condition is If a message is customer-specific spam and the action is Create a quarantine incident. This action lets you monitor the messages that violated the custom rules to monitor the rules' effectiveness and to help you troubleshoot issues.

See “Creating the policies that detect spam and unwanted email” on page 256.

You can view the status of your spam submissions on the Status > Submission > Submission Detail page. The Control Center dashboard contains information about the submission service as well as your customer-specific rules. Spam submission data can also be included in reports.

See “Monitoring your spam email submissions” on page 437.

See “Using the Dashboard” on page 603.
See “Report types” on page 582.

There may be an instance in which you want to disable this feature and remove all of the customer spam submission data. Or you might want to delete all of the existing rules and start with new ones. Symantec Messaging Gateway lets you delete all customer spam submission data. This data includes the submitter ID, all related rules, email addresses in the submitters list, reporting information, and so on. Once this data is deleted, however, it cannot be retrieved or restored.

See “Deleting customer-specific spam data” on page 278.

Symantec considers all messages that are submitted as Spam or NOT Spam for global rules regardless of whether the customer-specific spam submission feature is enabled. By default, the customer-spam submissions feature is disabled. When you enable this feature, all of the messages that are submitted are considered for customer-specific rule generation. In addition, false positives can result in the elimination of a rule. If you disable the feature, messages that are submitted are still considered for customer-specific rule generation or rule elimination. Symantec continues to create new rules, but the new rules are not deployed. Customer-specific spam filtering policies are restricted to apply these rules against mail flow. If you enable the feature again, the rules that Symantec delivers change from the previous state when the feature was initially disabled. Customer-specific spam filtering policies are enabled, and these policies apply the latest customer-specific rules. If you delete all submission data, all of the messages that are submitted are considered only for global rule generation or rule elimination.

BodyHash rules are highly accurate because they target the precise fingerprints of an email message. BodyHash rules are particularly effective in combating the short messages and repeated messages that spammers and other attackers use.

BrightSig3 rules adapt to spammer attempts to randomize and obfuscate malicious email. These rules target the messages that have statistical similarity with a sample message. They are particularly effective combating spam attacks where there is significant similarity between messages. These rules employ fuzzy logic algorithms to defeat the spammer who attempts to use obfuscation and variation techniques to evade more traditional signatures.

The combination of BodyHash and BrightSig3 rules provide a highly effective shield against attackers who use short messages or attacks where spammers use various attack obfuscation techniques. These technologies represent two of over 20 different technologies that Symantec uses to secure the global email threat vector. Users of the customer-specific spam rules have the supplemental protection of additional BodyHash and BrightSig3 rules. Together, these rules are targeted specifically to the threats that individual organizations typically see.

To enable, set up, modify, or delete spam submission settings, you must have Full Administration or modify privileges for Manage Spam Submissions.

See "Administrator rights" on page 661.
Symantec goes through the following process to determine whether it should create a ruleset based on the messages that are submitted:

1. Verifies that the customer-specific spam submission feature is enabled.
   See “Enabling or disabling customer-specific spam submissions” on page 269.

2. Verifies that the message originated from a valid source.
   See “Provisioning the submitter ID for customer-specific spam submissions” on page 270.

3. Verifies that the person who submitted the message is either in the **Allowed** list or is not in the **Blocked** list.
   See “Specifying who can submit messages for customer-specific rules” on page 273.

4. Determines if the message itself is valid.
   The following are reasons why Symantec may consider messages to be invalid and not use them for a custom ruleset:
   - Any message that is not RFC5322-compliant is considered invalid.
   
   **Note:** Outlook Messages that are saved as .msg files are not RFC compliant and are not considered valid submissions.

   You can upload or paste any valid RFC5322 message in the Control Center. For more information about RFC5322 requirements, on the Internet, go to the following URL:

   - Sometimes a message is modified in transit and loses its fidelity by the time it reaches Symantec. Messages that lose their fidelity cannot be used for custom rules. Loss of fidelity can occur for a variety of reasons.

5. Determines whether a global rule already exists.
   Symantec may create a custom rule even if a global rule already exists as a safeguard in case a global rule is deleted or disabled.

6. Determines whether the aggressiveness level is met.
   If the aggressiveness level is conservative, multiple users must submit the same message before the message is considered for a rule.
   See “Setting the customer-specific spam submission aggressiveness level” on page 272.
7. If all of the preceding conditions are met, if a spam message is submitted, Symantec creates a new rule. If a false positive message is submitted, no new rule is created, and Symantec might delete the custom rule that resulted in the false positive.

### Setting up customer-specific spam submissions

Table 11-6 describes the process that you must take to set up the customer-specific spam submission feature. You must have Full Administration, Manage Settings, or Manage Spam Submission modify rights to perform these tasks.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable the customer-specific spam submission feature.</td>
<td>You must enable this feature for Symantec to create custom rules. This feature is disabled by default. See “Enabling or disabling customer-specific spam submissions” on page 269.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Either obtain a submitter ID or specify an existing submitter ID.</td>
<td>The submitter ID ensures that the custom ruleset is available only to those Scanners that a given Control Center manages. See “Provisioning the submitter ID for customer-specific spam submissions” on page 270.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Specify the submission aggressiveness level.</td>
<td>You can specify whether you want all messages that are submitted to be considered for a custom rule. Or you can specify whether a message must be submitted multiple times from different users before it should be considered. See “Setting the customer-specific spam submission aggressiveness level” on page 272.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Specify who may or may not submit messages for custom rules.</td>
<td>Symantec Messaging Gateway lets you specify who can submit messages for custom rules. Alternatively, you can specify who cannot submit messages. See “Specifying who can submit messages for customer-specific rules” on page 273.</td>
</tr>
</tbody>
</table>
Table 11-6  Set up the Customer-specific Spam submissions feature (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Enable the policies that use customer-specific rules.</td>
<td>You must enable customer-specific policies for the customer-specific rules to be applied to incoming messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Enabling and disabling spam and unwanted email policies” on page 259.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Default email spam and unwanted email policies” on page 250.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure the options This is Spam and This is NOT Spam to appear in content quarantine incident folders.</td>
<td>If you want to let administrators submit messages for customer-specific rules from content quarantine incident folders, you must configure these options to appear on the Incidents detail page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable these options for each content quarantine incident folder in which you want them to appear.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This option is not available for informational incident folders.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring message submission options to appear in quarantine incident folders” on page 426.</td>
</tr>
</tbody>
</table>

See “About submitting messages for customer-specific spam rules” on page 265.
See “How rules are created and why messages may not result in custom rules” on page 267.

**Enabling or disabling customer-specific spam submissions**

Enable the customer-specific spam submissions feature to obtain customer-specific spam rules based on the email messages that administrators and end users identify as missed spam or false positives. Messages are still submitted to Symantec even when this feature is disabled; however, no custom rules are created.

After you enable the feature, ensure that you complete the remainder of the steps that are required to fully set up this feature.

See “Setting up customer-specific spam submissions” on page 268.

If you no longer want to leverage customer-specific rules in your environment, you can disable this feature. You may also want to delete all of the related rules and data.

See “Deleting customer-specific spam data” on page 278.

You must have Full Administration, Manage Settings, or Manage Spam Submission modify rights to enable or disable this feature.
To enable customer-specific spam submissions

1. In the Control Center, click **Spam > Settings > Submission Settings**.
2. On the **Customer-specific Spam submissions** page, check **Enable Customer-Specific Spam Submission**.
   
   This feature is disabled by default.
3. Read the privacy policy agreement and check **I agree to the terms of this privacy policy**.
   
   The privacy agreement only appears the first time that you enable this feature.
4. Click **Enable customer-specific spam submissions**.
   
   You must provision your submitter ID before you can click **Save**.
   
   See “Provisioning the submitter ID for customer-specific spam submissions” on page 270.

To disable customer-specific spam submissions

1. In the Control Center, click **Spam > Settings > Submission Settings**.
2. On the **Customer-specific Spam submissions** page, uncheck **Enable Customer-Specific Spam Submission**.
3. Click **Save**.

See “About submitting messages for customer-specific spam rules” on page 265.

Provisioning the submitter ID for customer-specific spam submissions

Symantec requires that each Control Center that submits messages for custom rules has a submitter ID. Symantec creates custom rules based on the messages that are submitted from the Control Center with that ID. Those rules are then applied to any Scanners that the Control Center with that submitter ID manages.

You can have a unique submitter ID for each Control Center or you can share submitter IDs among multiple Control Centers. Control Centers that share submitter IDs also share the same custom rules.

Table 11-7 provides guidance as to whether Control Centers should use unique submitter IDs or share submitter IDs.

Table 11-7 Submitter ID use recommendations

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A single Control Center</td>
<td>Obtain and use a unique submitter ID.</td>
</tr>
<tr>
<td>(Typical configuration)</td>
<td>See “To provision a new submitter ID for customer-specific spam submissions” on page 272.</td>
</tr>
</tbody>
</table>
### Table 11-7 Submitter ID use recommendations (continued)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Recommendation</th>
</tr>
</thead>
</table>
| Multiple Control Centers in which you want to share rules (Typical configuration) | For example, assume that you have two Control Centers. You want both Control Centers to use the same custom rules regardless of which Control Center submits the spam messages for ruleset creation.  
Obtain a unique submitter ID for one Control Center. Then apply that submitter ID to the remaining Control Centers.  
See “To specify an existing submitter ID for customer-specific spam submissions” on page 272.  
Symantec creates rules based on all of the messages that are submitted from any of the Control Centers. It applies the same rules across all of the Control Centers. |
| Multiple Control Centers in which you want to have unique rules (Advanced configuration) | For example, assume that you have two Control Centers. One Control Center has a much different configuration and use than the other Control Center. So you want each Control Center to submit its own messages for their own custom rules.  
Obtain unique submitter IDs for each Control Center. Each Control Center receives its own custom ruleset based on the spam messages that are submitted from that Control Center. |

Whether you obtain a new submitter ID or provision an existing submitter ID, the administrator receives an email message from Symantec that confirms the operation and contains the submitter ID number. Symantec recommends that as a best practice you keep this email for reference. You must enable alert notifications for administrators to receive these email notifications.

See “Configuring alerts” on page 688.

When you delete customer-specific spam data, you also delete the submitter ID. The submitter ID is also lost when you perform a factory reset. When you perform a full backup or a configuration backup, you back up the submitter ID. The ID is available upon a successful restore of the backup.

See “Deleting customer-specific spam data” on page 278.

See “Resetting an appliance to its factory defaults” on page 700.

See “Scheduling backups” on page 706.

See “Performing an on-demand backup” on page 709.

See db-backup on page 744.
You must have Full Administration, Manage Spam Submission, or Manage Settings modify rights to perform these tasks. You must also have a valid license to obtain a new submitter ID.

To provision a new submitter ID for customer-specific spam submissions
1 In the Control Center, click Spam > Settings > Submission Settings.
2 On the Customer-specific Spam submissions page, click Register For A New Submitter ID Now.
3 In the Register Submission ID dialog box, click Register.
4 In the confirmation dialog box, click Close.
5 Click Save.

To specify an existing submitter ID for customer-specific spam submissions
1 In the Control Center, click Spam > Settings > Submission Settings.
2 On the Customer-specific Spam submissions page, click Enter an Existing Submitter ID.
3 In the Multiple Control Centers dialog box, type the existing submitter ID.
4 Click Validate Submitter ID.
5 In the Register Submission ID dialog box, click Register.
6 In the confirmation dialog box, click Close.
7 Click Save.
8 Repeat this procedure for each Control Center that you want to share custom rules.

See “Setting up customer-specific spam submissions” on page 268.
See “About submitting messages for customer-specific spam rules” on page 265.

Setting the customer-specific spam submission aggressiveness level

Symantec Messaging Gateway creates custom rules based on the messages that administrators and end users submit. By default, Symantec only creates rules for the messages that administrators submit. Additionally, you can configure Symantec to create rules for the messages that end users submit. The default setting for end user submissions better ensures that you do not obtain any rules that are based on accidental submissions or erroneous ones. However, you can specify that all messages that end users submit are used to create custom rules.

You must have Full Administration, Manage Spam Submission, or Manage Settings modify rights to modify this setting.
To set the customer-specific spam submission aggressiveness level

1 In the Control Center, click Spam > Settings > Submission Settings.

2 On the Customer-specific Spam submissions page, under Submission Aggressiveness, select either of the following options:

   - **Conservative - Only messages with multiple submissions get rules**
     Multiple end users must submit the same message before Symantec considers it for a new rule.

   - **Aggressive - Every submission gets a rule**
     Instances occur in which some of the messages that are submitted do not result in a new ruleset.
     See “How rules are created and why messages may not result in custom rules” on page 267.

The default setting is Conservative.

3 Click Save.

See “Setting up customer-specific spam submissions” on page 268.

See “About submitting messages for customer-specific spam rules” on page 265.

### Specifying who can submit messages for customer-specific rules

Symantec Messaging Gateway lets you specify who can submit messages for custom rules. Alternatively, you can specify who cannot submit messages for custom rules. Restricted users’ messages are submitted, but their messages are not considered for ruleset creation. Restricted users’ submissions appear in reports as Blocked.

You can add users to the Submitter Email Address list in either of the following ways:

   - **Type them manually.**
     Separate multiple email addresses with a comma.

   - **Import a user list.**
     Imported users lists must be in a text file (.txt) with a new line character that separates the entries.

---

**Warning:** When you import email addresses, all existing email addresses are replaced with those in the imported file — not appended.

---

**Note:** Wildcards are unsupported, and you must enter a valid email address.
You can have a maximum of 1,000 email addresses in the **Submitter Email Address** list. Symantec Messaging Gateway validates your entries to ensure that you use a valid email address and that you do not have duplicate entries.

You can also remove, export, and view all of the email addresses in the list as needed.

See “Working with the Submitters Email Address list” on page 275.

The **Submitter Email Address** list is backed up when you perform a full backup or a configuration backup. Symantec recommends that as a best practice you schedule regular backups to ensure that you can retrieve the most recent **Submitter Email Address** list. You can also periodically export your **Submitter Email Address** list as you make changes to keep as backups.

See “Scheduling backups” on page 706.

Administrators who have Full Administration Rights, Manage Spam Submissions modify rights, or Manage Settings modify rights can submit messages for rules. Administrators must also have one of these sets of rights to modify these settings.

Submissions from administrators with Limited Administration Rights that include Manage Spam Submissions modify rights and Manage Quarantine/Quarantine Incidents view or modify rights can contribute to customer-specific spam rule creation.

As long as a submitter ID is provisioned, enabling and disabling the customer-specific spam submission feature has no impact on submissions and customer-specific rule generation. Customer-specific spam rule creation happens even if the customer-specific spam submission feature is disabled, provided a submitter ID is provisioned.

However, the created rules are downloaded only when the customer-specific spam submission feature is enabled.

### To specify who can submit messages for customer-specific rules

1. In the Control Center, click **Spam > Settings > Submission Settings**.

2. On the **Customer-specific Spam submissions** page, click the **Submitters List** tab.

3. Select the option that you want to use to either allow users in the **Submitter Email Address** to submit messages for spam rules or to block them.

   - The default setting is **Allowed - Only administrators and email addresses on this list can submit messages**.

4. Perform any of the following tasks:

   - To manually add an email address: In the **Manually add email addresses** field, type the email address and then click **Add**.
To import email addresses  Do all of the following tasks:
  ■ Click **Browse**.
  ■ Locate and select the file that you want to import.
  ■ Click **Import**.

**Warning:** When you import email addresses, all existing email addresses are replaced with those in the imported file — not appended.

5  Click **Save**.

See “Setting up customer-specific spam submissions” on page 268.

See “About submitting messages for customer-specific spam rules” on page 265.

Working with the Submitters Email Address list

The following describes what you can do with the **Submitters Email Address** list on the Spam > Submission Settings > Submitters List tab.

Delete one or more entries  You can delete one or more entries at a time. You can also delete all of the entries in the list at once. Once you delete an entry, it cannot be retrieved.

See “To delete one or more entries at a time” on page 275.

Export entries  You may want to export email addresses from the **Submitters Email Address** on one Control Center and import it on another Control Center. This feature eliminates the need to retype all of the email address entries.

See “To export email addresses from the Submitters Email Address list” on page 276.

View entries  You can have up to 1,000 email addresses in the **Submitters Email Address**. Symantec Messaging Gateway provides icons that help you navigate more easily through this list.

See “To navigate the Submitters Email Address list” on page 276.

You must have Full Administration rights, Manage Spam Submissions, or Manage Settings modify rights to modify these settings.

To delete one or more entries at a time

1  In the Control Center, click **Spam > Settings > Submission Settings**.

2  On the **Customer-specific Spam submissions** page, click the **Submitters List** tab.

3  Do one of the following tasks:
To delete one or more email addresses

Do any of the following tasks:
- Check the box beside the email address or addresses that you want to delete and click Delete.
- To select all of the addresses in the Submitters Email Address list that are in view, check the box beside Submitters Email Address, and then click Delete.

To delete all of the email addresses in the Submitter Email Address list.

Click Delete All, and in the confirmation dialog box, click OK.

4 Click Save.

To export email addresses from the Submitters Email Address list

1 Click Export.
2 Follow your Web browser's dialog box instructions to specify where you want to save the export file.

To navigate the Submitters Email Address list

- Do any of the following tasks:

To specify how many addresses that you want to view per page

Click the Entries per page drop-down arrow and select how many entries you want to view per page.

You can view 10, 25, 50, or 100 entries per page. The default value is 25.

To specify which page of the email addresses that you want to view

Click the Display drop-down arrow and select the page number.

To advance to another page

Select any of the following navigation icons:
- 
  Navigates you to first page of submitter email addresses.
- 
  Navigates you to the previous page of submitter email addresses.
- 
  Navigates you to the next page of submitter email addresses.
- 
  Navigates you to last page of submitter email addresses.
Submitting messages through the Control Center for customer-specific rules

In addition to submitting messages for rules from Spam Quarantine and content filtering incident folders, administrators can also submit messages directly from the Control Center.

See “Submitting messages from Spam Quarantine for customer-specific rules” on page 302.

Messages that you submit through the Control Center must contain both the headers and bodies and must be valid RFC5322 messages.

Note: Outlook Messages that are saved as .msg files are not RFC compliant and are not considered valid submissions.

See “How rules are created and why messages may not result in custom rules” on page 267.

Submissions from administrators receive higher consideration for the creation of rules than those submitted by end users. However, all of the messages that administrators submit are considered equally whether they are submitted from Control Center, Spam Quarantine, or content incident folders.

If the customer-specific spam submission feature is disabled, Symantec still analyzes the messages that you submit through Spam Quarantine. It considers those messages for global spam rules or global false positive rules. However, no custom rules are created.

Only administrators with Full Administration rights or rights to modify Manage Spam Submissions can submit messages through the Control Center.

Note: Submitted messages cannot exceed 5 MB in size. An error message is displayed if you attempt to submit a message that exceeds this limit.

To submit messages through the Control Center for customer-specific rules

1  In the Control Center, click Spam > Submissions > Submit Messages.

2  Under Message Type, check the appropriate box to indicate if the message is a missed spam or was misidentified as spam.
3 Perform one of the following tasks:

To upload an existing message: Click **Upload a Message**, then click **Browse**. Locate and select the message that you want to upload, and click **Open**.

To paste the contents of a message: Copy the contents of the message from the source, and in the **Paste a Message** field, paste the contents of the message.

4 Click **Submit Message**.

See “Setting up customer-specific spam submissions” on page 268.

See “About submitting messages for customer-specific spam rules” on page 265.

### Deleting customer-specific spam data

Symantec Messaging Gateway retains data about the messages that administrators and end users submit for ruleset creation along with the accompanying rules. You may want to delete customer-specific spam data to remove previous rules and start with entirely new rules. If you no longer want to leverage customer-specific rules in your environment, you can permanently delete all of customer-specific spam data. Afterwards, you should also disable the feature.

See “Enabling or disabling customer-specific spam submissions” on page 269.

When you delete customer-specific spam data, you delete all of the following:

- All of the data that was submitted for the creation of rules
- All of the rules that Symantec created based on that data
- Data that is used in spam submission reports
- The submitter ID
- All of the email addresses in the **Submitter Email Address** list

**Warning:** Once you delete the customer-specific spam data, it cannot be retrieved.

In addition, the aggressiveness option returns to the default setting, and Symantec Messaging Gateway no longer takes the actions that you specify for the spam policy condition if a message is customer-specific spam.

You must have Full Administration rights, Manage Spam Submission, or Manage Settings modify rights to perform this task.
To delete customer-specific spam data

1 In the Control Center, click **Spam > Settings > Submission Settings**.

2 On the **Configuration** tab under **Customer-specific Spam Data Retention**, click **Delete All Customer-Specific Spam Data**.

3 In the confirmation dialog box, read the warning and then click **Delete All Customer-Specific Spam Data**.

See “About submitting messages for customer-specific spam rules” on page 265.
Quarantining spam

This chapter includes the following topics:

- About quarantining spam
- Before you use Spam Quarantine
- Quarantining spam sent to unresolved email addresses
- About navigating Spam Quarantine
- Configuring Spam Quarantine settings
- Viewing messages in the Spam Quarantine
- Working with messages in the Spam Quarantine
- Configuring Spam Quarantine notifications
- Troubleshooting Spam Quarantine
- Spam Quarantine best practices for large deployments

About quarantining spam

You can route spam, suspected spam, or both to Spam Quarantine so that administrators and users can access the messages to check for false positives, if necessary. Spam Quarantine can help you fine-tune your spam settings and spam policies. Too many false positives can indicate that spam settings are too stringent and should be modified. Use of Spam Quarantine is optional.

Spam Quarantine stores spam messages and provides Web-based user and administrator access to those messages. Users access Spam Quarantine with their LDAP user names and authentication. If a message is marked as spam or suspected spam, but is legitimate, users can release the messages to their inboxes. Users can notify you of false positives so that you
can continue to adjust your spam settings and spam policies accordingly. You can also set up summary notifications to be delivered to users inboxes.

You can configure thresholds to control the space that is allocated for Spam Quarantine.

See “Before you use Spam Quarantine” on page 281.

See “Configuring end user quarantine” on page 284.

See “How Spam Quarantine differs for administrators and users” on page 291.

**Before you use Spam Quarantine**

If you intend to permit users to access Spam Quarantine, before you use Spam Quarantine, ensure that you have done all of the following:

Create and enable the spam policies that quarantine spam and suspected spam. One or more policy groups must have an associated filter policy that quarantines messages. For example, you can create a spam policy that quarantines inbound suspected spam messages for the Default group.

See “Creating the policies that detect spam and unwanted email” on page 256.

Configure your LDAP server and ensure it works properly. Control Center access to your LDAP server using authentication must work properly for users to logon to Spam Quarantine to check their quarantined messages. You also need LDAP authentication to expand LDAP email aliases and for the Delete Unresolved Email setting.

See “About using the authentication function with your data source” on page 510.

Ensure that you have an SMTP mail server available. Spam Quarantine does not require a separate SMTP mail server to send notifications and resend misidentified messages. However, an SMTP mail server must be available to receive notifications and the misidentified messages that Spam Quarantine sends. The SMTP server that you choose should be downstream from the Scanner, as notifications and misidentified messages do not require filtering.

See “Configuring SMTP advanced settings” on page 54.

See “About quarantining spam” on page 280.

See “Enabling users to bypass Control Center login credentials” on page 681.
Quarantining spam sent to unresolved email addresses

If LDAP is configured for address resolution, the messages that are sent to non-existent email addresses (based on LDAP lookup) are deleted by default. If you uncheck **Delete messages sent to unresolved email addresses** on the **Spam > Settings > Quarantine Settings** page of the Control Center, these messages are stored in the Spam Quarantine postmaster mailbox.

See “Creating an address resolution data source” on page 508.

**Delete messages sent to unresolved email addresses** is unchecked and is grayed out by default if LDAP is not configured for address resolution.

---

**Note:** If an LDAP server connection fails or LDAP settings have not been configured correctly, then quarantined messages addressed to unresolved email addresses are consigned to the Scanner's deferred queue and the SMTP connection between Control Center and Scanner is closed, whether the Delete unresolved email check box is checked or unchecked. Once the Scanner's deferred retry or timeout limit is reached, the message bounces back to the sender.

---

**To quarantine spam sent to unresolved email addresses**

1. In the Control Center, click **Spam > Settings > Quarantine Settings**.
2. In the General Settings section, uncheck **Delete messages sent to unresolved email addresses**.
3. Click **Save**.

---

**About navigating Spam Quarantine**

The following icons show how to navigate through the Spam Quarantine message list page:

- Go to beginning of messages.
- Navigate to last page of messages or 50 pages ahead if there are more than 50 pages.
- Go to previous page of messages.
- Go to next page of messages.
- Choose up to 500 entries per page before or after the current page of messages.

The following icons show how to navigate through the Spam Quarantine message details page:
When you navigate to a different page of messages, the status of the check boxes in the original page is not preserved. For example, assume that you select three messages on the first page of messages and then move to the next page. When you return to the first page, all of the message check boxes are cleared.

### Configuring Spam Quarantine settings

Spam Quarantine is a repository for the messages that Symantec Messaging Gateway identifies as spam.

**Table 12-1** describes the ways that you can configure Spam Quarantine settings. You can perform any of these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure Spam Quarantine for individual policy groups | If you have an LDAP directory server configured, you can configure Spam Quarantine so that only the members of a specific policy group (or groups) can access it. To configure access for administrators only, you enable quarantine globally and then enable end-user quarantine for Administrative policy groups only.  
  
  See “Configuring end user quarantine” on page 284. |
| Enable language encoding when needed.          | In most cases, the Auto-detect setting properly determines the language encoding for a message in Spam Quarantine. However, the Control Center may not be able to determine the proper language encoding for some messages. If the message is garbled, select the language encoding most likely to match the encoding that is used in the message.  
  
  See “Choosing the language encoding for spam messages” on page 286. |
| Set quarantine thresholds to minimize the amount of space that it uses on your appliance. | Spam Quarantine thresholds let you control the maximum size for Spam Quarantine. You can use the Expunger to enforce Spam Quarantine threshold settings.  
  
  See “Modifying Spam Quarantine thresholds” on page 287.  
  
  See “Spam Quarantine threshold considerations” on page 288. |
Configure Spam Quarantine settings (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the quarantine message retention period.</td>
<td>You can change the amount of time spam messages are kept before being deleted. You may want to shorten the retention period if quarantined messages use too much disk space.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying how long spam messages are retained in quarantine” on page 288.</td>
</tr>
<tr>
<td>Configure the Expunger.</td>
<td>You can specify the time that the Quarantine Expunger begins the purge process and how frequently the purge process occurs. The Expunger lets you keep Spam Quarantine at a manageable size.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying when and how often Spam Quarantine is expunged” on page 289.</td>
</tr>
<tr>
<td>Configure false positive notifications.</td>
<td>You can also automatically send a copy to a local administrator, Symantec, or both. These messages should be sent to an administrator who monitors misidentified messages at your organization to determine the effectiveness of Symantec Messaging Gateway.</td>
</tr>
<tr>
<td></td>
<td>See “Specifying who to notify of false positive messages” on page 290.</td>
</tr>
</tbody>
</table>

Configuring end user quarantine

End user quarantine allows individual users to access their messages in Spam Quarantine and to receive quarantine notifications. If you have an LDAP directory server configured, you can configure Spam Quarantine so that only the members of a specific policy group (or groups) can access it.

You must complete these basic steps to enable end user quarantine.

- **Step 1: Choose settings on your directory data source**
- **Step 2: Enable end user quarantine globally**
- **Step 3: Assign end user quarantine rights to your groups**

**Step 1: Choose settings on your directory data source**

End user quarantine uses LDAP information to authenticate end users who attempt to log on and view their quarantined messages. The quarantine also uses LDAP information for address resolution, and to assign quarantined messages to individual user quarantines.

The following instructions assume that you already added and configured a directory data source.

See “Configuring Directory Data integration” on page 495.
To enable the LDAP settings that end user quarantine requires

1. In the Control Center, select Administration > Settings > Directory Integration.

2. On the Directory Integration page, select your directory data source and click Edit.

3. On the Authentication tab, select Enable Authentication. From the drop-down menu, select either Control Center authentication only or Control Center and SMTP authentication.

4. On the Address Resolution tab, select Enable Address Resolution. From the drop-down menu, select either Email Scanning only or Both Control Center Authorization and Email Scanning.

5. Click Save.

Step 2: Enable end user quarantine globally

After you set up your LDAP settings, you can enable end user quarantine. This process acts like a global on and off switch for end user quarantine.

To configure end user quarantine globally

1. Select Spam > Settings > Quarantine Settings.

2. In the End User Settings panel, select Enable quarantine.

Note: Enable Quarantine is disabled if you did not connect a directory data source.

3. If necessary, edit the Spam Quarantine login URL.

Note: The default Spam Quarantine login URL is https://<host_FQDN>:41443/brightmail. The default URL changes automatically if you change the fully-qualified domain name (FQDN) of the host. However, if you customize the Spam Quarantine login URL, and then later change the FQDN of the host, you must change the customized URL manually.

4. Click Save.

Step 3: Assign end user quarantine rights to your groups

After you enable end user quarantine globally, you must enable the feature for individual policy groups (including administrator policy groups) before end users can access their quarantined messages.
To add end user quarantine access to a policy group

1. In the Control Center, select Administration > Users > Policy Groups.
2. On the Policy Groups page, select a group and click Edit, or click Add to add a new policy group.
3. On the End Users tab, select Enable end user quarantine.
4. Optional: Select Enable end user settings for this policy group. Then enable Create personal Good and Bad Senders lists and Specify language settings, if you want to give these permissions to group members.

   Leave these settings disabled if you want to prevent end users from modifying their own settings.
5. Click Save.

Configuring End User Quarantine for Administrators only

To allow only Administrators to log in and use end user quarantine, perform Step 1: Choose settings on your directory data source and Step 2: Enable end user quarantine globally. Then in Step 3: Assign end user quarantine rights to your groups, assign end user quarantine only to your Administrative policy groups.

See “Viewing spam and suspected spam messages in quarantine” on page 292.
See “How Spam Quarantine differs for administrators and users” on page 291.

Choosing the language encoding for spam messages

In most cases, the Auto-detect setting properly determines the language encoding for a message in Spam Quarantine. However, the Control Center may not be able to determine the proper language encoding for some messages. If the message is garbled, select the language encoding most likely to match the encoding that is used in the message.

Only the administrators that have Full Administration rights or Manage Quarantine modify rights can choose language encoding for messages in quarantine.

See “Viewing spam and suspected spam messages in quarantine” on page 292.
See “About navigating Spam Quarantine” on page 282.
See “Sorting spam and suspected messages in quarantine by date” on page 296.

To choose the language encoding for spam messages

1. In the Control Center, click Spam > Quarantine > Email Spam.
2. Click on the subject line of the message that you want to view.
3. On the message details page, select the language encoding in the drop-down list.
Modifying Spam Quarantine thresholds

Spam Quarantine thresholds let you control the maximum size for Spam Quarantine. You can use the Expunger to enforce Spam Quarantine threshold settings. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.

Note: Since the Expunger maintains the maximum size of Spam Quarantine, the quarantine can exceed maximum thresholds until the Expunger runs at the next scheduled interval.

See “Specifying how long spam messages are retained in quarantine” on page 288.
See “Specifying when and how often Spam Quarantine is expunged” on page 289.
Before you modify the Spam Quarantine thresholds, ensure that you understand the implications and considerations.
See “Spam Quarantine threshold considerations” on page 288.
Table 12-2 describes the Spam Quarantine thresholds that you can configure.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of quarantine</td>
<td>Maximum amount of the disk space that is used for quarantined messages for all users.</td>
</tr>
<tr>
<td></td>
<td>The maximum Quarantine size reflects the actual size on disk of each message file in the message store. The actual disk usage may be slightly higher due to other unaccounted disk usage, such as database tables and indexes.</td>
</tr>
<tr>
<td>Maximum size per user</td>
<td>Maximum amount of the disk space that is used for quarantine messages per user.</td>
</tr>
<tr>
<td>Maximum number of messages</td>
<td>Maximum number of messages for all users (a single message sent to multiple recipients counts as one message).</td>
</tr>
<tr>
<td>Maximum number of messages per user</td>
<td>Maximum number of quarantine messages per user.</td>
</tr>
</tbody>
</table>

To modify Spam Quarantine thresholds

1. In the Control Center, click Spam > Settings > Quarantine Settings.

2. Under Thresholds, for each type of threshold that you want to configure, check the box and enter the size threshold or message threshold.

   You can configure multiple thresholds.

3. Click Save.
### Spam Quarantine threshold considerations

*Table 12-3* describes the issues that you should consider before you modify Spam Quarantine thresholds.

<table>
<thead>
<tr>
<th>Issues to consider</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thresholds are enforced when the Expunger runs.</td>
<td>Thresholds may be exceeded temporarily until the next Expunger run.</td>
</tr>
<tr>
<td>The Expunger deletes older messages to enforce thresholds.</td>
<td></td>
</tr>
<tr>
<td>Per-user thresholds are the most processing-intensive to enforce.</td>
<td>Per-user thresholds are not recommended for larger deployments, such as those with over 5000 users. When the Expunger runs, per-user thresholds are checked and enforced before the other thresholds.</td>
</tr>
<tr>
<td><strong>The Maximum size of Quarantine and Maximum number of messages</strong> thresholds provide the most precise control over disk usage and message count.</td>
<td>Spam Quarantine searches run faster with fewer messages.</td>
</tr>
<tr>
<td>Shortening the Spam Quarantine message retention period can also limit the size of Spam Quarantine.</td>
<td>A more efficient method to manage Spam Quarantine size is to conserve disk space rather than using Spam Quarantine thresholds.</td>
</tr>
<tr>
<td>No alert or notification occurs if the specific Spam Quarantine thresholds are exceeded.</td>
<td>You can configure an alert for <strong>Usage of the maximum configured disk space for Spam Quarantine exceeds.</strong></td>
</tr>
<tr>
<td></td>
<td>See “Configuring alerts” on page 688.</td>
</tr>
</tbody>
</table>

See “Modifying Spam Quarantine thresholds” on page 287.

### Specifying how long spam messages are retained in quarantine

You can change the amount of time spam messages are kept before being deleted. You may want to shorten the retention period if quarantined messages use too much disk space. However, a shorter retention period increases the chance that users may have messages deleted before they have a chance to check them. The default retention period is 7 days. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.
By default, the Expunger runs at 1 A.M. every day to delete messages older than the retention period. For example, if you have a retention period of 7 days, when the Expunger runs it deletes all messages older than 7 days. The Expunger also deletes messages as necessary to enforce the Spam Quarantine message and size thresholds.

See “Specifying when and how often Spam Quarantine is expunged” on page 289.

See “Modifying Spam Quarantine thresholds” on page 287.

You can also delete messages manually from Spam Quarantine.

See “Deleting spam messages in quarantine” on page 300.

To specify how long spam messages are retained in quarantine

1. In the Control Center, click Spam > Settings > Quarantine Settings.
2. Under Spam Quarantine Expunger, in the Days to store in Quarantine before deleting field type the number of days.
3. Click Save on the Quarantine Settings page.

Specifying when and how often Spam Quarantine is expunged

You can specify the time that the Quarantine Expunger begins the purge process and how frequently the purge process occurs. The Expunger lets you keep Spam Quarantine at a manageable size. Messages that are purged cannot be retrieved. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.

See “Specifying how long spam messages are retained in quarantine” on page 288.

See “Modifying Spam Quarantine thresholds” on page 287.

See “Deleting spam messages in quarantine” on page 300.

You can check the status of your scheduled task from the Status > Scheduled Tasks page.

See “About scheduled tasks” on page 648.

To specify when and how often Spam Quarantine is purged

1. In the Control Center, click Spam > Settings > Quarantine Settings.
2. Click the Quarantine Expunger frequency drop-down list to specify how often the Expunger runs.
3. In the Quarantine Expunger start time drop-down lists, specify the time that you want the Expunger to start.
4. Click Save.
Specifying who to notify of false positive messages

If users or administrators find false positive messages in Spam Quarantine, they can click Release. Clicking Release redelivers the selected messages to the user’s normal inbox. You can also automatically send a copy to a local administrator, Symantec, or both. These messages should be sent to an administrator who monitors misidentified messages at your organization to determine the effectiveness of Symantec Messaging Gateway.

Symantec Security Response analyzes message submissions to determine if filters need to be changed. However, Symantec Security Response does not send confirmation of the misidentified message submission to the administrator or the user submitting the message. Nor is there any guarantee that filters are altered based on those submissions.

**Note:** Symantec does not consider the legitimate messages that receive a suspected spam verdict to be false positives. Messages that are submitted to Symantec Security Response that receive suspected spam verdicts are not reviewed. The reason is that Symantec cannot control how organizations configure the Suspect Spam threshold value. So Symantec does not create filters or modify filters based on suspected spam verdicts. Filters that are created based on suspected spam threshold values that are set too low can impact spam effectiveness for all Symantec customers.

Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.

See “Releasing false-positive messages from quarantine” on page 299.

To specify who to notify of false positive messages

1. In the Control Center, click **Spam > Settings > Quarantine Settings**.
2. To report misidentified messages to Symantec, under **Misidentified Messages**, click **Symantec Security Response**.
   
   This option is selected by default.
3. To send copies of misidentified messages to a local administrator, under **Misidentified Messages**, click **Administrator** and type the appropriate email address.
   
   Type the full email address including the domain name, such as admin@symantecexample.com. The administrator email address must not be an alias, or a copy of the misidentified message is not delivered to the administrator email address.
4. Click **Save**.
Viewing messages in the Spam Quarantine

Table 12-4 describes the tasks that you can perform to view messages in Spam Quarantine. You can perform these tasks as needed in any order.

Table 12-4  View messages in Spam Quarantine

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how the users' Spam Quarantine differs from the Administrator's Spam Quarantine.</td>
<td>This topic provides a table that describes the differences. See “How Spam Quarantine differs for administrators and users” on page 291.</td>
</tr>
<tr>
<td>View messages in Spam Quarantine.</td>
<td>View messages that are in Spam Quarantine to determine if they are spam or false positives. See “Viewing spam and suspected spam messages in quarantine” on page 292.</td>
</tr>
<tr>
<td>View messages that are sent to the postmaster mailbox.</td>
<td>If Spam Quarantine cannot determine the proper recipient for a message that it receives and it is configured not to delete such messages, it delivers the message to a postmaster mailbox. The postmaster mailbox is accessible from the administrator’s Spam Quarantine. Your network may also have a postmaster mailbox that you access with a mail client that is separate from Spam Quarantine postmaster mailbox. Spam messages may also be delivered to the Spam Quarantine postmaster mailbox if there is a problem with the LDAP configuration. See “Viewing spam and suspected spam messages sent to the postmaster mailbox” on page 294.</td>
</tr>
</tbody>
</table>

How Spam Quarantine differs for administrators and users

Table 12-5 describes the differences between the Spam Quarantine for administrators and users.
Table 12-5  Spam Quarantine differences between administrators and users

<table>
<thead>
<tr>
<th>Page</th>
<th>Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message List page</td>
<td>The Message List page has the following differences:</td>
</tr>
<tr>
<td></td>
<td>■ Users can only view and delete their own quarantined messages.</td>
</tr>
<tr>
<td></td>
<td>Quarantine administrators can view and delete all users' quarantined</td>
</tr>
<tr>
<td></td>
<td>messages, either one by one, deleting all messages, or deleting the</td>
</tr>
<tr>
<td></td>
<td>results of a search.</td>
</tr>
<tr>
<td></td>
<td>■ When users click Release, the message is delivered to their own</td>
</tr>
<tr>
<td></td>
<td>inbox. When a Quarantine administrator clicks Release, the message</td>
</tr>
<tr>
<td></td>
<td>is delivered to the inbox of each of the intended recipients.</td>
</tr>
<tr>
<td></td>
<td>■ The administrator Message List page includes a &quot;To&quot; column that</td>
</tr>
<tr>
<td></td>
<td>contains the intended recipient of each message. Users can only see</td>
</tr>
<tr>
<td></td>
<td>their own messages, so the &quot;To&quot; column is unnecessary.</td>
</tr>
<tr>
<td></td>
<td>■ Users only have access to Spam Quarantine, not the rest of the Control</td>
</tr>
<tr>
<td></td>
<td>Center.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users access Spam Quarantine by logging into the Control</td>
</tr>
<tr>
<td></td>
<td>Center. They use the user name and password that your LDAP server</td>
</tr>
<tr>
<td></td>
<td>requires.</td>
</tr>
<tr>
<td>Message Details page</td>
<td>Users can only view and delete their own quarantined messages.</td>
</tr>
<tr>
<td></td>
<td>Quarantine administrators can view and delete messages for all users.</td>
</tr>
<tr>
<td>Search filters</td>
<td>Quarantine administrators can search for recipients.</td>
</tr>
<tr>
<td></td>
<td>In the search results, users can only delete their own quarantined</td>
</tr>
<tr>
<td></td>
<td>messages. Quarantine administrators can delete all users' quarantined</td>
</tr>
<tr>
<td></td>
<td>messages.</td>
</tr>
</tbody>
</table>

See “Configuring end user quarantine” on page 284.

See “Viewing spam and suspected spam messages in quarantine” on page 292.

See “About navigating Spam Quarantine” on page 282.

Viewing spam and suspected spam messages in quarantine

View messages that are in Spam Quarantine to determine if they are spam or false positives. Administrators with Full Administration rights or Manage Quarantine view rights can view spam messages in quarantine. However, these administrators cannot release messages or delete messages in Spam Quarantine. Administrators with Full Administration rights or Manage Quarantine modify rights can view, delete, and release spam messages from Spam Quarantine.

When you click on the subject line of a message on the Message List page, the contents appear on the Message Details page. When you finish viewing the details of that spam message, you can return to the Message List page.
Note the following Message Details page behavior:

- **Graphics appear as gray rectangles**
  The original graphics in messages are replaced with graphics of gray rectangles. The purpose is to suppresses offensive images and prevents spammers from verifying your email address. If you release the message by clicking Release, the original graphics are viewable by the intended recipient. Users cannot view the original graphics within Spam Quarantine.

- **Attachments cannot be viewed**
  The names of attachments are listed at the bottom of the message, but the actual attachments cannot be viewed from within Spam Quarantine. However, if you redeliver a message by clicking Release, the message and attachments are accessible from the inbox of the intended recipient.

---

**Note:** The "To" column in the Message List page indicates the intended recipient of each message as listed in the message envelope. Use caution when considering this information, since spammers oftentimes forge this header.

See “About navigating Spam Quarantine” on page 282.

See “Configuring end user quarantine” on page 284.

See “How Spam Quarantine differs for administrators and users” on page 291.

**To view spam and suspected spam messages in quarantine**

- Do one of the following:
  - If you are not on the Spam Message Quarantine page
    In the Control Center, click **Spam > Quarantine > Email Spam**.
  - If you are on the Spam Message Quarantine page and want to see newly arrived messages
    Click **Show Filters** if the Display All option is not visible, and click **Display All**.

**To view the contents of a spam and suspected spam message**

- Click on the subject line of the message.
  The Message Details page appears.

**To return to the Message List page from the Message Details page**

- To return to the message list, click **Back to Messages**.
Viewing spam and suspected spam messages sent to the postmaster mailbox

Your network may also have a postmaster mailbox that you access with a mail client that is separate from Spam Quarantine postmaster mailbox. Spam messages may also be delivered to the Spam Quarantine postmaster mailbox if there is a problem with the LDAP configuration. If you run version 8.0.3 or earlier and Spam Quarantine cannot determine the proper recipient for a message that it receives and it is configured not to delete such messages, it delivers the message to a postmaster mailbox accessible from Spam Quarantine.

No notification messages are sent to the postmaster mailbox.

You must have Full Administration Rights or Manage Quarantine view or modify rights to view the messages in the postmaster mailbox.

To view spam and suspected spam messages sent to the postmaster mailbox

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click **Show Filters**.
3. In the To box, type **postmaster**.
4. Specify additional filters as needed.
5. Click **Display Filtered**.

You should note the following behavior based on the version of Symantec Messaging Gateway that you use:

8.0.3 or earlier
What appears are the spam messages addressed to unresolved recipients only.

9.0 or later
What appears are the spam messages addressed to both resolved (valid) and unresolved (invalid) recipients.

See “Viewing spam and suspected spam messages in quarantine” on page 292.
See “About navigating Spam Quarantine” on page 282.
See “Configuring end user quarantine” on page 284.
See “How Spam Quarantine differs for administrators and users” on page 291.

Working with messages in the Spam Quarantine

**Table 12-6** describes the tasks that you can perform with messages in Spam Quarantine. You can perform these tasks as needed in any order.
Table 12-6 Work with messages in Spam Quarantine

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Customize the message list page.                   | You can specify the number of entries that appear at a time on the message list page.  
See “Specifying the number of entries to appear on the Spam Quarantine Message list page” on page 295. |
| Sort messages in Spam Quarantine.                  | You can sort messages in Spam Quarantine to make it easier to categorize the messages or locate a specific message. By default, messages appear in date descending order. The newest messages are listed at the top of the page.  
See “Sorting spam and suspected messages in quarantine by date” on page 296. |
| Search for a message in Spam Quarantine.           | You can search for messages in Spam Quarantine. The ability to search messages lets you more easily find a specific message that you want to view or delete.  
See “Searching quarantined spam messages” on page 296.  
See “Spam message search criteria and tips” on page 297. |
| View spam message headers.                         | Viewing headers of spam messages may provide clues about the origin of a message. Keep in mind, however, that spammers usually forge some of the message headers.  
See “Viewing spam message headers” on page 298. |
| Release false-positive messages from Spam Quarantine.| Occasionally you may see messages in Spam Quarantine that are not spam. You can redeliver these messages to the intended recipient.  
See “Releasing false-positive messages from quarantine” on page 299. |
| Delete spam messages from Spam Quarantine to free up disk space. | When you delete a message in the administrator's Spam Quarantine, you also delete it from the user's Spam Quarantine. When you or a user deletes a message, it is no longer accessible.  
See "Deleting spam messages in quarantine" on page 300. |

Specifying the number of entries to appear on the Spam Quarantine Message list page

You can specify the number of entries that appear at a time on the message list page. You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Spam Quarantine.

See “Viewing spam and suspected spam messages in quarantine” on page 292.
See “About navigating Spam Quarantine” on page 282.
To specify the number of entries to appear on the Spam Quarantine message list page

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. On the **Entries per page** drop-down list, click a number.

### Sorting spam and suspected messages in quarantine by date

You can sort messages in Spam Quarantine to make it easier to categorize the messages or locate a specific message. By default, messages appear in date descending order. The newest messages are listed at the top of the page.

A triangle appears in the date column that indicates ascending or descending sort order. Click on the column heading to toggle between ascending and descending sort order. By default, messages are listed in date descending order, meaning that the newest messages are listed at the top of the page.

You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Spam Quarantine.

See “Viewing spam and suspected spam messages in quarantine” on page 292.
See “About navigating Spam Quarantine” on page 282.
See “Searching quarantined spam messages” on page 296.
See “Viewing spam message headers” on page 298.

To sort spam and suspected messages in quarantine by date

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click the **Date** column heading to sort messages by date.

### Searching quarantined spam messages

You can search for messages in Spam Quarantine. The ability to search messages lets you more easily find a specific message that you want to view or delete. You must have Full Administration rights or Manage Quarantine view or modify rights to view messages in Spam Quarantine.

See “Viewing spam and suspected spam messages in quarantine” on page 292.
See “About navigating Spam Quarantine” on page 282.
See “Sorting spam and suspected messages in quarantine by date” on page 296.

To search quarantined spam messages

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. On the message list page, click **Show Filters**.
3. Do any of the following to perform a search:

- **To search message envelope "To" recipient**: Type a name or address in the To box to search the message envelope RCPT TO: header.
  
  You can search for a display name, the user name portion of an email address, or any part of a display name or email user name. If you type a full email address in the To box, Symantec Messaging Gateway searches only for the user name portion of user_name@example.com. The search is limited to the envelope To:, which may contain different information than the header To: that appears on the message details page. You can search for the domain portion of an email address by typing the domain.

- **To search "From" headers**: Type a name or address in the From box to search the From: header in all messages for a particular sender.
  
  You can search for a display name, email address, or any part of a display name or email address. The search is limited to the visible message From: header, which is usually forged in spam messages. The visible message From: header may contain different information than the message envelope.

- **To search the Message ID header**: Type in the Message ID box to search the message ID in all messages.
  
  You can view the message ID on the message details page in Spam Quarantine by clicking Display Full Headers. In addition, most email clients can display the full message header, which includes the message ID. For example, in Outlook 2000, double click on a message to show it in a window by itself, click View and then click Options.

  See “Viewing spam message headers” on page 298.

- **To search subject headers**: Type in the Subject box to search the Subject: header for all messages about a specific topic.

- **To search a time range**: Select a time range from the Time Range drop-down list to display all of the messages that were received during that time range.

4. Click **Display Filtered**.

**Spam message search criteria and tips**

The search function is optimized for searching a large number of messages but can lead to unexpected search results.

Consider the following tips and information to help you conduct searches in Spam Quarantine:
<table>
<thead>
<tr>
<th>Tokens</th>
<th>Tokens are matched with substring semantics. Searching for a subject with the search target <code>&lt;in&gt;</code> will match &quot;Lowest rate in 45 years,&quot; &quot;RE: re: Sublime Bulletin (verification),&quot; &quot;Up to 85% off Ink Cartridges + no shipping!,&quot; and &quot;Re-finance at todays super low rate.&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple word searches</td>
<td>If any word in a multiple word search is found in a message, that message is considered a match. For example, searching for red carpet match &quot;red carpet,&quot; &quot;red wine,&quot; and &quot;flying carpet.&quot;</td>
</tr>
<tr>
<td>Case sensitivity</td>
<td>All text searches are case-insensitive. For example, assume you type emerson in the From box. Messages with a From header that contains emerson, Emerson, and eMERSOn all appear in the search results.</td>
</tr>
<tr>
<td>Exact phrases</td>
<td>To search for an exact phrase, enclose the phrase in &quot;&quot; (double quotes).</td>
</tr>
<tr>
<td>Wildcards</td>
<td>You can use * (asterisk) to perform wildcard searches. It also functions as a logical AND character.</td>
</tr>
<tr>
<td>Single characters</td>
<td>Even a single character is treated as a substring target.</td>
</tr>
<tr>
<td>Special characters</td>
<td>You can search on special characters such as &amp; (ampersand), ! (exclamation point), $ (dollar sign), and # (pound sign).</td>
</tr>
<tr>
<td>Multiple characteristics</td>
<td>If you search for multiple characteristics, only the messages that match the combination of characteristics are listed in the search results. For example, assume you type LPQTech in the From box and Inkjet in the Subject box. Only the messages that contain LPQTech in the From: header and Inkjet in the Subject: header appear in the search results.</td>
</tr>
<tr>
<td>Forged header information</td>
<td>Spammers usually &quot;spoof&quot; or forge some of the visible messages headers such as From and To and the invisible envelope information. Sometimes they forge header information using the actual email addresses or domains of innocent people or companies.</td>
</tr>
<tr>
<td>Time to perform a search</td>
<td>The amount of time it takes to perform the search depends on how many search boxes you use and the number of messages in the mailbox. Searching in the administrator mailbox takes longer than searching in a user's mailbox.</td>
</tr>
</tbody>
</table>

See “Searching quarantined spam messages” on page 296.

See “Viewing spam and suspected spam messages in quarantine” on page 292.

See “About navigating Spam Quarantine” on page 282.

**Viewing spam message headers**

Viewing headers of spam messages may provide clues about the origin of a message. Keep in mind, however, that spammers usually forge some of the message headers. You must have
Full Administration rights or Manage Quarantine view or modify rights to view messages in Spam Quarantine.

See “Viewing spam and suspected spam messages in quarantine” on page 292.

See “About navigating Spam Quarantine” on page 282.

See “Releasing false-positive messages from quarantine” on page 299.

See “Sorting spam and suspected messages in quarantine by date” on page 296.

To view full spam messages headers

1. In the Control Center, click Spam > Quarantine > Email Spam.
2. Click on the subject line of the message that you want to view.
3. To display all headers available to Spam Quarantine, click Display Full Headers.

To view brief spam messages headers

1. In the Control Center, click Spam > Quarantine > Email Spam.
2. Click on the subject line of the message that you want to view.
3. To display only the From:, To:, Subject:, and Date: headers, click Display Brief Headers.

Releasing false-positive messages from quarantine

Occasionally you may see messages in Spam Quarantine that are not spam. You can redeliver these messages to the intended recipient. When you redeliver a message, it also removes the message from Spam Quarantine. Depending on how you configure Spam Quarantine, a copy of the message can also be sent to an administrator, Symantec, or both. This configuration lets the email administrator or Symantec monitor the effectiveness of the spam settings and filters.

See “Specifying who to notify of false positive messages” on page 290.

Only the administrators that have Full Administration rights or Manage Quarantine modify rights can release messages from quarantine.

See “Viewing spam and suspected spam messages in quarantine” on page 292.

See “About navigating Spam Quarantine” on page 282.

See “Modifying Spam Quarantine thresholds” on page 287.

See “Specifying when and how often Spam Quarantine is expunged” on page 289.

See “Deleting spam messages in quarantine” on page 300.
To release false-positive messages from the quarantine message list page

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click on the check box to the left of a misidentified message and then click **Release** to redeliver the message to the intended recipient.

To release false-positive messages from the quarantine message details page

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click on the subject line of the spam message that you want to review and possibly redeliver.
3. On the message details page, click **Release**.

Deleting spam messages in quarantine

Delete spam messages from Spam Quarantine to free up disk space. When you delete a message in the administrator's Spam Quarantine, you also delete it from the user's Spam Quarantine. For example, assume that you delete spam messages in the administrator's Spam Quarantine. The users to whom those messages are addressed cannot view the messages in their Spam Quarantine.

Users remove messages from the Quarantine when they release them or delete them. When you or a user deletes a message, it is no longer accessible.

See “Releasing false-positive messages from quarantine” on page 299.

You can delete messages from the message list page or from the message details page. Only the administrators that have Full Administration rights or Manage Quarantine modify rights can delete messages in quarantine. Users do not need special permissions to delete messages from their own quarantine.

You can also use an Expunger to automatically delete messages from Spam Quarantine. The Expunger frees you from having to manually delete messages from Spam Quarantine to free up space. The Expunger purges messages based on the schedule that you specify.

See “Specifying when and how often Spam Quarantine is expunged” on page 289.

To delete individual messages from the message list page

1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click on the check box to the left of each message that you want to delete.
3. Click **Delete**.
To delete all messages from the message list page
1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click **Delete All** to delete all the messages in Spam Quarantine, including those on other pages.
   
   This task deletes all of the spam messages in the users' Spam quarantine. Users see no mail in their quarantine.

To delete spam messages from the message details page
1. In the Control Center, click **Spam > Quarantine > Email Spam**.
2. Click on the subject line of the message that you want to view.
3. To delete the message that you are currently viewing, click **Delete**.

Specifying when to notify users of spam messages in their quarantine

You can change the frequency at which notifications are automatically sent to users. The default frequency is every day. To disable notification messages, change the notification frequency to **NEVER**.

If you modify the notification frequency, keep in mind the potential impact of frequent notifications. If you have a large number of users, notifications that occur more than once daily could become overwhelming for your users. And frequent notifications can impact network performance. Symantec recommends that for larger deployments, notifications should not occur more frequently than daily.

To specify when to notify users of spam messages in their quarantine
1. In the Control Center, click **Spam > Settings > Quarantine Settings**.
2. Under **Notification Settings**, in the **Maximum summary entries per notification** box, specify how many items to include in the summary notification message.
   
   The default setting is 100.
3. Click the **Notification frequency** drop-down list and select how often you want notifications sent.
4. Click the **Notification start time** drop-down lists and select hour and minute that you want notifications sent.
5. Click **Save**.
Submitting messages from Spam Quarantine for customer-specific rules

You can submit the messages that are in Spam Quarantine to Symantec for customer-specific rule creation. You must have Full Administration rights or Manage Spam Submission modify rights to submit messages. You must also have Manage Spam Quarantine modify or view rights to access Spam Quarantine.

If the customer-specific spam submission feature is disabled, Symantec still analyzes the messages that you submit through Spam Quarantine. It considers those messages for global spam rules or global false positive rules. However, no custom rules are created.

See “Specifying who can submit messages for customer-specific rules” on page 273.

To submit messages from Spam Quarantine for customer-specific rules

1. In the Control Center, click Spam > Quarantine > Email Spam.
2. On the Spam Message Quarantine page, check the box beside the message that you want to submit for custom rules.
   - You can select multiple messages to submit.
3. Select one of the following options:
   - This is Spam: The message is spam and should be identified as such.
   - This is NOT Spam: The message is a legitimate message and should not be identified as spam.
4. In the confirmation dialog box, click Submit as Spam or Submit as NOT Spam, as appropriate.
   - If the submission is successful, the submission type appears in the Submission Status column for the message that you selected.

See “About submitting messages for customer-specific spam rules” on page 265.

Configuring Spam Quarantine notifications

Table 12-7 describes the options that you can configure to create Spam Quarantine notifications. You can perform these tasks as needed in any order.
Table 12-7 Configure Spam Quarantine notifications

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about spam notification messages.</td>
<td>By default, a notification process runs at 4:00 A.M. every day. The process determines if users have new spam messages in Spam Quarantine since the last time the notification process ran. If so, it sends a message to users who have new spam to remind them to check their Spam Quarantine. The process can also send notification digests to users on distribution lists. See “About configuring the user and distribution list notification digests” on page 303. See “About how spam is handled when addressed to distribution lists” on page 304.</td>
</tr>
<tr>
<td>Specify how frequently users are notified of messages in their Spam Quarantines.</td>
<td>You can change the frequency at which notifications are automatically sent to users. The default frequency is every day. See “Specifying when to notify users of spam messages in their quarantine” on page 301.</td>
</tr>
<tr>
<td>Modify the spam notification template.</td>
<td>The notification digest templates determine the appearance of notification messages that are sent to users as well as the message subjects and send from addresses. See “Modifying the spam notification message digest templates” on page 305. See “Spam notification message variables” on page 307.</td>
</tr>
<tr>
<td>Specify the notification digest format.</td>
<td>The notification digest template determines the MIME encoding of the notification message that is sent to users. It also determines as whether View and Release links appear in the message. See “Selecting the notification digest format” on page 308.</td>
</tr>
</tbody>
</table>

About configuring the user and distribution list notification digests

By default, a notification process runs at 4 A.M. every day. The process determines if users have new spam messages in Spam Quarantine since the last time the notification process ran. If so, Symantec Messaging Gateway sends a message to users who have new spam to remind them to check their spam messages in Spam Quarantine. The process can also send notification digests to users on distribution lists.

Note: Notification messages and notification settings are disabled if LDAP is not configured or if administrator-only access is enabled.
By default, the notification templates for standard quarantined messages and quarantined
distribution list messages are different. Separate templates let you customize the notification
templates for each type of quarantined message.

See “About how spam is handled when addressed to distribution lists” on page 304.
See “Specifying when to notify users of spam messages in their quarantine” on page 301.

### About how spam is handled when addressed to distribution lists

If Spam Quarantine is enabled, a spam message that is sent to an alias with a one-to-one
correspondence to a user's email address is delivered to the user's normal quarantine mailbox.
For example, if "tom" is an alias for "tomevans," the quarantined messages that are sent to
"tom" or to "tomevans" all arrive in the Spam Quarantine account for "tomevans."

**Note:** An "alias" on UNIX or "distribution list" on Windows is an email address that translates
to one or more other email addresses. In this text, distribution list is used to mean an email
address that translates to two or more email addresses.

Symantec Messaging Gateway does not deliver a spam message that is sent to a distribution
list in the intended recipients' Spam Quarantine mailboxes. Instead, the message is delivered
in a special Spam Quarantine mailbox for that distribution list. However, you can configure
Spam Quarantine to send notification digests about the messages in a distribution list mailbox
to the recipients of that distribution list. You configure this option by selecting the Notify
distribution lists check box on the Quarantine Settings page.

**Note:** When there is one or more address resolution DDS source, and the **Expand Distribution
Lists** option is enabled, distribution lists expand to a recipient list of individual users before
the message is sent to quarantine. In this case, individual users receive notifications from the
user template, not the distribution list template.

If the Include View link box is selected, a list of the quarantined distribution list messages is
included in the notification digest. Each message has a View link that users can click to view
that message in Spam Quarantine. If the Include Release link box is selected, each message
that is listed in the digest has a Release link. Users can click this link to release that distribution
list message without accessing Spam Quarantine. If any one recipient clicks the **Release link**
for a message in the quarantined distribution list mailbox, the message is delivered to the
normal inboxes of all distribution list recipients. The View link and Release link do not appear
if the notification format is text only.

**Table 12-8** provides an example of how messages are routed to members of distribution lists.
### Table 12-8 Distribution list notification and delivery examples

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>A distribution list that is called mktng contains Ruth, Fareed, and Darren</td>
<td>Spam sent to mktng and configured to be quarantined is not delivered to the Spam Quarantine inboxes for Ruth, Fareed, and Darren.</td>
</tr>
<tr>
<td>The Notify distribution lists check box on the Quarantine Settings page is selected</td>
<td>Ruth, Fareed, and Darren receive email notifications about the quarantined mktng messages.</td>
</tr>
<tr>
<td>The Include View link box is selected on the Quarantine Settings page</td>
<td>Ruth, Fareed, and Darren can view the quarantined mktng messages by clicking on the View link in the notification digests.</td>
</tr>
<tr>
<td>The Include Release link box is also selected</td>
<td>Ruth, Fareed, and Darren can redeliver any quarantined mktng message by clicking on the Release option in the notification digest.</td>
</tr>
<tr>
<td>Ruth clicks the Release option for a quarantined mktng message</td>
<td>The message is delivered to the normal inboxes of Ruth, Fareed, and Darren.</td>
</tr>
</tbody>
</table>

#### Modifying the spam notification message digest templates

The notification digest templates determine the appearance of notification messages that are sent to users as well as the message subjects and send from addresses. The default notification templates are similar to the text that is listed as follows. The distribution list notification template lacks the information about how to logon. In your browser, the text does not wrap, so you need to scroll horizontally to view some of the lines. This layout prevents unusual line breaks or extra lines if you choose to send notifications in HTML format.

Spam Quarantine Summary for %USER_NAME%

There are %NEW_MESSAGE_COUNT% new messages in your Spam Quarantine since you received your last Spam Quarantine Summary. These messages will automatically be deleted after %QUARANTINE_DAYS% days.

To review the complete text of these messages, go to %QUARANTINE_URL% and log in.

```
================================= NEW QUARANTINE MESSAGES =========================
%NEW_QUARANTINE_MESSAGES%
================================= NEW QUARANTINE MESSAGES =========================
```
You can reposition each variable in the template or remove it. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.

See “About configuring the user and distribution list notification digests” on page 303.

See “About how spam is handled when addressed to distribution lists” on page 304.

See “Specifying when to notify users of spam messages in their quarantine” on page 301.

See “Enabling notification digests for distribution lists” on page 307.

See “Selecting the notification digest format” on page 308.

To modify the spam notification message digest templates

1. In the Control Center, click **Spam > Settings > Quarantine Settings**.

2. Under **Notification Settings**, click **Edit** next to Notification template.

3. In the **Encoding** drop-down list, select the character encoding for the notification message.


4. In the **Send from** box, type the email address from which the notification digests appear to be sent.

   Since users can reply to the email address that you provide, type an address where you can monitor users’ questions about the notification digests. Specify the full email address, which includes the domain name, such as: admin@symantecexample.com

5. In the **Subject** box, type the text that should appear in the **Subject:** header of notification digests, such as "Your Suspected Spam Summary."

   Use of message variables in the subject box is unsupported.

   The Send from settings and Subject settings are the same for both the user notification template and distribution list notification template.

6. Edit the user notification and distribution list notification as necessary.

   See Table 12-9 on page 307.

   Refrain from using manually insert line breaks if you plan to send notifications in HTML.
7 Click one of the following icons:

- **Save** Saves and applies your changes.
- **Default** Erase the current information and replace it with default settings.
- **Cancel** Discard your changes to the notification template and close the template editing window.

8 Click **Save** on the Quarantine Settings page.

### Spam notification message variables

**Table 12-9** lists the spam notification message variables.

See "Modifying the spam notification message digest templates" on page 305.

**Table 12-9** Notification Message Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%USER_NAME%</td>
<td>User name of user receiving the notification message.</td>
</tr>
<tr>
<td>%NEW_MESSAGE_COUNT%</td>
<td>Number of new messages in the user's Spam Quarantine since the last notification message was sent.</td>
</tr>
<tr>
<td>%QUARANTINE_DAYS%</td>
<td>Number of days messages in Spam Quarantine are kept. After that period, messages are purged.</td>
</tr>
<tr>
<td>%QUARANTINE_URL%</td>
<td>URL that the user clicks on to display the Spam Quarantine logon page.</td>
</tr>
<tr>
<td>%NEW_QUARANTINE_MESSAGES%</td>
<td>List of messages in the user's Spam Quarantine since the last notification was sent. For each message, the contents of the <strong>From:</strong>, <strong>Subject:</strong> , and <strong>Date:</strong> headers are printed. View and Release links are displayed for each message if they are enabled and you've chosen a Multipart or HTML notification format.</td>
</tr>
</tbody>
</table>

### Enabling notification digests for distribution lists

You can configure Spam Quarantine to send notification digests about the messages in a distribution list mailbox to the recipients in a distribution list. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.
To enable notification digests for distribution lists

1. In the Control Center, click **Spam > Settings > Quarantine Settings**.
2. Under **Notification Settings**, check **Notify distribution lists**.
3. Click **Save**.

### Selecting the notification digest format

The notification digest template determines the MIME encoding of the notification message that is sent to users. It also determines as whether **View** and **Release** links appear in the message.

Details about the View and Release links are as follows:

**View**

When a user clicks on the **View** link in a notification digest message, the selected message appears in Spam Quarantine in the default browser. This check box is only available if you choose Multipart (HTML and text) or HTML only notification format. If you remove the **%NEW_QUARANTINE_MESSAGES%** variable from the notification digest template, the new message summary (including the View links) are not available.

**Release**

The **Release** link is for misidentified messages. When a user clicks on the **Release** link in a notification digest message, the adjacent message is released from Spam Quarantine and sent to the user’s normal inbox. This check box is only available if you choose Multipart (HTML and text) or HTML only notification format. If you remove the **%NEW_QUARANTINE_MESSAGES%** variable from the notification digest template, the new message summary (which includes the Release links) are not be available.
Only the administrators that have Full Administration rights or Manage Settings modify rights can modify quarantine settings.

To select the notification digest format

1  In the Control Center, click Spam > Settings > Quarantine Settings.
2  Under Notification Settings, click one of the following items in the Notification format drop-down list:
   - Multipart (HTML and Text) Send notification messages in MIME multipart format. Users see either the HTML version or the text version depending on the type of email client they use and the email client settings. The View and Release links do not appear next to each message in the text version of the summary message.
   - HTML only Send notification messages in MIME type text/html only.
   - Text only Send notification messages in MIME type text/plain only. If you choose Text only, the View and Release links do not appear next to each message in the summary message.
3  Check the Include View link box to include a View link next to each message in the notification digest message summary.
4  Check the Include Release link box to include a Release link next to each message in the notification digest message summary.
5  Click Save.

Troubleshooting Spam Quarantine

Table 12-10 lists some problems that may occur with Spam Quarantine.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error in log file &quot;error.mail.transport.connect=Cannot release mail, cannot connect to any available MTA service&quot;</td>
<td>This error can occur if the IP address of the Control Center is not specified for inbound and outbound mail settings on the Administration &gt; Hosts &gt; Configuration &gt; Add/Edit &gt; SMTP tab. See &quot;About Scanner email settings&quot; on page 43.</td>
</tr>
</tbody>
</table>
Table 12-10  Spam Quarantine issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users do not see distribution list messages in their Spam Quarantine</td>
<td>A Scanner does not deliver a spam message that is sent to a distribution list in the intended recipients' Quarantine mailboxes. Instead, the message is delivered to a special Spam Quarantine mailbox for that distribution list. See &quot;About how spam is handled when addressed to distribution lists&quot; on page 304.</td>
</tr>
<tr>
<td>Undeliverable quarantined messages go to Spam Quarantine postmaster</td>
<td>If Spam Quarantine cannot determine the proper recipient for a message that is received by Symantec Messaging Gateway, it delivers the message to a postmaster mailbox accessible from Spam Quarantine. Alternatively you can specify Delete message sent to unresolved email addresses in the Quarantine Settings page. Your network may also have a postmaster mailbox you access using a mail client that is separate from the Spam Quarantine postmaster mailbox. If the LDAP server fails or has been improperly configured, however, spam messages to non-LDAP-recognized addresses are held in the Scanner's deferred queue (up to the delivery retry and timeout limits) and not in the Spam Quarantine postmaster mailbox. <strong>Note:</strong> No notification messages are sent to the postmaster mailbox. See &quot;Viewing spam and suspected spam messages sent to the postmaster mailbox&quot; on page 294.</td>
</tr>
<tr>
<td>Users receive notification messages, but cannot access messages</td>
<td>If users who cannot access their messages are in a different Active Directory domain from users who can access their messages, configure Directory Integration in the Control Center to use a Global Catalog. Alternatively, ensure that you have a directory data source for each active directory domain. To configure access to an Active Directory Global Catalog, specify the port for the Global Catalog, usually 3268, on the Administration &gt; Settings &gt; LDAP/Edit page. See &quot;Creating a data source&quot; on page 496.</td>
</tr>
<tr>
<td>Duplicate messages appear in Spam Quarantine</td>
<td>You may notice multiple copies of the same message when logged into Spam Quarantine as an administrator. When you read one of the messages, all of them are marked as read. This behavior is intentional. If a message is addressed to multiple users at your company, Spam Quarantine stores one copy of the message in its database, although the status (read, deleted) of each user's message is stored per-user. Because the administrator views all users' messages, the administrator sees every user's copy of the message. If the administrator clicks on Release, a copy of the message is redelivered to each affected user mailbox.</td>
</tr>
</tbody>
</table>
Table 12-10  Spam Quarantine issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of messages in Spam Quarantine</td>
<td>The total Quarantine size is calculated by summing the block size (size on disk) of each message file in the message store. Be aware that the actual disk usage will be higher due to other unaccounted disk usage such as database tables and indexes. See &quot;Modifying Spam Quarantine thresholds&quot; on page 287.</td>
</tr>
<tr>
<td>Message &quot;Cannot release the message&quot; appears</td>
<td>This message may occur if there is a problem with message traffic on your inbound or outbound mail flow. It occurs when the message cannot be delivered to any of the configured non-local relays (default) or cannot be delivered to the SMTP host configured on the Administration &gt; Control Center &gt; SMTP page. It may also occur if a Scanner is not installed on the same appliance as the Control Center and the SMTP host setting has not been set for a host that has an MTA. This causes delivery problems for releasing messages from Spam Quarantine. See &quot;Configuring Control Center SMTP settings for alerts and reports&quot; on page 694.</td>
</tr>
<tr>
<td>Quarantining spam messages and suspected spam messages takes longer than expected</td>
<td>This issue might be the result of slow access to the LDAP server. Try the following tasks:  ■ If the LDAP server is configured for Active Directory as a global catalog server, ensure that you use port 3268 instead of 389. See &quot;Creating a data source&quot; on page 496.  ■ Check the base DN query. A more specific DN query returns faster than a more general one. For example, &quot;ou=quarantine-test,dc=brightmail,dc=com&quot; is a more specific query than &quot;dc=brightmail,dc=com.&quot;</td>
</tr>
<tr>
<td>When an administrator clicks on one spam message, multiple messages are marked as 'read'</td>
<td>This situation occurs when the same message is sent to different recipients. When an administrator accesses one instance of the message, then all instances of that message (regardless of the recipient) are marked as read. The reason this situation occurs is because the administrator read flag is associated to the message itself. This situation does not occur for end-user Spam Quarantine. That read flag is associated to each message/recipient combination.</td>
</tr>
</tbody>
</table>

Spam Quarantine best practices for large deployments

If your organization has a deployment of 1,000 users or more, consider the following best practices to enhance Spam Quarantine effectiveness:
- The Quarantine should not run on the same box as a Scanner. See “Configuring mail flow direction” on page 45.

- The Quarantine Expunger should be set to run no more than once per day. You should also schedule the Expunger to run in off-peak hours. See “Specifying when and how often Spam Quarantine is expunged” on page 289.

- For deployments of 5,000 users or more, also consider the following suggestions:
  - Disable per user limits (for example, maximum number of messages per user). See “Modifying Spam Quarantine thresholds” on page 287.
  - The Spam Quarantine digest notification can take long time to run, so schedule it to run less frequently. The notification process impacts availability of the Control Center to accept messages from the delivery queue. See “Specifying when to notify users of spam messages in their quarantine” on page 301.

See “Troubleshooting Spam Quarantine” on page 309.
Participating in the Symantec Probe Network

This chapter includes the following topics:

- About the Symantec Probe Network
- About probe accounts
- About creating probe accounts
- Setting up probe accounts

About the Symantec Probe Network

The Probe Network is crucial to Symantec's ongoing effort to fight spam. As spammers find new ways to bypass filters, the Symantec Probe Network helps Symantec stay one step ahead by monitoring spamming methods through the use of probe accounts.

The Probe Network is effective for the following reasons:

- Drives early detection of spam attacks
- Probe accounts are the first step in the real-time detection and analysis of spam. The structure of the Probe Network essentially provides Symantec Security Response with a stream of real-time spam being disseminated over the Internet. This virtual net of numerous accounts spread all over the Internet makes it easy for Symantec to verify that a given message was sent using bulk methods.
Spreadsheets and accurate filters

A key marketplace differentiator for Symantec Messaging Gateway is the near perfect accuracy rate of its spam filtering technology. The antispam capability is largely due to core filters that are based on actual spam. The probe network also provides key data that is used to develop Symantec's more predictive filters, such as heuristics. What makes all this possible is the volume, quality, and timeliness of data that flows in real time from the probe network to Symantec Security Response.

Spams are constantly changing their tactics and dissemination methods to evade filtering software. Symantec's Customer Response and AntiSpam Systems teams mine the data from the probe network to advance Symantec's AntiSpam technology. Examples include staying abreast of the latest spam trends, evaluating the spam-catching differences between product versions and monitoring detection rates in different languages.

See “About probe accounts” on page 314.
See “Enabling probe participation” on page 317.

About probe accounts

Symantec Messaging Gateway provides options to convert your invalid recipient email addresses into probe accounts which can be used in the Symantec Probe Network. Probe accounts help Symantec track spam and learn from it. The intelligence that Symantec gains from probe accounts enables continuous improvement of the rules that govern spam filters. Better filters mean fewer spam intrusions on your network.

See “About the Symantec Probe Network” on page 313.

The tools for creating probe accounts are available from the Spam > Settings > Probe Accounts page.

See “Enabling probe participation” on page 317.
See “Setting up probe accounts” on page 316.
See “Creating probe accounts from invalid recipient email addresses” on page 318.
See “Creating probe accounts manually” on page 319.
See “Enabling probe accounts” on page 320.
See “Disabling a probe account” on page 320.
See “Deleting a probe account” on page 321.

You can track the effectiveness of your probe accounts by viewing the reports that track the top probe accounts.

See “Report types” on page 582.
About creating probe accounts

When you create probe accounts, you may wonder which email addresses make the best probe accounts. You have the option to select as many invalid recipient email addresses as you want. You can also create any number of invalid or unused email addresses for use in the probe network.

However, when you upload email addresses for use as probe accounts, it is important to consider the following guidelines:

**Invalid Recipients**

You should select the invalid recipient addresses that receive the most amount of email or those that you believe receive high percentages of spam email. You should not select the invalid recipients addresses that are former employees' addresses or common misspellings of public addresses (for example, support@symantecexample.com). These addresses likely receive mostly valid emails.

To see your top invalid recipients, use the Reporting feature to view the Invalid Recipient report.

See “Select data to track for reports” on page 576.

See “Report types” on page 582.

See “Creating probe accounts from invalid recipient email addresses” on page 318.

**Manual entering of addresses**

Use this method to add other addresses that you believe receive only spam content. These may include the addresses that you have seeded on the Internet that you expect to receive only spam messages. Seeding is the deliberate publishing of email addresses on the Internet in order for spammers to harvest and target these addresses.

See “Creating probe accounts manually” on page 319.

The Control Center can store a maximum of 5000 probe accounts.

In some cases you may employ **Alias** addresses. Probe accounts always override aliases. Remember the following when you create probe accounts and alias addresses:

- If you create a probe account for an address that already has an alias, then the probe feature overwrites that alias.

- You cannot create an alias for an address that is already a probe account.

In some cases you may employ **Masqueraded** addresses. Masqueraded accounts override probe accounts.

For example, you use the reports to find that jay@symantecexample.com is a top invalid recipient. You make jay@symantecexample.com a probe address.
Sometime later, the company changes its name from symantecexample to symantecdomain, and all of the email addresses change to @symantecdomain.com.

You use address masquerading to masquerade domain ‘symantecexample’ to ‘symantecdomain’ so the mails that are sent to someone@symantecexample.com gets sent to the new someone@symantecdomain.com address. In doing so, you invalidate the jay@symantecexample.com probe account. All mail to that address is seen as going to jay@symantecdomain.com, which is not a probe address.

See “Adding or editing address masquerades” on page 93.

### Setting up probe accounts

The following table describes the steps to create probe accounts and add them to the Symantec Probe Network.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Enable probe participation. | Probe participation must be enabled to activate probe accounts.  
See “Enabling probe participation” on page 317. |
| Step 2 | Verify domain and enable recipient validation. | The probe account domain must match one of your local domains. Verify that there is a matching domain and that it is enabled for recipient validation. If there is no matching domain you can add one using the add domain task.  
See “Adding or editing domains” on page 82. |
| Step 3 | Specify invalid recipient handling. | You must configure invalid recipient handling on the domain that you want to use for a probe account.  
You can choose any of the three handling options: accept, reject, or drop; but you must choose one.  
See “Setting up invalid recipient handling” on page 99. |
### Table 13-1  
Creating probe accounts *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 4 | Add a data source (optional) and enable recipient validation. **Note:** Skip this step if you plan to create probe accounts using the manual method only. | A directory data source that is enabled for recipient validation is necessary only if you want to upload invalid recipient email addresses captured in the directory data service filters.  
See "Enabling or editing the recipient validation function" on page 556.  
If you do not already have a directory data source, you need to create one and enable recipient validation.  
See "Adding a data source" on page 496. |
| Step 5 | Enable reporting.                                                                                                                      | To track top invalid recipients and top probe accounts, enable the Invalid Recipients report.  
See "Select data to track for reports" on page 576.  
See "Create, save, email, and print a report" on page 578. |
| Step 6 | Create probe accounts.                                                                                                                | The probe feature provides two methods for creating probe accounts. You can manually create probe accounts by entering email addresses or uploading them from a file. Or, you can create probe accounts using the invalid recipient method.  
See "Creating probe accounts manually" on page 319.  
See "Creating probe accounts from invalid recipient email addresses" on page 318. |
| Step 7 | Enable or disable one or more probe accounts.                                                                                          | Although probe accounts are enabled by default, you may want to temporarily disable a probe account and enable it again later.  
See "Enabling probe accounts" on page 320.  
See "Disabling a probe account" on page 320. |

### Enabling probe participation

You must first enable probe participation before you can add email addresses for use in the Symantec Probe Network. When you enable probe participation, a Probe account policy group is automatically created and added to your list of policy groups. If you already have a policy group named Probe account, when you enable probe participation, your existing Probe account policy group is renamed to Backup of Probe account <n>. (When Symantec Messaging Gateway must rename more than one existing Probe account policy group, it uses sequential numbers <n> in the group name.)
When you disable probe participation, the Probe account policy group is automatically deleted. To enable probe participation:

1. In the Control Center, click **Spam > Settings > Probe Accounts**.

2. Under **Probe Email Address**, check **Enable probe participation**.

Once you have enabled probe participation, you can select individual probe accounts to enable or disable.

See “Enabling probe accounts” on page 320.

### Creating probe accounts from invalid recipient email addresses

You must first make a few minor system configurations before completing this task. For assistance on determining which accounts make good probe accounts, refer to the probe account create guidelines.

See “About creating probe accounts” on page 315.

Once you create a probe account, you can track its effectiveness on the **Reports** tab by running a **Top Probe Accounts** report.

See “Create, save, email, and print a report” on page 578.

---

**Note:** To view **Top Probe Account** reports, you must first enable the **Invalid Recipient** setting on the **Administration > Settings > Reports** page.

See “Select data to track for reports” on page 576.

---

**Note:** The Control Center can store a maximum of 5000 probe accounts.

To create probe accounts from invalid recipient email addresses:

1. In the Control Center, click **Spam > Settings > Probe Accounts**.

2. Check **Enable probe participation** if it is not already checked.

3. Under **Add Probe Addresses**, click **Invalid Recipients**.

   Ensure that you have configured the system to track invalid recipient data, otherwise an error message appears.

See “Select data to track for reports” on page 576.
4 Click the Time range drop-down list, select a time range, and click View.

In the Invalid Recipient address table, use the drop-down menus to specify the number of Entries (email addresses) you want to see per page and which ones to Display. You can select 1-10 to see the top 10 invalid recipient accounts, or you can select 10-20 to see the next 10 accounts. Use the arrows to quickly navigate through your results.

5 Check the box beside each address that you want to make into a probe account and click Add Selected to Probes. Click Add All to Probes to add all the addresses to the Symantec Probe Network.

This returns you to the initial probe accounts page where you see the selected addresses in the Email Address table with a status of Enabled.

Creating probe accounts manually

You must make a few minor system configurations before completing this task.

See “Setting up probe accounts” on page 316.

For assistance on determining which accounts make good probe accounts, refer to the probe account create guidelines.

See “About creating probe accounts” on page 315.

Once you create a probe account you can track its effectiveness on the Reports tab by running a Top Probe Accounts report.

See “Create, save, email, and print a report” on page 578.

---

Note: To view the Top Probe Account reports, you must first enable the Invalid Recipient setting on the Administration > Settings > Reports page.

See “Select data to track for reports” on page 576.

---

To manually create a probe account

1 In the Control Center, click Spam > Settings > Probe Accounts.

2 Check the Enable probe participation box if it is not already checked.
3 In the **Manually add probe email addresses** field, type one or more email addresses, separated by commas, to add to the probe network.

You can alternatively add email addresses from an external text file by clicking **Browse**. When the **Browse** window opens, select the file that contains the email addresses that you want to add as probe accounts and click **Upload**.

Email addresses uploaded from a text file must be formatted correctly. Apply one email address per line; no commas.

The Control Center can store a maximum of 5000 probe accounts.

4 Click **Add**.

When the screen refreshes, the probe accounts appear in the **EmailAddress** table with an Enabled status.

### Enabling probe accounts

By default a probe account is enabled when you create it. In some cases you may want to temporarily disable a probe account. When you are ready to reactivate the account, you use the **Enable** option.

Before enabling individual probe accounts, make sure the **Enable Probe Participation** check box is checked at the top of the **Spam > Settings > Probe Accounts** page. If it is unchecked, it overrides individually enabled probe accounts, making them inactive.

See “**Enabling probe participation**” on page 317.

#### To enable probe accounts

1 In the Control Center, click **Spam > Settings > Probe Accounts**.

2 From the probe accounts list, check each probe account that you want to enable.

   You can also check the topmost box to select all the accounts that are listed on the page.

   You can sort the list of probe accounts by clicking the column title **EmailAddress**, which sorts the accounts alphabetically. To sort the probe addresses by status, click the table title **Enabled**.

3 Click **Enable**.

   The selected probe accounts are now active in the Symantec Probe Network.

### Disabling a probe account

When you want to temporarily disable a probe account in the Symantec Probe Network, you use the **Disable** option.
To permanently remove a probe account, use the **Delete** option.

See “Deleting a probe account” on page 321.

To disable a probe account

1. In the Control Center, click **Spam > Settings > Probe Accounts**.
2. In the **Email Addresses** table, check each probe account that you want to disable, or click the topmost box to select all accounts listed on the page.
3. Click **Disable**.

   The disabled account is no longer active, but it remains in the Symantec Probe Network where it can be reactivated.

Deleting a probe account

When you no longer want a probe account in the Symantec Probe Network, you can permanently remove it using the **Delete** option.

Note: If you want to save the probe account but temporarily remove it from the Symantec Probe Network, use the **Disable** option.

See “Disabling a probe account” on page 320.

To delete a probe account

1. In the Control Center, click **Spam > Settings > Probe Accounts**.
2. In the **Email Addresses** table, check the check box beside each probe account that you want to delete. You can also check the topmost box to select all the accounts that are listed on the page.
3. Click **Delete** or **Delete All**.

   The deleted accounts are removed from the Symantec Probe Network and no longer appear in the list of probe accounts.
Filtering content

This chapter includes the following topics:

- About content filtering
- Viewing, editing, adding, and managing your content filtering policies
- Creating a content filtering policy
- Defining conditions for a content filtering policy
- Adding actions to a content filtering policy
- Applying content filtering policies to policy groups
- Tips for testing a content filtering policy
- Managing how multiple content filtering policies are applied
- How the Message Audit Log helps to fine-tune and troubleshoot content filtering policies

About content filtering

Content filtering policies determine how Symantec Messing Gateway evaluates email messages, including their content, attachments, and attributes. Symantec Messing Gateway scans message content for the specific conditions that you set up. When a message meets the policy conditions, and the sender or recipient is part of a group to which the policy is assigned, the policy triggers a verdict. Symantec Messing Gateway then applies the policy actions.

For example, you can use content filtering policies to:

- Limit the ability of email users to communicate or conduct the activities that are contrary to your organization's values and policies.
- Prevent confidential or sensitive information from leaving your organization.
Send clicked URL requests to Symantec Email Threat Isolation or to Symantec Blue Coat ProxySG, if your organization includes one of those systems.

Route messages to an alternate mail server for traffic control or special handling.

Send copies of messages to an archive server to retain them for future reference.

Quarantine and remediate the messages that Data Loss Prevention detects with its response rules, if your organization includes that system.

After you install Symantec Messaging Gateway, the Content > Policies > Email > Email Content Filtering Policies page shows the list of default policies. These policies are enabled. You can assign them to your policy groups right away, or you can customize the conditions and actions to suit your organization’s requirements.

You create, edit, copy, delete, and manage the priority order of content filtering policies from the Email Content Filtering Policies page.

Viewing, editing, adding, and managing your content filtering policies

The Content > Policies > Email > Email Content Filtering Policies page lists all your content filtering policies. Symantec Messaging Gateway evaluates your content filtering policies in the order in which they appear on this page. The policy at the top of the list is evaluated first. The policy at the bottom of the list is evaluated last.

To add a new policy, click Add.

See “Creating a content filtering policy” on page 325.

To change an existing policy, select the policy and click Edit, or click the policy name. The Edit Email Content Filtering Policy page has the same controls as the Add Email Content Filtering Policy page.

To copy a policy, select the policy and click Copy. For example, instead of creating a new content filtering policy from the beginning, you can copy a similar policy. You can then edit the copy to create your new policy.

To delete a policy, select the policy and click Delete.

To enable a policy, select the policy and click Enable.

If the policy has a ? status, you must add the missing resources before you can enable the policy.

To disable a policy, select the policy and click Disable.

To change the priority of a policy, drag it to a new position in the list.

Be aware of the settings in the Subsequent Policy Actions column. The new position can affect the policies that are now lower in the list. For example, assume that you move a
policy that has a Bypass action from the bottom of the list to the top of the list. When this policy triggers a verdict, SMG no longer evaluates any other content filtering policies.

The Email Content Filtering Policies page also provides the following information for each policy.

Table 14-1 Email content filtering policy details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Shows one of the following statuses:</td>
</tr>
<tr>
<td></td>
<td>✓ The policy is enabled.</td>
</tr>
<tr>
<td></td>
<td>— The policy is disabled.</td>
</tr>
<tr>
<td></td>
<td>? The policy is disabled because it requires a resource. For example, if the</td>
</tr>
<tr>
<td></td>
<td>policy uses a dictionary and that dictionary is empty, you see the question</td>
</tr>
<tr>
<td></td>
<td>mark. If you add words to the dictionary, the policy state changes to</td>
</tr>
<tr>
<td></td>
<td>disabled. You can then enable it, if you want.</td>
</tr>
<tr>
<td></td>
<td>During scanning, SMG evaluates only enabled policies.</td>
</tr>
<tr>
<td>Applied to</td>
<td>Shows whether the policy is used to scan inbound mail, outbound mail, or</td>
</tr>
<tr>
<td></td>
<td>both inbound mail and outbound mail.</td>
</tr>
<tr>
<td></td>
<td>■ Inbound - The policy applies only to recipients who are in the policy groups</td>
</tr>
<tr>
<td></td>
<td>to which the policy is assigned.</td>
</tr>
<tr>
<td></td>
<td>■ Outbound - The policy applies only to senders who are in the policy groups</td>
</tr>
<tr>
<td></td>
<td>to which the policy is assigned.</td>
</tr>
<tr>
<td></td>
<td>■ Inbound and Outbound - The policy applies only to senders and recipients</td>
</tr>
<tr>
<td></td>
<td>who are in the policy groups to which the policy is assigned.</td>
</tr>
<tr>
<td>Number of groups</td>
<td>Shows the number of groups to which the policy is assigned.</td>
</tr>
</tbody>
</table>
Table 14-1  Email content filtering policy details  (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsequent Policy Actions</td>
<td>Shows what happens to policies that are lower in the list when a policy triggers a verdict. The policy's <strong>Subsequent Content Filter Handling</strong> setting controls this behavior.</td>
</tr>
<tr>
<td></td>
<td><strong>All non-conflicting</strong>: SMG evaluates the content filtering policies that are lower in the list. When the next policy triggers a verdict, SMG adds all the policy actions. SMG applies these actions after all filtering is complete, unless they conflict with a higher-priority action. See &quot;Action combinations from multiple verdicts&quot; on page 830. The policy's <strong>Subsequent Content Filter Handling</strong> setting is <strong>Continue with Evaluations &amp; Actions</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Bypass</strong>: SMG stops evaluating content filtering policies when this policy triggers a verdict. All policies that are lower in the list are bypassed. The policy's <strong>Subsequent Content Filter Handling</strong> setting is <strong>Halt Evaluations &amp; Actions</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Incidents and Notifications only</strong>: When the next policy triggers a verdict, SMG continues to evaluate messages, but ignores all the policy actions except incident actions and notification actions. The policy's <strong>Subsequent Content Filter Handling</strong> setting is <strong>Provide Incidents and Notifications Actions Only</strong>.</td>
</tr>
</tbody>
</table>

See "Managing how multiple content filtering policies are applied" on page 347.

Creating a content filtering policy

Content filtering policy conditions and actions commonly use resources such as annotations, notifications, attachment lists, and dictionaries. You set up these resources from the **Content > Resources** menu. Before you begin to create a content filtering policy, make sure that you have the resources that you need. If you don't set up the resources in advance, you must save your policy in an incomplete state. You can then set up the resources and edit the policy to add them.

To create a content filtering policy

1. In the Control Center, select **Content > Policies > Email**.
2. On the **Email Content Filtering Policies** page, click **Add**.
3. Select a template and then click **Select**.
   - The default **Blank** template has no preprogrammed conditions or actions.
   - A **Described Content** template uses existing resources from the **Content > Resources** menu. For example, the Credit Card template looks for words in the **Credit Card Number Keywords** dictionary and the **Credit Card** pattern.
A **Structured Data** template includes conditions that require custom data from a **Record** resource. These conditions display "**Not Defined**" in red. You must set up the **Record** resources, and then edit the conditions to add the resources, before you can use a **Structured Data** template. See “**Using structured data in a content filtering policy**” on page 354.

4 On the **Add Content Filtering Policy** page, type a name for the policy. The name must be unique and should describe the purpose of the policy.

5 If you want to view reports about violations of this policy, make sure that **Track violations of this policy in the dashboard and reports** is enabled. If you disable this option, you can view policy activity in the message audit log, but not in the dashboard or reports.

For example, you may want to enable this option to track violations of a policy against sending executable file attachments. You may want to disable this option for a policy that adds a privacy annotation to every outgoing message.

6 You can use the **Enable or Disable decomposition of files in list** option to limit which attachments are scanned. When this option is unchecked, which is the default setting, Symantec Messaging Gateway decomposes and scans all attachments.

- To scan **only** the attachment types in a list, check this option and select **Enable**. Then select the attachment list from the drop-down menu.

- To scan all attachment types **except** the ones in the selected list, check this option and select **Disable**. Then select the attachment list from the drop-down menu.

**Note:** If you disable an attachment type, SMG does not scan files that are embedded in those attachments. For example, if you disable attachments that are in Word format, SMG does not detect an Excel file that is embedded in a Word file.

You can create additional attachment lists from the **Content > Resources > Attachment Lists** page. After you create an attachment list, the list name appears in the drop-down menu.

7 Select a **Subsequent Content Filter Handling** setting. This setting affects the next content filtering policy that triggers a verdict.

See “**Managing how multiple content filtering policies are applied**” on page 347.

8 In the **Conditions** panel, select whether to apply the policy to **Inbound messages**, **Outbound messages**, or **Inbound and outbound messages** and then select your content filtering conditions.

See “**Defining conditions for a content filtering policy**” on page 327.
9 In the **Actions** panel, add the actions that you want Symantec Messaging Gateway to take when messages match the policy conditions.  
See “Adding actions to a content filtering policy” on page 332.

10 In the **Apply to the following policy groups** panel, check the box next to **Policy Groups** to enable this policy for all groups. Or check the boxes next to individual groups to enable the policy only for the selected groups.

11 Click **Save**.

12 On the **Email Content Filtering Policies** page, adjust the position of the new policy, if needed.  
See “Managing how multiple content filtering policies are applied” on page 347.

## Defining conditions for a content filtering policy

To define the conditions for a content filtering policy, you can add as many individual conditions as you need. You can then group any of these conditions together to build a compound condition that scans for exactly what you want to detect.

### Grouping conditions

You can set up your policy to evaluate each condition separately, or you can group conditions together. To group conditions together, select them and then click (X&Y). To ungroup conditions, select the group and click (X),(Y).

Within a policy, each condition can be part of only one group. For example, to detect the combination of a valid credit card, US zip code, and US phone number or the combination of a valid social security number, US zip code, and US phone number, you must create two separate policies.

### Choosing Any or All

From the **Which of the following conditions must be met** menu, choose **Any** to trigger a verdict when one condition in the policy is met. Choose **All**, to trigger a verdict only when every condition in the policy is met. Grouped conditions are treated as a single condition.

For example, assume that a policy has these conditions:

- Text in the Body part of the message contains 2 or more occurrences of "CONFIDENTIAL"
- The Message size is greater than 56 MB
- The file metadata has a file name that contains the words "TOP SECRET"

The following examples show how the **Any** or **All** setting affects how SMG evaluates messages against the policy.
### All conditions must be met

Every condition that you specify must exist in an email message to trigger a violation.

For example:

An email message without attachments, is 70 MB, and contains the word "CONFIDENTIAL" twice in the body of the message. This message does not meet the file name condition, so it does not trigger a violation.

An email with an attachment TOP SECRET.doc, is 70 MB, and contains the word "CONFIDENTIAL" twice in the body of the message. This message meets all conditions, so it triggers a violation.

### Any condition must be met

At least one condition must exist in an email message to trigger a violation.

For example:

An email without attachments, is 10 MB, and contains the word "CONFIDENTIAL" once in the body of the message. This message does not meet any of the policy conditions, so it does not trigger a violation.

An email message without attachments, is 70 MB, and contains the word "CONFIDENTIAL" once in the body of the message. This message meets the "greater than 56 MB" condition, so it triggers a violation.

### Any condition must be met and You grouped the first two conditions

At least one condition must exist in an email to trigger a violation. However, the body part that contains two or more occurrences of the word "CONFIDENTIAL" and the message size greater than 56 MB is considered a single condition.

For example:

An email with 10 occurrences of the word "CONFIDENTIAL" in the message body, is 10 MB, and has no attachments does not trigger a violation.

An email with no occurrences of the word "CONFIDENTIAL" in the message body, is 70 MB, and has no attachments does not trigger a violation.

An email that contains 10 occurrences of the word "CONFIDENTIAL" in the message body, is 70 MB, and has no attachments triggers a violation.

An email with no occurrences of the word "CONFIDENTIAL" in the message body, is 10 MB, and contains an attachment TOP SECRET.doc triggers a violation.

---

See “Creating a content filtering policy” on page 325.

See “Considerations for content filtering policy conditions” on page 328.

### Considerations for content filtering policy conditions

Keep in mind the following suggestions and requirements as you create content filtering policy conditions:
To give you more flexibility when you create policies, you can add negative conditions to your content filtering policies. However, if you create a policy that has positive and negative versions of the same condition, either every message triggers a verdict or no message triggers a verdict from that policy.

For example, assume that you create a policy with the condition "Text in the subject, body, or attachments contains 1 or more words from the Financial Keywords dictionary." Then you add the condition "Text in the subject, body, or attachments does not contain 1 or more words from the Financial Keywords dictionary."

If the policy specifies that any condition must be met, all messages trigger a violation. A message must either contain words from the Financial Keywords dictionary or it does not contain words from the Financial Keywords dictionary.

If the policy specifies that all conditions must be met, no message triggers a violation. The same message can't contain words from the Financial Keywords dictionary and not contain words from the Financial Keywords dictionary.

If you want to scan for the positive and negative versions of the same condition, create two separate policies.

See “Positive and negative content filtering rule condition examples” on page 842.

### Using negative conditions

<table>
<thead>
<tr>
<th>Using negative conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>To give you more flexibility when you create policies, you can add negative conditions to your content filtering policies. However, if you create a policy that has positive and negative versions of the same condition, either every message triggers a verdict or no message triggers a verdict from that policy.</td>
</tr>
</tbody>
</table>

For example, assume that you create a policy with the condition "Text in the subject, body, or attachments contains 1 or more words from the Financial Keywords dictionary." Then you add the condition "Text in the subject, body, or attachments does not contain 1 or more words from the Financial Keywords dictionary."

If the policy specifies that any condition must be met, all messages trigger a violation. A message must either contain words from the Financial Keywords dictionary or it does not contain words from the Financial Keywords dictionary.

If the policy specifies that all conditions must be met, no message triggers a violation. The same message can't contain words from the Financial Keywords dictionary and not contain words from the Financial Keywords dictionary.

If you want to scan for the positive and negative versions of the same condition, create two separate policies.

See “Positive and negative content filtering rule condition examples” on page 842.

### Using conditions when you integrate with Enforce Server

<table>
<thead>
<tr>
<th>Using conditions when you integrate with Enforce Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Enforce Server adds headers to the messages that violate their policies. For Symantec Messaging Gateway to detect these headers, you must describe this header in your policy conditions.</td>
</tr>
</tbody>
</table>

For example, assume that Enforce Server adds the header 'X-DLP-violation: Yes' to the messages that violate policies. You would add the following condition: "If text in Message header 'X-DLP-violation' contains 1 or more occurrences of 'yes' to your content filtering policy."

See “Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway” on page 471.

### File attachment size limits

<table>
<thead>
<tr>
<th>File attachment size limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you create a policy that uses file attachment size limits and you receive a compressed file, Messaging Gateway evaluates the size of the file to determine whether the attachment's size exceeds your specified limit. Compressed files within containers (e.g. ZIP files) are evaluated based on their uncompressed size by default. Files that are compressed without being enclosed in a container (e.g. files created using the Linux gzip command) are evaluated based on both their compressed and uncompressed sizes, and the policy is triggered if either size exceeds the limit set in your policy.</td>
</tr>
</tbody>
</table>
Compressed files: SMG does not scan a compressed file attachment if the uncompressed attachment exceeds the **Maximum individual file size when opened** container limit. You set this file size in the **Container limits** panel of the **Protocols > SMTP > Settings > Content Scanning** tab. Make sure that any limit you set on attachment file size in a content filtering policy condition does not exceed the limit for container files. If the attachment file size condition exceeds the **Maximum individual file size when opened** container limit, any messages that trigger the policy receive an Unscannable verdict.

See “Setting limits on nested files” on page 228.

Case sensitivity: All tests for words and phrases are not case-sensitive. Lowercase letters in your conditions match both lower- and uppercase letters in messages. Uppercase letters in your conditions match lower- and uppercase letters in messages.

Multiple white spaces: Multiple white spaces in an email header or body are treated as a single-space character.

See “Positive and negative content filtering rule condition examples” on page 842.
See “Viewing the text that violated a content filtering policy” on page 447.

### Content filtering condition match criteria

**Table 14-2** describes how Symantec Messaging Gateway evaluates the match criteria (for example, match/does not match) in content filtering policy conditions.

<table>
<thead>
<tr>
<th>Match criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains/Does not contain</td>
<td>This match is evaluated differently based on its use:</td>
</tr>
</tbody>
</table>
| | - Dictionaries  
  Tests the message content against the words or file extensions that are found in the selected dictionary.  
- User-defined text  
  Tests for the user-defined text within the component that is specified.  
  Sometimes called a substring test.  
- Occurrences  
  Tests the user-specified number of instances. |
| Matches regular expression/Does not match regular expression | Tests the message content against user-specified regular expressions. Regular expressions combine alphanumeric characters with metacharacter variables to identify pattern variations. |
| Matches pattern/Does not match pattern | Tests the message content against known regular-expression patterns such as those found in Social Security numbers or credit card numbers patterns. |
Table 14-2  Condition match criteria *(continued)*

<table>
<thead>
<tr>
<th>Match criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matches data in the record resource</td>
<td>Compares the contents of a message with the data in the selected record.</td>
</tr>
</tbody>
</table>
| Starts with/Does not start with                     | The regular expression equivalent to ^text.*  
| Ends with/Does not end with                         | The regular expression equivalent to *text.$  
| Match exactly/does not match exactly                | The equivalent of match exactly or does not match exactly for the supplied test.                                                            |
| Contains the message part/Does not contain the      | Tests the message against the user-specified message part to see if the message part exists.                                                |
| message part                                        |                                                                                                                                              |
| Is equal to/Is greater than/Is less than            | Compares the message size or attachment size with the specified number of bytes, kilobytes (KB), or megabytes (MB).                     |
| Is in the attachment list/Is not in the attachment   | Compares the body part and message attachment to the user-specified attachment list to see if it appears in the list.                     |
| list (true file type and class only)                |                                                                                                                                              |
| Is in the attachment list/Is not in the attachment   | Note: For the condition Is in attachment list, SMG evaluates attachments and any objects that are embedded in message bodies for true file type, true file class, file name, file extension, and MIME. |
| list (true file type and class only)                | For the condition Is not in attachment list, SMG evaluates attachments and the objects that are embedded in message bodies for true file type and true file class. SMG does not test for file name, extension, or MIME type for this condition. |
| Has a file name which contains/Has a file name       | Compares the file name to the user-specified file name to determine if a match exists.                                                     |
| which does not contain                               |                                                                                                                                              |
| Has a MIME type which is/Has a MIME type which is   | Tests the message to determine if it is the same as the user-defined MIME type.                                                             |
| not                                                 |                                                                                                                                              |
| Has a file name from dictionary/Has a file name      | Compares the file name to file names in the user-specified dictionary to determine if a match exists.                                       |
| not from dictionary                                 |                                                                                                                                              |
| Has a file extension from dictionary/Has a file      | Compares the file extension to file extensions in the user-specified dictionary to determine if a match exists.                            |
| extension not from dictionary                        |                                                                                                                                              |
Using regular expressions in content filtering policy conditions

A regular expression is a pattern that you want SMG to use to identify specific information. You can use Perl regular expressions when you create conditions for a content filtering rule. To use Perl expressions, you must use either matches regular expression or does not match regular expression as a policy condition.

SMG matches regular expressions in the following ways:

- When matched against the message body, matches against the entire body text, not on a line-by-line basis.
- When matched against each attachment in the message, matches against the entire attachment text, not on a line-by-line basis.

By default, Symantec Messaging Gateway treats regular expressions as case-insensitive. However, you can use the following strings to change the case sensitivity to a different mode.

- Type the string (?i) into the regular expression statement and everything after that ignores case sensitivity. (?!)
- Type the string (?-i) into the regular expression statement and everything after that is case-sensitive. (?-i)

You can switch your regular expression query from case-insensitive to case-sensitive as many times as you want.

To use a pattern to match certain special characters (including forward slashes), you must precede each character with backslash (\).

See “Perl-compatible regular expressions” on page 414.

For more information about Perl-compatible regular expressions, search the documentation at https://www.perl.org/.

Adding actions to a content filtering policy

When you create a content filtering policy, you add the actions that you want Symantec Messaging Gateway to take when a message meets the policy conditions.
You can select multiple actions to perform when the policy is violated. Symantec Messaging Gateway applies the actions in the order in which they appear in the policy’s Actions list.

To add content filtering policy actions

1. On the Add Email Content Filtering Policy page under Actions, click Add.
2. In the Configure An Action dialog box, select the action that you want SMG to take when a message violates the conditions of the policy.
   - For some actions, you must provide additional information.
     - See “Policy actions and what they do” on page 333.

3. Click Add Action.
4. If you select the action Create a quarantine incident, you must also specify the actions to take when a quarantine administrator processes the messages.
   - Click Add Approved Action. On the Configure An Action page, select an action, and click Add Approved Action.
   - Click Add Reject Action. On the Configure An Action page, select an action and click Add Reject Action.
   - Click Add Custom Action. On the Configure An Action page, select the action and click Add Custom Action.
     - If you integrate with the Enforce Server, make sure that the response rule actions in the Enforce Server administration console are consistent with the SMG actions for Approve, Reject, and Custom.
     - If you do not integrate with the Enforce Server, you must still select a Custom action for legacy support.
     - See “Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway” on page 471.

5. Repeat this procedure to add as many actions as you need.
   - See “Creating a content filtering policy” on page 325.

Policy actions and what they do

The following table describes the actions that you can add to Symantec Messaging Gateway policies.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver message normally</td>
<td>Deliver the message to the intended recipients without any modifications to the message.</td>
</tr>
</tbody>
</table>
Table 14-3  Policy actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete message</td>
<td>Permanently delete the message. The message cannot be retrieved.</td>
</tr>
<tr>
<td>Hold message in Spam Quarantine</td>
<td>Place the message in the end user's Spam Quarantine. See “About quarantining spam” on page 280.</td>
</tr>
<tr>
<td>Forward a copy of the message</td>
<td>Sends a copy of the message to the people that you specify. You must also provide this additional information:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Forward to</strong></td>
</tr>
<tr>
<td></td>
<td>Type the email addresses of the people to whom you want to forward a copy of the message. Separate multiple entries with commas.</td>
</tr>
<tr>
<td>Route the message</td>
<td>Sends the original message to the specified mail server for delivery to the original recipients. You must also provide this additional information:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Host</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the host where you want to route the message.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Port</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the host’s port number.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Use MX Lookup</strong></td>
</tr>
<tr>
<td></td>
<td>Check this box if you want to route the message with MX Lookup to locate the information that corresponds to the SMTP host.</td>
</tr>
<tr>
<td></td>
<td>You can use <strong>Route the message</strong> for traffic control. Suppose your regular mail server can’t accept messages with attachments that are larger than 100 GB, for example. You can create a content filtering policy that routes all messages with attachments larger than 100 GB to a different mail server.</td>
</tr>
</tbody>
</table>
### Table 14-3  Policy actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive the message</td>
<td>Specifies where to send an archive copy of the message.</td>
</tr>
<tr>
<td></td>
<td>Complete the following information:</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Archive email address</strong></td>
</tr>
<tr>
<td></td>
<td>Enter an email address to which archived copies of message are sent.</td>
</tr>
<tr>
<td></td>
<td>If you entered an archive email address on the Content &gt; Settings &gt; Archive page, that address is the default.</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Optional archive tag</strong></td>
</tr>
<tr>
<td></td>
<td>Specify an archive tag to add an <code>X-archive:</code> header to archived messages, followed by your text. You can enter any characters except carriage return, line feed, or semicolon.</td>
</tr>
<tr>
<td></td>
<td>The <code>X-archive:</code> header may be useful to sort archived messages when you view them with an email client. However, Symantec Messaging Gateway itself does not use the <code>X-archive:</code> header.</td>
</tr>
<tr>
<td></td>
<td>If multiple policy actions archive the same message, each unique <code>X-archive:</code> header is added to the message. For example, the archive tag <code>Docket 53745</code> adds the header <code>X-archive: Docket 53745</code> to the message when it is archived.</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Encoding</strong></td>
</tr>
<tr>
<td></td>
<td>Specify the encoding for the archive tag.</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Configure Archive Server</strong></td>
</tr>
<tr>
<td></td>
<td>If you entered archive server information on the Content &gt; Settings &gt; Archive page, that mail server is the default archive server. If not, these fields are blank. You can use the default server or enter the following information:</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Archive server host</strong></td>
</tr>
<tr>
<td></td>
<td>Type the host name or IP address for the archive mail server.</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Archive server port</strong></td>
</tr>
<tr>
<td></td>
<td>If you specified an archive server host, also type the archive server port.</td>
</tr>
<tr>
<td></td>
<td>■  <strong>Enable MX Lookup</strong></td>
</tr>
<tr>
<td></td>
<td>Check this box if you want to route archive messages with MX Lookup to locate the information that corresponds to the archive server host.</td>
</tr>
<tr>
<td></td>
<td>An email address is required. Archive server information is optional. If you enter only an email address, SMG uses the normal routing to send the messages to the archive address.</td>
</tr>
</tbody>
</table>

See “Specifying where to save archived messages” on page 417.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
</table>
| Send a Delivery Status Notification | Returns the message to its From: address with an explanation, and delivers the message to the recipient.  
You must also provide this additional information:  
  - **Explanation**  
    Enter the message text that notifies the sender of the delivery status.  
  - **Encoding**  
    Specify the encoding that you want to use for the notification.  
  - **Include original message**  
    Check this box to include the original message in the notification to the sender.                                                                                                                                                                                                                                        |
| Add BCC recipients               | Sends a blind copy of the message to the email recipients that you specify. Blind copy recipients are not visible in the address line of the message.  
You must also provide this additional information:  
  - **BCC recipients**  
    Specify the email addresses of the recipients that you want to receive a blind copy of the message. Separate multiple entries with commas.                                                                                                                                                                   |
| Modify the subject line          | Adds text to the beginning or the end of the message’s Subject: line.  
You must also provide this additional information:  
  - **Modification**  
    Enter the text that you want to add to the subject line.  
  - **Encoding**  
    Click the drop-down list and select the encoding for the message.  
  - Select **Prepend to subject** to add the Modification text to the beginning of the subject line.  
  - Select **Append to subject** to add the Modification text to the end of the subject line.                                                                                                                                                                |
| Add a header                     | Adds a header to the message.  
You must also provide this additional information:  
  - **Header**  
    Type the header that you want to add to the message; for example, X-Cfilter.  
  - **Value**  
    Enter the value of the header; for example, Data violation incident.  
  - **Encoding**  
    Select the encoding to use for the header.                                                                                                                                                                                                                           |
### Table 14-3 Policy actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add annotation</td>
<td>Adds an annotation to the message body.</td>
</tr>
<tr>
<td></td>
<td>You must also provide this additional information:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Annotation</strong></td>
</tr>
<tr>
<td></td>
<td>Select the annotation that you want to use.</td>
</tr>
<tr>
<td></td>
<td>You can add annotations to the drop-down list from the <em>Content &gt; Resources &gt; Annotations</em> page.</td>
</tr>
<tr>
<td></td>
<td>■ Select <strong>Prepend annotation</strong> to add the annotation before the message body. Select <strong>Append annotation</strong> to add the annotation after the message body.</td>
</tr>
<tr>
<td></td>
<td>See “Creating and managing annotations for policy violations” on page 399.</td>
</tr>
<tr>
<td>Send notification</td>
<td>Deliver the original message to the intended recipient and send a predefined notification.</td>
</tr>
<tr>
<td></td>
<td>You must also provide this additional information:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Notification</strong></td>
</tr>
<tr>
<td></td>
<td>Select the notification that you want to send.</td>
</tr>
<tr>
<td></td>
<td>You can add notifications to the drop-down list from the <em>Content &gt; Resources &gt; Notifications</em> page.</td>
</tr>
<tr>
<td></td>
<td>See “About policy violation notifications” on page 377.</td>
</tr>
<tr>
<td>Strip attachments</td>
<td>Delete the attachments that meet the specified options.</td>
</tr>
<tr>
<td></td>
<td>You can choose from the following options:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Strip all attachments</strong></td>
</tr>
<tr>
<td></td>
<td>Deletes all attachments, regardless of whether the attachments violated the policy.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Strip attachment lists</strong></td>
</tr>
<tr>
<td></td>
<td>Click the drop-down list and select the type of attachments that you want to delete, regardless of whether any of the attachments violate the policy.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Strip matching attachments</strong></td>
</tr>
<tr>
<td></td>
<td>Only deletes the attachments that violated the policy.</td>
</tr>
<tr>
<td>Create an informational</td>
<td>When the policy is violated, send a copy of the message to the <em>Informational Incidents</em> folder that you specify. The original message is delivered, unless you select a delete action or a quarantine action.</td>
</tr>
<tr>
<td>incident</td>
<td>You must also provide this additional information:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>In content informational incident folder</strong></td>
</tr>
<tr>
<td></td>
<td>Click the drop-down list and select the Informational Incidents folder in which you want the incident created.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify an Informational Incidents folder, the incident is created in the default Informational Incidents folder.</td>
</tr>
<tr>
<td></td>
<td>See “About content incident folders” on page 419.</td>
</tr>
</tbody>
</table>
Table 14-3  Policy actions *(continued)*

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a quarantine incident</td>
<td>Send the original message to the Quarantine Incidents folder that you specify. You must also provide this additional information:</td>
</tr>
<tr>
<td></td>
<td>■ In content quarantine incident folder</td>
</tr>
<tr>
<td></td>
<td>Click the drop-down list and select the Quarantine Incidents folder in which you want the incident created. If you do not specify a Quarantine Incidents folder, the incident is created in the default Quarantine Incidents folder.</td>
</tr>
<tr>
<td></td>
<td>After you add the Create a quarantine incident action, three Message Review actions appear in the Actions list. You must select an action for each Message Review action.</td>
</tr>
<tr>
<td></td>
<td>■ Click Add Approved Action and select the action that you want SMG to take when an administrator approves a quarantined email from the folder's Incident Management page.</td>
</tr>
<tr>
<td></td>
<td>■ Click Add Reject Action and select the action that you want SMG to take when an administrator rejects a quarantined email.</td>
</tr>
<tr>
<td></td>
<td>■ Click Add Custom Action and select the action that you want SMG to take when an administrator selects the Custom option for a quarantined email. This option is provided for legacy support and is not recommended. However, you must add a custom action.</td>
</tr>
<tr>
<td></td>
<td>You can only apply a Quarantine Incidents action once per policy. Note: After you add a Quarantine Incidents action, you may also want to add a notification action to the policy. For example, if you quarantine large messages, you can send a notification that tells the recipient that they received a large message that is quarantined. The notification might include the sender, the attachment information, and how to contact the administrator to get the original message.</td>
</tr>
<tr>
<td></td>
<td>See “About content incident folders” on page 419.</td>
</tr>
<tr>
<td>Deliver message with TLS encryption</td>
<td>Send the message over an encrypted channel. Specify one of the following options, based on the encryption that the recipient host expects:</td>
</tr>
<tr>
<td></td>
<td>■ Attempt TLS encryption</td>
</tr>
<tr>
<td></td>
<td>■ Require TLS encryption and don't verify certificate</td>
</tr>
<tr>
<td></td>
<td>■ Require TLS encryption and verify certificate</td>
</tr>
<tr>
<td>Deliver message with content encryption</td>
<td>Deliver the message with content encryption. Note: You must have a content encryption license installed to select this action.</td>
</tr>
<tr>
<td></td>
<td>See “Encrypting data with Symantec Content Encryption” on page 449.</td>
</tr>
</tbody>
</table>
### Table 14-3  Policy actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treat as spam</td>
<td>Consider the message spam and take the action that is specified in your spam policies. See “About filtering email spam and unwanted messages” on page 248.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat as suspected spam</td>
<td>Consider the message suspected spam and take the action that is specified in your suspected spam policies. See “About filtering email spam and unwanted messages” on page 248.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat as a virus</td>
<td>Consider the message a virus and take the actions that are specified in your virus policies. See “About detecting viruses, malware, and malicious attacks” on page 204.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat as a mass-mailing worm</td>
<td>Process the message based on the action in the associated mass-mailing worm policy. See “About detecting viruses, malware, and malicious attacks” on page 204.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat as a bad sender</td>
<td>Process the message based on the action that you specify in the Local Bad Sender Domains group. This action applies even if the Local Bad Sender Domains group is disabled. See “About blocking and allowing messages using sender groups” on page 151.</td>
</tr>
<tr>
<td>Treat as a good sender</td>
<td>Process the message based on the action that you specify in the Local Good Sender Domains group. This action applies even if the Local Good Sender Domains group is disabled. These messages are not scanned for spam. See “About blocking and allowing messages using sender groups” on page 151.</td>
</tr>
<tr>
<td>Bypass spam scanning</td>
<td>Do not scan the message for spam. See “About filtering email spam and unwanted messages” on page 248.</td>
</tr>
<tr>
<td>Bypass Disarm scanning</td>
<td>Do not use Disarm scanning to locate and remove potentially malicious content from attachments. See “About Disarm” on page 207.</td>
</tr>
<tr>
<td>Bypass Threat Defense scanning</td>
<td>Do not send the message to Content Analysis for advanced threat scanning. See “About threat defense scanning” on page 455.</td>
</tr>
</tbody>
</table>
Table 14-3 Policy actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and additional options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify clickable URLs</td>
<td>Change, replace, or delete all clickable links in messages. Select a Type of service and enter options:</td>
</tr>
<tr>
<td></td>
<td>■ Select Email Threat Isolation to route all URL requests through your Symantec Threat Isolation instance. In the Prepend Value field, enter the fully-qualified domain name (FQDN) or IP address of your Email Threat Isolation instance. Make sure that you also select the Inbound only condition for the policy. See “Integrating Symantec Messaging Gateway with Symantec Email Threat Isolation” on page 341.</td>
</tr>
<tr>
<td></td>
<td>■ Select Web Service (ProxySG) to route all URL requests through your Symantec Blue Coat ProxySG server. In the Proxy URL field, enter the URL of your ProxySG server in the format <a href="https://FQDN/">https://FQDN/</a>. The URL must include the fully-qualified domain name (FQDN) of your ProxySG appliance, and must end with a forward slash (/). Make sure that you also select the Inbound only condition for the policy. See “Redirecting URLs to your ProxySG appliance” on page 343.</td>
</tr>
<tr>
<td></td>
<td>■ Select Replace clickable URLs in message to change all the URLs in the message to the string that you enter in the Value field. For messages in HTML format, all the underlying URL addresses change to the Value string. The recipient sees the original URLs in the message, but none are clickable. For messages in text format, the underlying URL is the same as the visible URL, so the recipient sees the modified URL. If you replace all URLs with a URL, the new URL may be clickable, depending on your email client. See “Modifying URLs to protect against threats and unauthorized access” on page 340.</td>
</tr>
<tr>
<td></td>
<td>■ Select Disable clickable URLs in message to prevent the browser from navigating to the URL destination when a recipient clicks a link. The original links are visible in the message body, but they do not work. See “Modifying URLs to protect against threats and unauthorized access” on page 340.</td>
</tr>
</tbody>
</table>

See “Adding actions to a content filtering policy” on page 332.

See “Managing how multiple content filtering policies are applied” on page 347.

Modifying URLs to protect against threats and unauthorized access

When you create a content filtering policy, you can add the action Modify clickable URLs in message. This action changes all the URLs in a message before the message is delivered. You can choose one of the following options to customize the action further:
- **Email Threat Isolation** sends the browser to your Symantec Threat Isolation instance for virtual sandboxing. 
  See "Integrating Symantec Messaging Gateway with Symantec Email Threat Isolation" on page 341.

- **Web Service (ProxySG)** sends the browser to your Symantec Blue Coat ProxySG appliance for secure web browsing. 
  See "Redirecting URLs to your ProxySG appliance" on page 343.

- **Replace clickable URLs in message** changes all URLs in the message to the Value that you enter in the dialog box. If the message is in HTML format, the underlying URLs change, but the message displays the original URLs. If the message is in text format, the recipient sees the Value string instead of the original URLs. 
  See "Replacing clickable URLs in messages" on page 345.

- **Disable clickable URLs in message** inserts the string noclick_ into the host name of each URL. 
  When the recipient clicks a URL in a message, nothing happens. If the message is in plain text format, the recipient may notice that the URL is modified. If the message is in HTML format, the URL modification is not visible. 
  Symantec recommends that you add an additional action to the policy to let recipients know that URLs in the message were disabled deliberately. For example, you can select **Modify the subject line of messages** and add the modification **For security, URLs in this message are disabled**.

SMG can perform only one **Modify clickable URLs in message** action on a message. If a message triggers two or more policies that have different **Modify clickable URLs in message** actions, SMG uses the following priority to select which action to perform:

1. Email Threat Isolation
2. Web Service (ProxySG)
3. Replace clickable URLs in message
4. Disable clickable URLs in message

**Integrating Symantec Messaging Gateway with Symantec Email Threat Isolation**

Symantec Email Threat Isolation provides a secure execution environment for web interactions. When a user clicks a link in an email message, Email Threat Isolation isolates the browser from the Internet. Email Threat Isolation executes all potentially malicious content. Only a safe visual stream is sent to the user.

You can integrate Symantec Messaging Gateway with Email Threat Isolation by adding a Modify URL action to your content filtering policies. When the policy triggers a verdict, the
action modifies every URL in the affected message. If a recipient clicks a link in the message, the browser redirects the request to Email Threat Isolation for isolation and execution.

**To add Symantec Email Threat Isolation to a content filtering policy**

1. In Control Center, from the **Content > Policies > Email** page, click **Add** to create a new content filtering policy. Or select a policy and click **Edit** to add Email Threat Isolation to an existing content filtering policy.

   See “Creating a content filtering policy” on page 325.

2. Under **Conditions**, from the **Apply to** menu, select **Inbound messages**.

   **Warning:** Never apply Email Threat Isolation to outbound messages. In most cases, outbound recipients do not have permission to access to your Email Threat Isolation instance. The result is that the links with modified URLs are likely to fail.

3. In the **Actions** panel, click **Add**.

4. In the **Configure An Action** dialog box, select **Modify clickable URLs in message**.

5. In the **Type of service** field, select **Email Threat Isolation**.

6. In the **Prepend value** field, enter the fully-qualified domain name (FQDN) or IP address of your Symantec Email Threat Isolation instance.

   **Note:** For Symantec Messaging Gateway 10.6.5, see https://www.symantec.com/docs/HOWTO127807 for instructions on how to enter the **Prepend value** for that version.

7. Click **Add Action**.

   When a message triggers a verdict, Symantec Messaging Gateway modifies all the URLs in the message to redirect them to the hostname that you specified in the **Prepend value**. When a recipient clicks a modified link, the browser request is routed to your Email Threat Isolation instance.

8. When you finish creating or editing the policy, click **Save**.

**Protecting all your users with Email Threat Isolation**

To create a content filtering policy that applies Email Threat Isolation protections to all inbound messages:

1. On the **Email Content Filtering Policies** page, click **Add**.

2. Select the **Blank** template.
3 In the **Settings** panel, disable *Track violations of this policy in the dashboard and reports*.

4 In the **Conditions** panel, from the **Apply to** menu, select *Inbound messages*.

5 Click **Add** to add a new condition.

6 Select *For all messages*, and then click **Add Condition**.

7 In the **Actions** panel, click **Add**. Follow the steps in the previous procedure to add the **Modify clickable URLs** action.

8 Apply the policy to all policy groups and then click **Save**.

9 On the **Email Content Filtering Policies** page, drag the policy to the top of the list.

**Redirecting URLs to your ProxySG appliance**

You can add an action to your Symantec Messaging Gateway content filtering policies to redirect all browser requests to your Symantec Blue Coat ProxySG appliance. If a message triggers a verdict for the policy, the action adds the ProxySG URL to the beginning of every clickable URL in the message. When a user clicks a link, the computer redirects the browser request to the ProxySG URL. Your ProxySG policies then determine whether the user gets access to the linked webpage.

---

**Note:** Your users’ computers and browsers must be set up to communicate with the ProxySG appliance. In addition, you must define policies on ProxySG to evaluate and process the browser requests. The ProxySG default is to refuse access, so all redirected browser requests from SMG will fail until you define the relevant policies. For instructions on how to set up ProxySG policies, refer to the ProxySG documentation.

---

**To send browser requests to Symantec Secure Web Gateway (ProxySG)**

1 In Control Center, from the **Content > Policies > Email** page, click **Add** to create a new content filtering policy. Or select a policy and click **Edit** to add ProxySG redirection to an existing content filtering policy.

   See “Creating a content filtering policy” on page 325.

2 Under **Conditions**, from the **Apply to** menu, select *Inbound messages*.

   **Warning:** Never apply a policy that redirects to Proxy SG to outbound messages. Outbound recipients don't have permission to access to your ProxySG appliance, so the links with modified URLs will fail.

3 In the **Actions** panel, click **Add**.
4. In the **Configure An Action** dialog box, select **Modify clickable URLs in message**.

5. In the **Type of service** field, select **Web Service (ProxySG)**.

6. In the **Proxy URL** field, enter the URL of your ProxySG appliance in the format **https://FQDN/**. For example: **https://mycompanyproxy.com/**

   The URL must include the fully-qualified domain name (FQDN) of your ProxySG appliance, and must end with a forward slash (/).

7. Click **Add Action**.

   When a message triggers a verdict, Symantec Messaging Gateway adds the **Proxy URL** to the beginning of all the URLs in the message. When a recipient clicks a modified link, the **Proxy URL** routes the browser request to your ProxySG.

8. To test the **Proxy URL**, type it into the address line of a browser. Then add a URL that you know is valid to the end of the **Proxy URL**, and press **Enter**. For example:

   If your **Proxy URL** is **https://mycompanyproxy.com/** and the URL is **https://www.symantec.com**


   If the **Proxy URL** is correct, the browser displays the Symantec Corporation home page.

   The test computer must be set up to communicate with your ProxySG appliance, and the ProxySG must have a policy to allow this access.

9. When you finish creating or editing the policy, click **Save**.

   See “**Adding actions to a content filtering policy**” on page 332.

### Protecting all your users with ProxySG

To create a content filtering policy that applies ProxySG protections to all inbound messages:

1. On the **Email Content Filtering Policies** page, click **Add**.

2. Select the **Blank** template.

3. In the **Settings** panel, disable **Track violations of this policy in the dashboard and reports**.

4. In the **Conditions** panel, from the **Apply to** menu, select **Inbound messages**.

5. Click **Add** to add a new condition.

6. Select **For all messages**, and then click **Add Condition**.
7 In the **Actions** panel, click **Add**. Follow the steps in the previous procedure to add the **Modify clickable URLs** action.

8 Apply the policy to all policy groups and then click **Save**.

9 On the **Email Content Filtering Policies** page, drag the policy to the top of the list.

### Replacing clickable URLs in messages

When you select the content filtering policy action **Modify clickable URLs in message** and choose the option **Replace clickable URLs in message**, you enter a **Value** string that replaces all the clickable URLs. The user experience for recipients depends on the **Value** string and whether the message is delivered in HTML or text format.

#### Table 14-4  Results when you modify clickable URLs

<table>
<thead>
<tr>
<th>When you replace each URL with:</th>
<th>Results when the message is in HTML format:</th>
<th>Results when the message is in text format:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text that does not contain a URL</td>
<td>The recipient sees the original URLs in the message, but the underlying links change to the text string that you specify. When a recipient clicks a modified link, a browser window opens and displays an error message that the webpage cannot be found.</td>
<td>The new text replaces each URL in the message. The recipient does not see the original URLs. The new text is not clickable.</td>
</tr>
<tr>
<td>Text that contains a URL</td>
<td>Recipients see the original URLs when they view their messages, but the underlying links change to the text and URL string that you specify. When a recipient clicks a modified link, a browser window opens and displays an error message that the webpage cannot be found.</td>
<td>The new text and URL string replaces each original URL in the message. The recipient does not see the original URLs. The new URL may be clickable, depending on the capabilities of the email client.</td>
</tr>
<tr>
<td>Another URL (no additional text)</td>
<td>Recipients see the original URLs when they view their messages, but the underlying links change to the URL that you specify. When the recipient clicks a link in the message, a browser window opens and displays the webpage for the replacement URL.</td>
<td>The new URL replaces each original URL in the message. The recipient does not see the original URLs. The new URL may be clickable, depending on the capabilities of the email client.</td>
</tr>
</tbody>
</table>
To provide the best user experience when you support message delivery in both HTML and text format, either:

- Replace all URLs with another URL. For example, you can enter the full URL of a webpage that explains your organization's privacy policies. Do not include additional text. Test the result to ensure that the replacement URL is clickable in both HTML and text formats.
- Replace all URLs with a text string; for example "Link was disabled for your protection." Then add a header action or annotation action to the policy to notify recipients that all the original URLs in the message are disabled.
  - If the message is in HTML format, recipients see the header or annotation, which explains why none of the visible links work. If the message is in text format, recipients see the replacement text instead of the original URLs. They also see the header or annotation.

### Applying content filtering policies to policy groups

After you define the actions for your content filtering policy, specify the policy groups for which the policy applies.

You must create separate policies for the messages that meet similar conditions but require separate actions for different policy groups. Similarly, inbound messages may be treated differently from the outbound messages that otherwise meet the same conditions for a policy group.

For example, assume that separate actions are required to route the email that contains sensitive human resource data. Create one policy in which the messages that are sent to executives do not include attachments. Create a separate policy that contains the same conditions, but the messages that are sent to managers are held for review.

You can apply content filtering policies to policy groups in either of the following ways:

- Create the policy group first and then apply the policy to that group when you create your content filtering policy.
  - The process to create a content filtering policy assumes that the policy group is created first, and then the policy is applied to the group.
- Create the content filtering policy and then create a policy group and apply the content filtering policy to the group.
  - Use this method in situations in which new employees or policy groups are added after policies are created.

A content filtering policy is automatically enabled when you create it. If you do not want to use the content filtering policy yet, disable it.
To specify the policy groups for which content policies apply

1. Under Policy Groups, check one or more groups to which this policy should apply.
2. Click Save.
3. After you create your content filtering policy, specify the order in which you want the policy evaluated.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.

Tips for testing a content filtering policy

When you add a new content filtering policy, you should run tests to make sure the policy filters as expected. Testing is particularly important when the policy includes a destructive action such as Delete message. You may also want to run tests when you make a meaningful change to an existing policy.

Here are some suggestions for testing a content filtering policy:

1. Create the policy with the conditions that you want.
2. Add at least one action that you can track easily. For example, you can:
   - Select the Add a header action and add a custom header. You can then monitor the message headers to determine which messages trigger a verdict for the policy.
   - Select the Create an informational incident action. Each time the policy triggers a verdict, SMG adds an informational incident that you can view.
3. Assign the policy to a test policy group. Or, if you assign the policy to policy groups in your production environment, do not include destructive actions in the policy before you complete your testing.
4. Send test emails that challenge the policy. Include test emails that you do not expect to trigger a verdict.
5. When you are satisfied that the policy works as expected, edit the policy to include the final actions that you want to assign.

Managing how multiple content filtering policies are applied

Symantec Messaging Gateway evaluates policies in the order in which they appear on the Email Content Filtering Policies page. The policy that appears first in the list is evaluated first; the next policy is evaluated second, and so on. You can drag the policies to different positions to change the order.
How the Subsequent Content Filter Handling setting affects the next policy that triggers a verdict

When a content filtering policy triggers the first verdict, Symantec Messaging Gateway adds all of that policy’s actions to an Action List. SMG uses that policy’s Subsequent Content Filter Handling setting to determine what to do if a second content filtering policy in the list triggers a verdict. The Subsequent Content Filter Handling setting of that second policy determines what SMG does if a third policy triggers a verdict, and so on. The following table describes each setting and its effect.

<table>
<thead>
<tr>
<th>If the previous policy that triggered has the setting:</th>
<th>Symantec Messaging Gateway does this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue with Evaluations &amp; Actions</td>
<td>Continues to evaluate the remaining content filtering policies. If another content filtering policy triggers a verdict, SMG adds the actions for that policy. SMG then uses the Subsequent Content Filter Handling setting for the newly-triggered policy to determine what to do next.</td>
</tr>
<tr>
<td>Provide Incidents and Notifications Actions Only</td>
<td><strong>Note:</strong> This setting is provided for legacy support and is not recommended. Adds only Create an informational incident and Send a notification actions to the list. Changes Create a quarantine incident to Create an informational incident, if the policy has that action. Ignores all other actions, and delivers the message normally.</td>
</tr>
<tr>
<td>Halt Evaluations and Actions</td>
<td>Does not evaluate any policies that are lower on the list. Does not add any additional actions to the list.</td>
</tr>
</tbody>
</table>

After all filtering completes, Symantec Messaging Gateway sorts the Action List by action precedence order. When multiple actions conflict, Symantec Messaging Gateway deletes all actions with a lower precedence.

See “Action combinations from multiple verdicts” on page 830.
Examples of how Subsequent Content Filter Handling affects policies and actions

Table 14-6 Examples and results

<table>
<thead>
<tr>
<th>Example</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example 1</td>
<td>Symantec Messaging Gateway evaluates all three policies, and all three policies were violated. Symantec Messaging Gateway modifies the subject line for Policy 1. Policy 1 specifies Provide Incidents and Notifications Actions Only. Policy 2 has the actions Add a header and Create an informational incident. The subsequent policy option is Continue with Evaluation &amp; Actions. Policy 3 has the action Add annotation. The subsequent policy option is Continue with Evaluation &amp; Actions.</td>
</tr>
</tbody>
</table>

Symantec Messaging Gateway modifies the subject line for Policy 1. Policy 1 specifies Provide Incidents and Notifications Actions Only. When Policy 3 triggers a verdict, Symantec Messaging Gateway adds an informational incident, but does not add a header. Policy 2 specifies Continue with Evaluation & Actions. When Policy 3 triggers a verdict, Symantec Messaging Gateway adds the annotation. The result is that Symantec Messaging Gateway modifies the subject line, adds the annotation, creates an informational incident, and delivers the message. |
### Table 14-6  
Examples and results *(continued)*

<table>
<thead>
<tr>
<th>Example</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example 2:</td>
<td>Symantec Messaging Gateway evaluates all three policies, and all three policies were violated.</td>
</tr>
<tr>
<td>■ Policy 1 has the action <strong>Add a header</strong>. The subsequent policy option is <strong>Provide Incidents and Notifications Actions Only</strong>.</td>
<td>For policy 1, Symantec Messaging Gateway adds <strong>Add a header</strong> to the action list.</td>
</tr>
<tr>
<td>■ Policy 2 has the action <strong>Create a quarantine incident</strong>. The subsequent policy option is <strong>Continue with Evaluation &amp; Actions</strong>.</td>
<td>Policy 1 specifies <strong>Provide Incidents and Notifications Actions Only</strong>. When policy 2 triggers a verdict, Symantec Messaging Gateway adds <strong>Create informational incident</strong> to the action list instead of <strong>Create a quarantine incident</strong>.</td>
</tr>
<tr>
<td>■ Policy 3 has the action <strong>Delete message</strong>. The subsequent policy option is <strong>Halt Evaluation &amp; Actions</strong>.</td>
<td>Policy 2 specifies <strong>Continue with Evaluation &amp; Actions</strong>. When Policy 3 triggers a verdict, Symantec Messaging Gateway adds <strong>Delete message</strong> to the action list.</td>
</tr>
<tr>
<td></td>
<td>Policy 3 specifies <strong>Halt Evaluation &amp; Actions</strong>, so Symantec Messaging Gateway does not evaluate any additional content filtering policies.</td>
</tr>
<tr>
<td></td>
<td>When all processing is complete, Symantec Messaging Gateway evaluates the actions. The <strong>Delete message</strong> action overrides the <strong>Add a header</strong> action. The <strong>Delete message</strong> and <strong>Create informational incident</strong> have the same precedence. The result is that Symantec Messaging Gateway deletes the message and creates an informational incident.</td>
</tr>
</tbody>
</table>

| Example 3: | For policy 1, Symantec Messaging Gateway adds **Add a header** to the action list. |
| ■ Policy 1 has the action **Add a header**. The subsequent policy option is **Halt Evaluation & Actions**. | Policy 1 specifies **Halt Evaluation & Actions**, so Symantec Messaging Gateway does not evaluate Policy 2 or Policy 3. |
| ■ Policy 2 has the action **Create a quarantine incident**. The subsequent policy option is **Continue with Evaluation & Actions**. | The result is that Symantec Messaging Gateway adds the header and delivers the message. |
| ■ Policy 3 has the action **Delete message**. The subsequent policy option is **Provide Incidents and Notifications Actions Only**. | |

See “Creating a content filtering policy” on page 325.
How the Message Audit Log helps to fine-tune and troubleshoot content filtering policies

Symantec Messaging Gateway enables you to create content filtering policies to monitor the content of inbound and outbound email messages.

You can also create content filtering polices to do the following:

- Comply with government-mandated regulations.
- Block or hold messages for review based on internal policies.
- Deploy more aggressive rules for blocking certain types of message content.

When users identify missing email or complain about unwanted email reaching their inbox, a number of policies may be involved. It may not be immediately clear how to adjust the appropriate policy to correct the problem. To troubleshoot these issues, you can view the Message audit log.

The Message audit log identifies the text that violated the policy and the part of the message that contained the violation.

For example, configure a content filtering policy to use a regular expression for content matching. You can set the action for the policy to delete the message. You begin receiving complaints about missing email messages. You can troubleshoot the issue by viewing the messages in the Message audit log to see the content that violated the policy. Based on your findings, you can fine-tune your policy as needed.

See “Searching for a message in the Message Audit Log” on page 637.

See “How the matching text feature is affected by upgrade for existing content” on page 449.

See “Content filtering condition match criteria” on page 330.
Filtering content with content filtering resources

This chapter includes the following topics:

■ About content filtering policy resources
■ Using structured data in a content filtering policy
■ About record views
■ Working with content filtering violation notifications
■ Working with dictionaries
■ Using patterns to detect policy violations
■ Creating and managing annotations for policy violations
■ Using lists to detect prohibited attachments
■ Specifying where to save archived messages

About content filtering policy resources

Symantec Messaging Gateway provides the following resources that you can use to create a content filtering policy:

Annotations

You can append text to a message that has violated a policy. The text that you choose depends on the policy. For example, it may advise the recipient that the accompanying email violates company norms and policies for corporate governance.

See “Creating and managing annotations for policy violations” on page 399.
Archive

Some regulations require that you archive any messages that might violate corporate policies. You can send copies of the message that you want to archive to a designated email address on a regular mail server. You can also send copies of the message to an archive server.

See “Specifying where to save archived messages” on page 417.

Attachment lists

Attachment lists are predefined lists based on an attachment’s true file type, MIME-type, or file name extension. An attachment list contains the file extensions and the file application types that you want Symantec Messaging Gateway to detect. You use an attachment list as a condition of a content filtering policy. When Symantec Messaging Gateway detects an attachment that has an extension that is on the file extension list, it applies the action that you specify. Symantec Messaging Gateway can determine the email attachment type based on the application that created it, regardless of its file extension.

See “About attachment lists” on page 401.

Dictionaries

Dictionaries provide lists of the predefined words that you can use when you create policy conditions. For example, you can use dictionaries to detect vulgar language or the language that might suggest a job search.

See “About content filtering dictionaries” on page 382.

Notifications

Symantec Messaging Gateway can send customized notifications to the sender or recipient of an email whenever a policy’s conditions are met. Notifications can be sent with or without the accompanying message. You can also configure the policy to notify the content filtering officer, manager, or the administrator that is charged with enforcing the policy of the violation.

See “About policy violation notifications” on page 377.

Patterns

Patterns are predefined lists of the character patterns that are associated with an object type or data type that you may want to restrict. For example, you can use patterns to screen outgoing messages for credit card numbers by searching for the standard credit card patterns.

See “About patterns” on page 395.

Records

A record consists of the structured data that your organization provides. Structured data contains the company-specific, delimited data that you want to protect. You can create views of records to use in content filtering policies that detect whether content in your data source file is in messages. Content can be detected in both incoming email messages and outgoing email messages. If the contents in the incoming or outgoing mail match the data defined in your data source record, you can specify the action that you want Symantec Messaging Gateway to take.

See “Using structured data in a content filtering policy” on page 354.
Using structured data in a content filtering policy

Table 15-1 describes the process to use structured data in a content filtering policy.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Decide which Structured Data policy template you intend to use to create your content filtering policy.</td>
<td>The pattern fields in your data source file must correspond to the data types that your Structured Data policy template uses. For example, assume that you want to create a policy with the Customer Data Protection template. You should use the pattern fields that correspond to social security number, credit card number, phone, and email.</td>
</tr>
<tr>
<td>2</td>
<td>Obtain a data source file from your database administrator.</td>
<td>Structured data is comprised of a data source file that your company provides. This file consists of columns of the company-specific, delimited data that you want to protect. See “About your data source files” on page 355.</td>
</tr>
<tr>
<td>3</td>
<td>Create a record.</td>
<td>When you create a record, you specify a name for the record, a description (optional), data source attributes, and the processing error threshold. See “Creating a record for structured data” on page 358.</td>
</tr>
<tr>
<td>5</td>
<td>Upload your data source file.</td>
<td>Symantec Messaging Gateway validates the file when you upload it and lets you know if the upload is successful. If the upload is successful, Symantec Messaging Gateway indexes the file. If the upload is unsuccessful, an error message appears that indicates the reason for failure. See “Uploading data source files” on page 366.</td>
</tr>
</tbody>
</table>
Table 15-1  How to use structured data in a policy *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Replicate the record.</td>
<td>You must replicate the record to all attached and enabled Scanners before you can use it in content filtering policies. Replicating data source files to your Scanners can be time consuming. You might want to wait to replicate the record during off-peak times. See “Replicating records” on page 367.</td>
</tr>
<tr>
<td>7</td>
<td>Define one or more views for a record.</td>
<td>A view lets you specify which fields in a record you want Symantec Messaging Gateway to search for when it evaluates a message. You also specify how many of those fields must be in a message to constitute an occurrence. You can have one or more views for a record. For example, one view might contain the Credit Card number pattern, the Email address pattern, and the IP address pattern. Another view for that same record might consist of the Credit Card number pattern, the US Phone pattern, and the US ZIP Code pattern. Multiple views let you create multiple content filtering policies from a single record or multiple conditions for the same policy. You must define at least one view before you can use the record in content filtering policies. See “Creating record views” on page 373. See “Editing record views” on page 374.</td>
</tr>
<tr>
<td>8</td>
<td>Create a content filtering policy with a Structured Data policy template.</td>
<td>You must use a Structured Data policy template or a blank template to use a record view as a policy condition. See “Creating a content filtering policy” on page 325.</td>
</tr>
<tr>
<td>9</td>
<td>Configure the policy to use a record view as a condition.</td>
<td>In the content filtering policy, you specify how many occurrences must take place to violate the policy. See “Defining conditions for a content filtering policy” on page 327.</td>
</tr>
</tbody>
</table>

**About your data source files**

To use structured data in content filtering policies, you must obtain a data source file from your database administrator.

*Table 15-2* describes the requirements and considerations that you should know about your data source file.
### Table 15-2 Data source file requirements and considerations

<table>
<thead>
<tr>
<th>Requirement or consideration</th>
<th>Description</th>
</tr>
</thead>
</table>
| Only one word per delimited field consisting of at least two alphanumeric characters | Each entry must contain at least two alphanumeric characters. Single character entries in a field are unsupported.  
Also, a data source file can only have a single word per delimited field. For example, if you want to match the data "1st Street", place "1st" in one delimited field. Place "Street" in a separate (but following) field. If you place two or more words in a field, a match is less likely.  
For example, if you place the string "1st Street" in a single delimited field, you have placed multiple "words" in the same cell. A match is then unlikely since the only match that is expected would be when the data that is examined is in a tabular format. In a tabular format, the two strings (1st) and (Street) are evaluated as one string (1st Street). Similar behaviors exist when you try to match any languages that recognize white spaces differently, such as Korean or Chinese. |
| Only specific separators are recognized for credit card and number patterns | Symantec Messaging Gateway recognizes only certain separator characters when it attempts to match record entries in credit card and number pattern fields.  
The recognized separator characters (other than space) for credit card and number pattern fields are as follows:  
- Tab  
- Comma (,)  
- Pound sign (#)  
- Hyphen (-)  
- Plus sign (+)  
- Pipe (|)  
- Semicolon (;)  
- Colon (:)  
Symantec Messaging Gateway interprets any numbers that contain an unrecognized separator as a word. For example, 4123*6666*7777*8888 would not return a valid match against a credit card number field. Symantec Messaging Gateway interprets this content as the word: 4123*6666*7777*8888. |
<table>
<thead>
<tr>
<th>Requirement or consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a delimiter other than commas to separate adjacent number patterns</td>
<td>Use a tab or pipe (</td>
</tr>
<tr>
<td></td>
<td>For example, assume that you have adjacent fields: Age and Weight. And assume that you have separated the fields for Age and Weight by a comma; for example: 25,150. Symantec Messaging Gateway might interpret 25,150 as belonging to the Age field instead of 25 belonging to the Age field and 150 belonging to the Weight field.</td>
</tr>
<tr>
<td>Data source file must have the minimum number of columns required by the Structured Data template</td>
<td>Ensure that your data source file contains the columns that you want to use to define a view. For example, assume that you use a Structured Data policy that calls for a minimum of three fields to trigger a violation. Those three fields must be mapped in the record so that Symantec Messaging Gateway can reference them.</td>
</tr>
<tr>
<td></td>
<td>For example, assume that you use the EU Data Protection Directives policy template. Any view that accesses the EU Data Protection Directives policy should be configured to match entries in at least four of five fields: Last name, email, phone, account number, and user name.</td>
</tr>
<tr>
<td></td>
<td>See “Creating record views” on page 373.</td>
</tr>
<tr>
<td>Pattern fields should match the data types that are used in the policy template</td>
<td>The pattern fields must correspond to the data types that your Structured Data policy template uses. For example, assume that you want to create a policy with the Customer Data Protection template. You should use the pattern fields that correspond to Social Security number, credit card number, phone, and email columns.</td>
</tr>
<tr>
<td>Mappings must match header row columns</td>
<td>If the mappings in your record do not match the columns in the header row, Symantec Messaging Gateway counts the actual header row as invalid. The header row is considered invalid because it returns values other than those expected.</td>
</tr>
<tr>
<td></td>
<td>See “About mapping your data source file columns” on page 361.</td>
</tr>
<tr>
<td>Credit card numbers must pass the Luhn checksum test</td>
<td>All credit card numbers must pass the Luhn checksum test, where total modulus 10 is congruent to 0, to produce a match. The Luhn test is used to distinguish valid numbers from random collections of digits.</td>
</tr>
</tbody>
</table>
Table 15-2 Data source file requirements and considerations (continued)

<table>
<thead>
<tr>
<th>Requirement or consideration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRLF line breaks that precede rows in a data source file are included in row counts</td>
<td>If the data source file does not contain CRLFs, Symantec Messaging Gateway skips the header row in the row count. If a data source file contains CRLFs, Symantec Messaging Gateway treats the first CRLF as the header row. So it returns the values from subsequent rows, including those for the actual header row. For example, assume that one column is mapped to recognize the US ZIP code pattern and one or more CRLFs begin the data set. Symantec Messaging Gateway counts the actual header row as a normal row. It expects to return a 5-digit number in that column. When the actual header row returns a word value instead of a 5-digit number, Symantec Messaging Gateway counts it as an invalid row. Symantec Messaging Gateway ignores the CRLFs that occur within a data set or at the end of a data set. Such CRLFs are not counted as rows.</td>
</tr>
<tr>
<td>Rows that occur more than 99 times are not matched</td>
<td>Because of implementation limitations, Symantec Messaging Gateway cannot match any rows that occur more than 99 times.</td>
</tr>
</tbody>
</table>

See “Using structured data in a content filtering policy” on page 354.

Creating a record for structured data

After you obtain a data source file, you can create a record.

See “About your data source files” on page 355.

When you create a record, you define the following criteria:

Name and description | Specify a name and description for your record. Select a name that identifies the data that the record contains. A description for your record is optional. If you change the name of a record, all conditions that reference views of that record reflect the name change. See “Modifying records” on page 368.
Data source attributes  Specify the delimiter that your data source file uses. The supported delimiter characters are tab, comma (","), or pipe ("|").

Also indicate whether your data source file contains a header row. The header row is neither processed nor included in the record.

You do not need to check the Data source file contains a header row box if you define all fields as system patterns.

See “Mapping data source file columns to fields in Symantec Messaging Gateway” on page 360.

Error threshold  Set Maximum Allowable Errors to a percentage of the total rows that can safely return errors when you upload the data source file and still continue processing. Setting a percentage that is too low may make it difficult to complete processing an otherwise useful data source file. Setting a percentage that is too high may hide the fact that the record file is partially corrupted.

To create a record, you must have Full Administration rights or rights to modify settings.

To create a record for structured data

1  In the Control Center, click Content > Resources > Records.

2  Click Add.

3  In the Record Resource Name field, type a name for the record.

4  In the Optional description field, type a description for the record.

5  Under Data Source Attributes, click the Delimiter drop-down list and select the appropriate delimiter character for your data source file.

6  Check the Data source file contains a header row checkbox if your data source file contains a header row.

7  Under Error Threshold, type the maximum allowable percentage of errors that can occur before processing is halted.

After you define your record, map your data source file columns to fields in Symantec Messaging Gateway.

See “Mapping data source file columns to fields in Symantec Messaging Gateway” on page 360.
Mapping data source file columns to fields in Symantec Messaging Gateway

After you define a record, map the columns in your data source file to fields in Symantec Messaging Gateway. You can use predefined system pattern fields, or you can create custom fields.

See “Creating a record for structured data” on page 358.

See “About mapping your data source file columns” on page 361.

See “Using structured data in a content filtering policy” on page 354.

To map a data source file, you must have Full Administration rights or rights to modify settings.

To map data source file columns to fields in Symantec Messaging Gateway

1. On the Add Record Resource page, under Mapping, click the Field Names drop-down list and do one of the following tasks:

   - To use a system pattern field: Select the system pattern that you want to associate with the corresponding column in your data source file. For example, if column 1 in your data source file consists of phone numbers, in column 1, select US phone pattern. See “System patterns” on page 362.

   - To create your own custom field: Select Customize, and in the adjacent text field, type a unique custom field name. Custom field names cannot be the same as any of the predefined list of field names. Nor can they be the same as any other custom field name in the record. For example, assume column 3 of your data source file consists of first names. In column 3, select Customize and in the adjacent box, type first name.

2. To change the order of the fields, check the box beside the field name that you want to move, and then click Move Up or Move Down.

3. To add additional fields, click Add and repeat the tasks in step 1 to use a system pattern or to create your own custom field.

4. Click Next.

   After you map your data source file columns, upload the data source file.

   See “Uploading data source files” on page 366.
About mapping your data source file columns

Patterns are the named regular expressions or system patterns that describe a commonly known data object, such as the pattern for credit card numbers. You must map the pattern of each column in your data source file to corresponding fields in Symantec Messaging Gateway.

Table 15-3 describes the field types that you can use to map your data source file.

### Table 15-3  Field types

<table>
<thead>
<tr>
<th>Field type</th>
<th>Description</th>
</tr>
</thead>
</table>
| System patterns  | Symantec Messaging Gateway matches data in each column of your data source file with a system pattern. A set of regular expressions defines a system pattern. Data in your data source file must conform to one of the regular expressions for a data file to be successfully uploaded and indexed. The system patterns are as follows:  
- Credit card number pattern  
- Email pattern  
- IP address pattern  
- Number pattern  
- Percent pattern  
- US phone pattern  
- US ZIP code pattern  
- SSN/ITIN pattern  

See “System patterns” on page 362. |
| Customized       | If data in your data source file does not fall into one of the system pattern categories, you can create a customized field. Symantec Messaging Gateway only recognizes a customized field as a WORD pattern. Customized fields are not indexed nor are they validated. 

Symantec recommends that you make the customized field names similar to the field names in your data source file. For example, if the first field in your data source file is first_name, then you could name the corresponding field in Symantec Messaging Gateway first_name. Custom field names cannot be the same as any of the predefined list of field names. Nor can they be the same as any other custom field name in the record. |

Table 15-4 provides an example of how a data source file is mapped.

### Table 15-4  Data source file mapping example

<table>
<thead>
<tr>
<th>Data source file column</th>
<th>Data that is contained in data source file column</th>
<th>Symantec Messaging Gateway column</th>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Credit card numbers</td>
<td>1</td>
<td>Credit card number pattern</td>
</tr>
</tbody>
</table>
### Table 15-4 Data source file mapping example (continued)

<table>
<thead>
<tr>
<th>Data source file column</th>
<th>Data that is contained in data source file column</th>
<th>Symantec Messaging Gateway column</th>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Email addresses</td>
<td>2</td>
<td>Email pattern</td>
</tr>
<tr>
<td>3</td>
<td>First names</td>
<td>3</td>
<td>Customize</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Customized field name: first_name</td>
</tr>
<tr>
<td>4</td>
<td>Last names</td>
<td>4</td>
<td>Customize</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Customized field name: last_name</td>
</tr>
</tbody>
</table>

See “About your data source files” on page 355.

See “Mapping data source file columns to fields in Symantec Messaging Gateway” on page 360.

See “Using structured data in a content filtering policy” on page 354.

### System patterns

Table 15-5 describes the system patterns that you can use to map your data source file columns to Symantec Messaging Gateway.
<table>
<thead>
<tr>
<th>System pattern</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card number</td>
<td>5369 7777 8888 9999</td>
<td>MasterCard: Any 16-digit number that begins with 5 and whose second digit is a number from 1 to 5, separated into four groups of four by spaces or hyphens.</td>
</tr>
<tr>
<td></td>
<td>5369-7777-8888-9999</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4567 1234 5678 9123</td>
<td>VISA: Any 16-digit number that begins with 4 and separated into four groups of four digits that are separated by a space or hyphen, or any 12-digit number that begins with 4.</td>
</tr>
<tr>
<td></td>
<td>4123-6666-7777-8888</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4123456789012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3442 456789 12345</td>
<td>American Express: Any 15-digit number that begins with 34 or 37 and separated into three groups of 4, 6, and 5 digits, respectively, by spaces or hyphens.</td>
</tr>
<tr>
<td></td>
<td>3758 456789 12345</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3056 123456 7890</td>
<td>Diners Club card: Any 15-digit number that begins with 30, 36, or 38 and separated into three groups of 4, 6, and 5 digits, respectively, by spaces or hyphens.</td>
</tr>
<tr>
<td></td>
<td>3667 123456 7890</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3878 123456 7890</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3056-123456-7890</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3667-123456-7890</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3842-123456-7890</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6011 1234 5678 9012</td>
<td>Discover card: Any 16-digit number that begins with 6011 and separated into groups of 4 by spaces or hyphens.</td>
</tr>
<tr>
<td></td>
<td>6011-1234-5678-9012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2014 123456 78901</td>
<td>Enroute card: Any 15-digit number that begins with 2014 or 2149 separated into groups of 4, 6, and 5 by spaces or hyphens.</td>
</tr>
<tr>
<td></td>
<td>2149-123456-78901</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3123 4567 8901 1234</td>
<td>JCB: Any 16-digit number that is separated into four groups of four by a space or hyphen and begins with 3; or any 15-digit number that begins with 2131 or 1800 and is followed by 11 digits.</td>
</tr>
<tr>
<td></td>
<td>3123-4567-8901-1234</td>
<td></td>
</tr>
<tr>
<td></td>
<td>213112345678901</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1800123245678901</td>
<td></td>
</tr>
</tbody>
</table>
### Table 15-5  System patterns (continued)

<table>
<thead>
<tr>
<th>System pattern</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>jabberwocky @symantec.com</td>
<td>Any alphanumeric string, that is divided by an underscore (_), hyphen (-), or period, followed by the @ sign and an alphanumeric string, a period, and one of the domain-name extensions listed. Symantec Messaging Gateway cannot validate top-level domains of two letters, where one or both letters are uppercase. It does, however, validate uppercase three-letter domains. For example, it does not validate <a href="mailto:harry@hogwarts.edu.UK">harry@hogwarts.edu.UK</a> or <a href="mailto:bilbo@canterbury.ac.Nz">bilbo@canterbury.ac.Nz</a>. However, Symantec Messaging Gateway validates mister_smith @senate.GOV.</td>
</tr>
<tr>
<td></td>
<td>mister_smith @senate.gov</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:tom.swift@gadgets.arpa">tom.swift@gadgets.arpa</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:t-rex9@nature.museum">t-rex9@nature.museum</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:harry@hogwarts.edu.uk">harry@hogwarts.edu.uk</a></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>1.2.3.4</td>
<td>Any grouping of four-digit numbers that start with three 1-, 2-, or 3-digit numbers less than 256 separated by periods. A CIDR address range can be indicated by a 1- or a 2-digit number from 0 to 32 inclusive and separated from the initial IP address by a forward slash. Symantec Messaging Gateway does not parse any terminal characters other than a 1- or 2-digit numeral that is preceded by a forward slash. Thus, 10.113.14.10a is not interpreted as a valid IP address.</td>
</tr>
<tr>
<td></td>
<td>10.0.0.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18.255.30.41</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.0.10.0/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.0.10.0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.0.10.0/0</td>
<td></td>
</tr>
</tbody>
</table>
Table 15-5  System patterns (continued)

<table>
<thead>
<tr>
<th>System pattern</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>10</td>
<td>Symantec Messaging Gateway recognizes European-style numbers, where the comma serves as decimal point and periods separate groups of three digits. Fractions must be preceded by a numeral, including zero (0) if necessary, and expressed as a decimal. Although numbers 8 digits or smaller with commas are supported, Symantec recommends that you use tab- or pipe-delimited data-source text files that contain numbers using commas. The use of the tab or pipe delimiters avoids the possibility that commas in numbers are mistaken as field delimiters. Numbers that are larger than eight digits are interpreted as of type WORD.</td>
</tr>
<tr>
<td></td>
<td>10.99</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.33</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9999</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.999,66</td>
<td></td>
</tr>
<tr>
<td></td>
<td>99,999.999</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-9,999</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-10.99</td>
<td></td>
</tr>
<tr>
<td>Percent</td>
<td>76%</td>
<td>Symantec Messaging Gateway recognizes European-style numbers, where the comma serves as decimal point and periods separate groups of three digits. Fractions of a percent must be preceded by a numeral, including zero (0) if necessary, and expressed as a decimal. Only the numbers that are adjacent to the percent sign (%) (no space) are regarded as valid percentages. The following patterns do not produce a match: .32 32 percent 32per 5 3/4%</td>
</tr>
<tr>
<td></td>
<td>23.4%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>56.78%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-1.089,01%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-0.32%</td>
<td></td>
</tr>
</tbody>
</table>
### Table 15-5  System patterns (continued)

<table>
<thead>
<tr>
<th>System pattern</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>US phone</td>
<td>(238) 832 5555</td>
<td>Any 10-digit phone number beginning with 2-9 and/or preceded by 1 followed by a hyphen or a space-hyphen-space. The 3-digit area code can be enclosed in parentheses or not, followed by a space, hyphen, or period and the 7-digit number grouped into 3 and 4 digits that are separated by a space, hyphen or period or not separated at all.</td>
</tr>
<tr>
<td></td>
<td>(238) 832-5555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238-832-5555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238 8325555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1-238-832-5555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238.832.5555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 - (238) 8325555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 - (238) 832-5555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 - (238) 832 5555</td>
<td></td>
</tr>
<tr>
<td>US ZIP code</td>
<td>90210</td>
<td>Any 5-digit ZIP code or combination of 5-digit code plus 4-digit extension that are separated by a hyphen.</td>
</tr>
<tr>
<td></td>
<td>89412-4321</td>
<td></td>
</tr>
<tr>
<td>SSN/ITIN</td>
<td>777-77-7777</td>
<td>Any 9-digit number, either continuous or separated into 3 groups of 3, 2, and 4 digits that are separated by a hyphen or space. The first group of three digits cannot be 000. The second number group must be greater than or equal to one, and the last number group must be greater than zero.</td>
</tr>
<tr>
<td></td>
<td>777 77 7777</td>
<td></td>
</tr>
<tr>
<td></td>
<td>123456789</td>
<td></td>
</tr>
</tbody>
</table>

See “About mapping your data source file columns” on page 361.

See “Mapping data source file columns to fields in Symantec Messaging Gateway” on page 360.

## Uploading data source files

After you map your data source file columns, you must upload your data source file. If the upload is unsuccessful, an error message appears that indicates the reason for failure. If upload is successful, Symantec Messaging Gateway indexes the record. Indexing records helps Symantec Messaging Gateway find rows in your data source file faster than if the record were not indexed.

See “Mapping data source file columns to fields in Symantec Messaging Gateway” on page 360.

See “Modifying records” on page 368.

The **Record Resource Status** page shows the status of the upload process. It displays the time that the upload process starts and finishes. It also indicates the number of rows that were successfully uploaded and unsuccessfully uploaded.
Uploading a large data source file can be processing-intensive and time consuming. Consider uploading data source files during off-peak hours.

Note: Symantec Messaging Gateway does not support uploading a data source file that is larger than 1.5 GB.

To upload a record, you must have Full Administration rights or rights to modify settings.

To upload data source files

1. On the Edit Record Resource page, under Record Resource Data Source, click Browse to locate the data source file that you want to upload.
2. Click Upload.

After you successfully upload a record, you must then replicate it to your Scanners.

See “Replicating records” on page 367.

Replicating records

After you successfully upload your data source file, you must replicate it to all of your Scanners. Transferring a large record to one or more Scanners can take a significant amount of time and processing resources. So Symantec Messaging Gateway lets you replicate records when you create a new record or at a later time.

See “Uploading data source files” on page 366.

The Record Resource Status page indicates the status, the time the replication started and finished, and the size of the record that was replicated.

To replicate records, you must have Full Administration rights or rights to modify settings.

To replicate records when you create a new record

1. On the Record Resource Status page, under Processing Status, ensure that the status is Completed.
2. Under Replication Status, click Replicate Now.
3. When replication is successfully completed, click OK.

To replicate records at a later time

1. In the Control Center, click Content > Resources > Records.
2. Check the box beside the record that you want to replicate, and then click Status Details.
3 If the **Record Resource Status** page shows that the data source file is uploaded, under **Replication Status**, click **Replicate Now**.

If the status is **Upload Failed**, you must try to upload your data source file again before you can replicate it.

See “Uploading data source files” on page 366.

4 Click **OK**.

To cancel the replication of a Record resource to all enabled Scanners, click **Cancel Replication**.

After you replicate the record, create a view.

See “About record views” on page 369.

See “Creating record views” on page 373.

### Modifying records

You can modify a record, provided that no upload of the record is in progress or pending. When you modify a record, you must upload and replicate the record again.

Policies that reference a record's views continue to use that record's existing data until Symantec Messaging Gateway uploads, indexes, and replicates the new data. If you change the name of a record, all conditions that reference views of that record reflect the name change.

In addition, if you modify any mappings, any existing views that a policy condition references remains valid during the update. After the updated record is uploaded and replicated, all previously defined policies remain valid. The new column fields are available to create views.

You cannot delete a named field from a record if it is part of any existing view. This restriction applies whether or not a policy condition references that view. If you attempt to delete such a field, Symantec Messaging Gateway displays an error message at the top of the **Edit Record Resource** page.

See “Using structured data in a content filtering policy” on page 354.

See “Deleting records” on page 369.

### To modify records

1 In the Control Center, click **Content > Resources > Records**.

2 Check the box beside the record that you want to modify and click **Edit**.

   You can also click on the name of the record to edit it.

3 On the **Edit Record Resource** page, make the desired changes and then click **Next**.

   See “Creating a record for structured data” on page 358.
4 On the Edit Record Resource page, under Record Resource Data Source, click Browse to locate the data source file that you want to upload.

5 Click Upload.

See “Uploading data source files” on page 366.

6 On the Record Resource Status page under Processing Status, ensure that the status is Completed.

7 Under Replication Status, click Replicate Now.

8 When replication is successfully completed, click OK.

See “Replicating records” on page 367.

Deleting records

To delete the record, you must first delete any of the record's views from all content filtering policy conditions. The Record Resource Views page lists all of the views that you have created. This page indicates the number of fields that you have selected for the view. It also shows the number of policies that use that view as a condition. However, this page does not indicate which policies use the views. Symantec Messaging Gateway lets you know which policies use the views for that record when you attempt to delete it.

To delete records, you must have Full Administration rights or rights to modify settings.

To delete records

1 In the Control Center, click Content > Resources > Records.

2 Check the box beside the record that you want to remove and click Delete.

A message appears at the top of the page indicating which content filtering policies use the views that are created from this record. Delete or modify this condition in these policies first, then repeat this procedure.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.

See “Deleting record views” on page 375.

See “Using structured data in a content filtering policy” on page 354.

About record views

You must create record views to use in a content filtering policy condition. You use views to specify which fields or combinations of fields in a record you want Symantec Messaging Gateway to match in a message.

You can create one or more views from a record. The benefit of multiple views is that you can create several conditions for a policy, and each condition can use a different view. Multiple
views also let you use the same record for several different policies, and each policy can use a different view.

The **Record Resource Views** page lists all of the views that you have created. This page indicates the number of fields that you have selected for the view. It also shows the number of policies that use that view as a condition.

**Table 15-6** describes the options that you use to create a view. It also provides an example. For the sake of our example, assume that Record A exists. Also assume that Record A and View A are used in a content filtering policy that is enabled.

Table 15-6  How to configure a record view

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Name</td>
<td>You should specify a unique name that describes the purpose of the view.</td>
<td>In our example, the view is named View A.</td>
</tr>
<tr>
<td>Field Selection</td>
<td>When you create a view, all of the fields that you mapped for that record appear in the <strong>Fields</strong> list on the <strong>Add Record Resource page</strong>. You specify which fields you want to use in the view.</td>
<td>Assume that Record A consists of the following fields:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Credit card number pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Email pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IP address pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Number pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Percent pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ US phone pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ US ZIP code pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ SSN/ITIN pattern</td>
</tr>
<tr>
<td></td>
<td>Now assume that you select the following fields for this view:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Credit card number pattern</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Email pattern</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ IP address pattern</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ US phone pattern</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ US ZIP code pattern</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SSN/ITIN pattern</td>
<td></td>
</tr>
</tbody>
</table>
Table 15-6  How to configure a record view (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of matched selected fields required for an occurrence</td>
<td>This option specifies how many of the fields in your view must appear in a message to constitute an &quot;occurrence.&quot; For example, assume that you select six fields for your view, and the Minimum number of matched selected fields required for an occurrence is four. If any of the four (or more) fields that you selected are found in a message, Symantec Messaging Gateway considers it an occurrence. An occurrence is not a violation. When you create a policy that uses this view, you can specify how many occurrences can occur in a message before the policy is violated. See &quot;Using structured data in a content filtering policy&quot; on page 354.</td>
<td>Assume that you specify the Minimum number of matched selected fields required for an occurrence as three. A message that meets or exceeds three matches is considered an occurrence. So if the only match in a message is Email address pattern, there is no occurrence. If the only match in a message is Email address pattern and US phone pattern, there is no occurrence. However, if a message contains matches for Email address pattern and US phone pattern, and SSN/ITIN pattern, the result is an occurrence.</td>
</tr>
</tbody>
</table>
### Table 15-6  How to configure a record view (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| Exception Combinations | Specific combinations of fields may be acceptable in a message. So Symantec Messaging Gateway lets you exclude the combination of fields from being considered a match. You can create multiple exceptions. | Assume that you create an exception that consists of **US phone pattern** and **Email address pattern**. If Symantec Messaging Gateway detects this combination of fields in a message, it does not consider it an occurrence. **Example 1**

A message contains the following matches:

- **Email address pattern**
- **US phone pattern**
- **SSN/ITIN pattern**

No occurrence is detected because the combination of **US phone pattern** and **Email address pattern** is permitted. Therefore, the only matches are: (1) **SSN/ITIN pattern** and **US phone pattern**, and (2) **SSN/ITIN pattern** and **Email address pattern**. Both matches have only two patterns, which are less than the threshold of three patterns.

**Example 2**

A message contains the following matches:

- **Email address pattern**
- **US phone pattern**
- **SSN/ITIN pattern**
- **US ZIP code pattern**

An occurrence is detected. Though the combination of **US phone pattern** and **Email address pattern** is permitted, their combination with other patterns is not permitted. Hence the matches with the following patterns exists: (1) **Email address pattern**, **SSN/ITIN pattern**, and **US ZIP code pattern**; (2) **US phone pattern**, **SSN/ITIN pattern**, and **US ZIP code pattern**.
Table 15-6  How to configure a record view (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
|        |             | **Example 3**  
A message contains the following matches:  
- US phone pattern  
- SSN/ITIN pattern  
- US ZIP code pattern  
- IP address pattern  
An occurrence is detected. The message contains four matches, which exceed the threshold for an occurrence and none of the matches are an exception. |

See “Using structured data in a content filtering policy” on page 354.
See “About mapping your data source file columns” on page 361.
See “Creating record views” on page 373.

Creating record views

After the record is replicated to the Scanner, you can define a view. A view is used to identify which fields from the associated record to use in a content filtering policy conditions. Symantec Messaging Gateway uses views (not records) to create policy conditions, so you must create at least one view per record.

See “Replicating records” on page 367.
See “About record views” on page 369.
See “Editing record views” on page 374.

To create views

1. In the Control Center, click Content > Resources > Records.
2. On the Records page, check the box beside the record for which you want to create a view.
3. Click Views.
5. In the View Name field, type a unique name for the view.
6. Under Field Selection, check the fields that you want to include in this view.
In the Minimum number of matched selected fields required for an occurrence box, specify the number of fields that must be matched in a message to create an occurrence.

To create an exception, under Exception Combinations, click Add.

Select the combination of fields that you want omitted from the match evaluation.

Click Save.

On the Add Record Resource page, click Save.

After you create a view, you can use it in a content filtering policy condition.

See “Creating a content filtering policy” on page 325.

Editing record views

You can modify a view at any time. You can also add, edit, or delete Exception Combinations. When you modify a view, the changes are automatically propagated to any content filtering policies that you have that use that view.

See “About record views” on page 369.

See “Creating record views” on page 373.

See “Deleting record views” on page 375.

To edit views

1. In the Control Center, click Content > Resources > Records.

2. On the Records page, check the box beside the record that contains the view that you want to edit.

3. Click Views.

4. On the Record Resource Views page, check the box beside the view that you want to edit.

5. Click Edit.

6. Make the desired changes to the name, fields, and the minimum number of matched selected fields required for an occurrence.

7. Do any of the following tasks:

   To add a new Exception Combination

   Do all of the following tasks:

   ■ Under Exception Combinations, click Add.

   ■ Select the combination of fields that you want omitted from the match evaluation.

   ■ Click Save.
To modify an existing Exception Combination

Do all of the following tasks:

- Under Exception Combinations, check the box beside the Exception Combination that you want to edit.
- Click Edit.
- Select the combination of fields that you want omitted from the match evaluation.
- Click Save.

To delete an existing Exception Combination

Do all of the following tasks:

- Under Exception Combinations, check the box beside the Exception Combination that you want to delete.
- Click Delete.

8 On the Record Resource Views page, click Save.

Deleting record views

To delete a view, you must first delete that view from any content filtering policy conditions in which it is used. The Record Resource Views page lists all of the views that you have created. This page indicates the number of fields that you have selected for the view. It also shows the number of policies that use that view as a condition. However, this page does not indicate which policies use the views. Symantec Messaging Gateway lets you know which policies use the view when you attempt to delete it.

See “About record views” on page 369.

See “Deleting records” on page 369.

See “Editing record views” on page 374.

To delete views

1 In the Control Center, click Content > Resources > Records.

2 On the Records page, check the box beside the record that contains the view that you want to delete.

3 Click Views.
4 On the Record Resource Views page, check the box beside the view that you want to delete.

5 Click Delete.

A message appears at the top of the page to indicate the content filtering policies in which a condition to use this view occurs. Delete or modify this condition in these policies first, then repeat this procedure.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.

Working with content filtering violation notifications

Table 15-7 describes what you can do with content filtering violation notifications. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about what content filtering policy violation notifications are.</td>
<td>Notifications are the messages that are sent when a content filtering policy is violated, and the policy action is to Send notification. See “About policy violation notifications” on page 377.</td>
</tr>
<tr>
<td>Create a policy violation notification.</td>
<td>Notifications can be sent to any of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Message sender</td>
</tr>
<tr>
<td></td>
<td>■ Message recipient</td>
</tr>
<tr>
<td></td>
<td>■ Third party (such as an administrator)</td>
</tr>
<tr>
<td></td>
<td>See “Creating policy violation notifications” on page 377.</td>
</tr>
<tr>
<td>Modify an existing policy violation notification as needed.</td>
<td>You can modify predefined and custom policy violation notifications as needed. However, the protocol for the predefined policy violation notifications cannot be changed. See “Editing policy violation notifications” on page 379.</td>
</tr>
<tr>
<td>Delete a policy violation notification when it is no longer needed.</td>
<td>You can delete policy violation notifications when they are no longer needed. To delete a policy violation notification, you must first delete that notification from any content filtering policy actions in which it is used. Symantec Messaging Gateway lets you know which policies use that notification when you attempt to delete it. See “Deleting policy violation notifications” on page 380.</td>
</tr>
</tbody>
</table>
About policy violation notifications

Notifications are the messages that are sent when a policy is violated, and the policy action is to **Send notification**. Notifications are different from annotations in that annotations are added to the message, while a notification is a separate message. When you specify to send a notification, the original message is delivered to the original recipient, unless you specify an additional action to do otherwise. Notifications can be used for any type of policy. You can select the notation that you want to use when you specify the action for a policy.

See “Adding actions to a content filtering policy” on page 332.

See “Policy actions and what they do” on page 333.

Symantec Messaging Gateway provides several predefined notifications that you can use. You can also create your own notification message. Predefined notifications can be modified and can only be deleted if they are not used in a policy.

Notifications can be sent to any of the following people:

- Message sender
- Message recipient
- Third party (such as an administrator)

You can customize the notification message subject and body text with variables. For example:

```
The message concerning $subject$ sent by $sender$ to $recipients$ was stripped of $attachments$.
```

See “Creating policy violation notifications” on page 377.

Creating policy violation notifications

Notifications are the predefined messages that SMG sends when a message meets the policy conditions and the action is to send a notification. When you create a notification, the notification name that you specify appears on the **Notifications** page. This name also appears in the **Notification** list when you choose the **Send notification** action for a reputation, spam, malware, threat defense, or content filtering policy.

See “Adding actions to a content filtering policy” on page 332.

Notification recipients can reply to the email address that sends the notification. Replies go to the address that is the envelope address, not the From: header address. As a best practice, either provide an email address for an account that is monitored or include a statement in the notification that responses are not monitored.

Email notification variables let you customize your notification subject text and body text. You can use one or more notification variables in your text, or none at all.
Table 15-8 lists the notification variables that you can use to customize your message subject text and body text and what the tags are replaced with.

Table 15-8  Email notification variable attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Variable tag</th>
<th>Message Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>$sender$</td>
<td>In the delivered notification message, this variable tag is replaced with the sender's email address.</td>
</tr>
<tr>
<td>Recipients</td>
<td>$recipients$</td>
<td>In the delivered notification message, this variable tag is replaced with a comma-separated list of recipient email addresses.</td>
</tr>
<tr>
<td>Subject</td>
<td>$subject$</td>
<td>In the delivered notification message, this variable tag is replaced with the subject line of the original message.</td>
</tr>
<tr>
<td>Attachment names</td>
<td>$attachments$</td>
<td>In the delivered notification message, this variable tag is replaced with a comma-separated list of top-level attachments from the original message.</td>
</tr>
<tr>
<td>Message ID</td>
<td>$messageid$</td>
<td>In the delivered notification message, this variable tag is replaced with the message ID of the original message.</td>
</tr>
</tbody>
</table>

Note: This variable does not appear in the Include message attribute (optional): menu. To add it to a notification, you must type the variable tag into the notification subject or body text.

The message ID is most useful in notifications to administrators. An administrator can use the message ID to quickly track down other information about the message as it passed through the systems.

To create a notification, you must have Full Administration rights or rights to modify policies. See “About policy violation notifications” on page 377.

To create policy violation notifications

1  In the Control Center, click Content > Resources > Notifications.
2  Click Add.
3  In the Notification description box, type a name for the notification.
   Your description cannot exceed 255 characters.
4 In the **Send from** box, type an email address to appear in the **From** header of the notification message.

Specify the full email address including the domain name, such as admin@symantecexample.com.

5 Under **Send to**, select one or more of the following options:

- **Sender**
  Check this box to send the notification to the sender that is listed in the message envelope (not the sender that is listed in the **From:** header).

- **Recipients**
  Check this box to send the notification to the recipients that are listed in the message envelope (not the recipients that are listed in the **To:** header).

- **Others**
  Check this box to send the notification to one or more complete email addresses that you specify. Then type the email address. Separate multiple email addresses with a comma, semicolon, or space.

6 Under **Subject**, click the **Encoding** drop-down list to change the character encoding for the notification subject line.

7 Optionally, click the **Include message attribute** drop-down list to select the type of variable you want to include in the subject line, and then click **Add**.

The variable appears in the **Subject** text box.

8 In the **Subject** text box, type the text for the subject header of the notification message.

9 Under **Body**, click the **Encoding** drop-down list to change the character encoding for the notification body.

10 Optionally, click the **Include message attribute** drop-down list to select the type of variable you want to include in the body, and then click **Add**.

The variable appears in the **Message body** text box.

11 In the **Message body** text box, type the text for the body of the notification message.

12 Optionally, check **Attach the original message** to attach the original message to the notification message.

13 Click **Save**.

**Editing policy violation notifications**

You can modify predefined and custom policy violation notifications as needed. However, the protocol for the predefined policy violation notifications cannot be changed.

To edit a policy violation notification, you must have Full Administration rights or rights to modify policies.
To edit policy violation notifications

1. In the Control Center, click **Content > Resources > Notifications**.
2. Check the box beside the notification that you want to edit.
3. Click **Edit**.
   - You can also click on the notification that you want to edit.
4. Make the desired changes.
5. Click **Save**.

Deleting policy violation notifications

You can delete policy violation notifications when they are no longer needed. To delete a policy violation notification, you must first delete that notification from any content filtering policy actions in which it is used. Symantec Messaging Gateway lets you know which policies use that notification when you attempt to delete it.

To delete a policy violation notification, you must have Full Administration rights or rights to modify policies.

To delete policy violation notifications

1. In the Control Center, click **Content > Resources > Notifications**.
2. Check the box beside the notification that you want to delete.
3. Click **Delete**.
   - A message appears at the top of the page to indicate the content filtering policies in which an action to use this notification occurs. Delete or modify this action in these policies first, then repeat this procedure.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.
See “About policy violation notifications” on page 377.

Working with dictionaries

You can use dictionaries of prohibited words and apply them to content filtering policy conditions. Table 15-9 describes all the ways that you can work with content filtering dictionaries. You can perform any task as needed in any order.
### Table 15-9 Work with dictionaries

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how Symantec Messaging Gateway uses dictionaries in content filtering policy rules.</td>
<td>A dictionary is a list of the words, phrases, file names, and the file name extensions that pertain to a specific topic. When a dictionary is part of a content filtering policy condition, Symantec Messaging Gateway searches your email messages for the contents of the dictionary. See “About content filtering dictionaries” on page 382. See “Considerations when you use dictionaries” on page 384. See “Premium and custom content filtering dictionaries” on page 391.</td>
</tr>
<tr>
<td>Scan text files against content in dictionaries.</td>
<td>Symantec Messaging Gateway can check any file attachments that are not plain text files against dictionaries. Scanning non-plain text files maximizes the effect of content filtering, but it can affect the system load and slow performance. See “Scanning non-plain text file attachments for content filtering violations” on page 385.</td>
</tr>
<tr>
<td>Import or export words or phrases into dictionaries.</td>
<td>This feature is helpful when you set up a new Control Center and Scanner deployment. Assume that your existing Control Center and Scanner deployment contain some dictionary words and phrases that you want to use in the new deployment. You can export the words and phrases that you want to use in the new deployment. Then you can import those words and phrases into the new deployment from the Control Center computer. See “Exporting words or phrases from dictionaries” on page 385. See “Importing words or phrases into dictionaries” on page 388.</td>
</tr>
<tr>
<td>Enable or disable words or phrases in dictionaries.</td>
<td>Predefined words and phrases are words or the phrases that Symantec Messaging Gateway provides. You cannot delete predefined dictionary words or phrases. However, you can disable the predefined words or phrases that you do not want to use in content filtering policies. See “Disabling and enabling predefined words or phrases in dictionaries” on page 386.</td>
</tr>
<tr>
<td>Create your own dictionaries.</td>
<td>Symantec Messaging Gateway provides the premium dictionaries and custom dictionaries that you can use in your content filtering policies. However, you can create your own user-defined dictionary to suit your specific needs. See “Creating user-defined dictionaries” on page 387.</td>
</tr>
<tr>
<td>Edit dictionaries as needed.</td>
<td>You can make modifications to any type of dictionary (premium, custom, user-defined) as needed. See “Editing dictionaries” on page 388.</td>
</tr>
</tbody>
</table>
Table 15-9  Work with dictionaries (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete your user-defined words or phrases from dictionaries.</td>
<td>User-defined words or phrases are the words or phrases that you add to any type of dictionary (premium, custom, and user-defined). You can delete any of the user-defined words or phrases when they are no longer needed. See “Deleting user-defined words or phrases from dictionaries” on page 389.</td>
</tr>
<tr>
<td>Locate words or phrases in dictionaries.</td>
<td>You may have an instance in which you want to enable or disable, modify, or delete a word or phrase in multiple dictionaries. Symantec Messaging Gateway lets you search for the words and phrases that are used in all types of dictionaries (premium, custom, and user-defined). See “Finding words or phrases in dictionaries” on page 390.</td>
</tr>
<tr>
<td>Delete dictionaries.</td>
<td>You can delete any user-defined dictionary that you create unless it is used in a custom filtering policy. See “Deleting dictionaries” on page 390.</td>
</tr>
</tbody>
</table>

About content filtering dictionaries

A dictionary is a list of the words, phrases, file names, and the file name extensions that pertain to a specific topic. When a dictionary is part of a content filtering policy condition, Symantec Messaging Gateway searches your email messages for the contents of the dictionary. If you configure Symantec Messaging Gateway to scan non-plain text file attachments, they too are scanned for contents of the dictionary.

See “Scanning non-plain text file attachments for content filtering violations” on page 385.

Content filtering policies evaluate matches to a referenced dictionary with substring text analysis, not regular expression analysis. When a substring in a message matches a dictionary entry, Symantec Messaging Gateway takes the actions that you specify in the policy.

For purposes of dictionary matching, words consist only of alphanumeric characters A-Z, a-z, and 0-9. All other characters are delimiters. For example, searching the dictionary for the word 'bad' would detect a match, as would the variation 'bad_guy', because the underscore is treated as a word delimiter. However, 'bad1' one would not detect a match because the number "1" is considered part of the word.

A dictionary item may contain a delimiter. A dictionary term of 'ice cream' or '415-738-2623' may match a message, if there are delimiter characters on either side of the dictionary term (e.g. "chocolate ice cream is tasty!" or "pls call me (415-738-2623) ASAP!"). The match will fail on a variation such as, "pls call me (415-738-2623x12) ASAP!" as the 'x12' is considered part of the word '2623x12'.

The types of dictionaries that you can use are as follows:
Most of the premium dictionaries and custom dictionaries that Symantec Messaging Gateway provides already contain predefined words, phrases, and characters. You can view the contents of the premium dictionaries and custom dictionaries, enable and disable existing keywords, and add words, phrases, or characters.

Examine the contents of the premium dictionaries and custom dictionaries before you use them to determine if they meet your needs. If they do not, you can add the new user-defined words and phrases that you need. You can also disable the predefined words and phrases that you do not want to use.

Some premium dictionaries and custom dictionaries are empty. You must populate them with user-defined words or phrases before you can use them in a content filtering policy.

Note: The dictionaries that are marked as ambiguous (such as Profanity (ambiguous)) contain the terms that can be legitimate when used in certain contexts.

See “Premium and custom content filtering dictionaries” on page 391.

In addition to premium dictionaries and custom dictionaries, you can create user-defined dictionaries. You populate user-defined dictionaries to suit a site-specific or business need. These dictionaries must contain at least one word or phrase.

Table 15-10 describes the tasks that you can perform with the different types of dictionaries.

Table 15-10 | Tasks that you can perform with dictionaries based on type
--- | --- | ---
Create a new dictionary | Premium or custom | User-defined
Create a new dictionary | | X
Edit the dictionary | | X
Edit the dictionary | Premium or custom | User-defined
Delete the dictionary | | X
Delete the dictionary | | X
Import words or phrases into the dictionary | Premium or custom | User-defined
Import words or phrases into the dictionary | | X
Export words or phrases from the dictionary | | X
Export words or phrases from the dictionary | | X

Table 15-10 describes the tasks that you can perform with the different types of dictionaries.
Table 15-10  Tasks that you can perform with dictionaries based on type (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Premium or custom</th>
<th>User- defined</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable and disable words and phrases in the dictionary</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>See “Disabling and enabling predefined words or phrases in dictionaries” on page 386.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete words or phrases in the dictionary</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>See “Deleting user-defined words or phrases from dictionaries” on page 389.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search for words or phrases in the dictionary</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>See “Finding words or phrases in dictionaries” on page 390.</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

See “Considerations when you use dictionaries” on page 384.

Considerations when you use dictionaries

Note the following additional information about dictionaries:

- Words in dictionaries are detected only if they match exactly with words as they appear in the dictionary. Words in dictionaries are not detected if they are variations, such as verb tenses. For example, "selling" is not a match with the word "sell."
- Wildcards are not supported in dictionaries.
- Up to 100 dictionaries are supported, and each dictionary can contain up to 10,000 words.
- Words and phrases in dictionaries cannot be prioritized.
- A dictionary can be used in multiple content filtering policies.
- When you add words to a dictionary, keep in mind that some words can be considered both profane and legitimate, depending on the context. For example, the word "breast" might be inappropriate until it is coupled with the word "cancer."
- Symantec Messaging Gateway does not search for dictionary matches in the HTML headers or tags of HTML messages or HTML attachments.
- Words are not case sensitive.
- Punctuation characters (such as a question mark (?)) cannot be used as the first character of a word.

See “About content filtering dictionaries” on page 382.
See “Creating user-defined dictionaries” on page 387.
Scanning non-plain text file attachments for content filtering violations

Symantec Messaging Gateway can check the text in any file attachment against dictionaries to detect content filtering violations. Scanning file attachments maximizes the effect of content filtering, but it can affect the system load and slow performance.

See “Working with dictionaries” on page 380.
See “About content filtering” on page 322.

To scan file attachments for content filtering violations
1. Click Protocols > SMTP > Settings and then click the Content Scanning tab.
2. Check Enable scanning of attachments for words in dictionaries.
3. Click Save.

Exporting words or phrases from dictionaries

Symantec Messaging Gateway lets you export words and phrases from custom dictionaries. By default, the exported words and phrases are saved in a text file named DictionaryWords.txt. You cannot choose specific words or phrases to export. You must export all of the words and phrases in the dictionary.

Note: You cannot export words or phrases from premium dictionaries.

This feature is helpful when you set up a new Control Center and Scanner deployment. Assume that your existing Control Center and Scanner deployment contain some dictionary words and phrases that you want to use in the new deployment. You can export the words and phrases that you want to use in the new deployment. Then you can import those words and phrases into the new deployment from the Control Center computer.

See “Importing words or phrases into dictionaries” on page 388.

You may want to export a custom dictionary before you delete it to maintain for your records. You could also restore the exported file, if needed.

See “Deleting dictionaries” on page 390.

To export words or phrases from custom dictionaries, you must have Full Administration rights or rights to modify settings.

To export words or phrases from dictionaries
1. In the Control Center, click Content > Resources > Dictionaries.
2. Check the box beside the dictionary that contains the words or phrases that you want to export, and click Edit.
3. Click Export.
4 In the **File Download** dialog box, click **Save**.

5 In the **Save As** dialog box, type the file name and select the location where you want to save the file.

6 Click **Save**.

7 In the **Download Complete** dialog box, click **Open** to view the text file or **Close** to close the dialog box.

### Disabling and enabling predefined words or phrases in dictionaries

Predefined words and phrases are words or phrases that Symantec Messaging Gateway provides. You cannot delete predefined dictionary words or phrases. However, you can disable the predefined words or phrases that you do not want to use in content filtering policies.

---

**Note:** You cannot disable user-defined words or phrases in any of the dictionaries (premium, custom, or user-defined). If you do not want to use user-defined words, you must delete them.

---

See "Deleting user-defined words or phrases from dictionaries" on page 389.

To enable or disable predefined words or phrases, you must have Full Administration rights or rights to modify policies.

See "About content filtering dictionaries" on page 382.

See "Creating user-defined dictionaries" on page 387.

**To disable or enable predefined words or phrases in dictionaries**

1 In the Control Center, click **Content > Resources > Dictionaries**.

2 Check the box beside the dictionary that contains the words or phrases that you want to disable or enable, and click **Edit**.

   See “Finding words or phrases in dictionaries” on page 390.

3 Check the box beside the predefined word or phrase that you want to enable or disable. Check **Word or Phrase** to select all of the words and phrases in the list.
4 Do one of the following tasks:

Click **Disable**. If the dictionary is a condition of a policy, Symantec Messaging Gateway does not search for this word or phrase when it evaluates messages.

Click **Enable**. Symantec Messaging Gateway searches for the word or phrase when it evaluates messages.

5 Click **Save**.

Creating user-defined dictionaries

Symantec Messaging Gateway provides the premium dictionaries and custom dictionaries that you can use in your content filtering policies. However, you can create your own user-defined dictionary to suit your specific needs.

To add a user-defined dictionary, you must have Full Administration rights or rights to modify policies.

See “About content filtering dictionaries” on page 382.

See “Importing words or phrases into dictionaries” on page 388.

See “Editing dictionaries” on page 388.

See “Disabling and enabling predefined words or phrases in dictionaries” on page 386.

To create user-defined dictionaries

1 In the Control Center, click **Content > Resources > Dictionaries**.

2 Click **Add**.

3 In the **Dictionary name** field, type a name for the dictionary.

4 In the **Optional description** field, type a description of the dictionary.

5 In the **Enter a word or phrase** field, type the word or phrase that you want to add to your dictionary.

6 Click **Add** to add the word or phrase to the **Word or Phrase** list. The word or phrase is automatically enabled when you add it.

7 Repeat steps 5 and 6 to add more words and phrases.

8 Click **Save**.
Importing words or phrases into dictionaries

You can import words or phrases into all types of dictionaries (premium and custom). The file that you import must be a newline-delimited text file in UTF-8 format, and each word or phrase must be on a separate line. The file must be accessible to the Control Center computer.

**Note:** Files with extended ASCII are not supported.

See “About content filtering dictionaries” on page 382.

See “Creating user-defined dictionaries” on page 387.

See “Editing dictionaries” on page 388.

See “Disabling and enabling predefined words or phrases in dictionaries” on page 386.

To import words or phrases into dictionaries

1. In the Control Center, click **Content > Resources > Dictionaries**.
2. Check the box beside the dictionary that you want to import words or phrases into, and then click **Edit**.
3. On the **Add Dictionary** page, click **Import**.
4. Under **Import**, do one of the following tasks:
   - In the **File name** box, type the name of the text file that you want to import.
   - Click **Browse** to locate the text file that you want to import.
   
   The newly imported words or phrases are enabled by default.
5. Click **Save**.

Editing dictionaries

You can make modifications to any type of dictionary (premium, custom, user-defined) as needed.

See “Creating user-defined dictionaries” on page 387.

**Note:** Once you create a user-defined dictionary and add at least one word, you must always have at least one word in that dictionary. If you no longer need the user-defined dictionary, you can delete it.

See “Deleting dictionaries” on page 390.

To edit a dictionary, you must have Full Administration rights or rights to modify policies.
To edit dictionaries

1. In the Control Center, click Content > Resources > Dictionaries.
2. Check the box beside the dictionary that you want to edit, and click Edit.
3. Make the desired modifications.
   
   See “Creating user-defined dictionaries” on page 387.
   See “Importing words or phrases into dictionaries” on page 388.
   See “Disabling and enabling predefined words or phrases in dictionaries” on page 386.
   See “Deleting user-defined words or phrases from dictionaries” on page 389.
4. Click Save.

Deleting user-defined words or phrases from dictionaries

User-defined words or phrases are the words or phrases that you add to any type of dictionary (premium, custom, and user-defined). You can delete any of the user-defined words or phrases when they are no longer needed.

Note: You cannot delete predefined words or phrases. However, you can disable the predefined word or phrase that you do not want to use in content filtering policies.

See “Disabling and enabling predefined words or phrases in dictionaries” on page 386.

To delete user-defined words or phrases from dictionaries, you must have Full Administration rights or rights to modify policies.

To delete user-defined words or phrases from dictionaries

1. In the Control Center, click Content > Resources > Dictionaries.
2. Check the box beside the dictionary that contains the user-defined word or phrase that you want to delete, and click Edit.
   
   See “Finding words or phrases in dictionaries” on page 390.
3. On the Edit Dictionary page, check the box beside the user-defined word or phrase that you want to remove.
   
   Check Word or Phrase to select all of the words and phrases in the list.
4. Click Delete.
5. Click Save.
Finding words or phrases in dictionaries

You may have an instance in which you want to enable or disable, modify, or delete a word or phrase in multiple dictionaries. Symantec Messaging Gateway lets you search for the words and phrases that are used in all types of dictionaries (premium, custom, and user-defined).

When you search for a word or phrase, Symantec Messaging Gateway displays a message at the top of the Dictionaries page. The message lists all of the dictionaries that contain the word or phrase. If no match is found, the following message appears: No dictionaries match the word or phrase.

To search for words or phrases in dictionaries, you must have Full Administration rights or rights to modify policies.

See “Creating user-defined dictionaries” on page 387.

To find words or phrases in dictionaries

1. In the Control Center, click Content > Resources > Dictionaries.
2. On the Dictionaries page, in the Find word or phrase field, type the word or phrase that you want to find.
3. Click Find.

Deleting dictionaries

You can delete any user-defined dictionary that you create unless it is used in a custom filtering policy. Before you delete a user-defined dictionary, you may want to export the words and phrases to a text file to maintain for your records. The text file can be reimported, if needed.

Note: You cannot delete premium or custom dictionaries.

See “Exporting words or phrases from dictionaries” on page 385.

See “Importing words or phrases into dictionaries” on page 388.

To delete a user-defined dictionary, you must first delete that dictionary from any content filtering policy conditions in which it is used. Symantec Messaging Gateway lets you know which policies use that dictionary when you attempt to delete it.

To delete a user-defined dictionary, you must have Full Administration rights or rights to modify policies.

See “About content filtering dictionaries” on page 382.
To delete dictionaries

1. In the Control Center, click **Content > Resources > Dictionaries**.
2. On the **Dictionaries** page, check the box beside the dictionary that you want to delete.
3. Click **Delete**.

A message appears at the top of the page to indicate the content filtering policies in which a condition to use this dictionary occurs. Delete or modify this condition in these policies first, then repeat this procedure.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.

Premium and custom content filtering dictionaries

Symantec Messaging Gateway provides premium dictionaries and custom content filtering dictionaries that you can use when you create content filtering policy conditions.

See “About content filtering dictionaries” on page 382.

Table 15-11 lists the premium dictionaries and custom dictionaries and the recommended policy templates with which to use them.

<table>
<thead>
<tr>
<th>Dictionary name</th>
<th>Associated templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Routing Number Keywords</td>
<td>PIPEDA; Employee Data Protection; Customer Data Protection; Swift Codes; Employee Data Protection; State Data Privacy; Gramm-Leach-Bliley</td>
</tr>
<tr>
<td>Affiliate Domains</td>
<td>State Data Privacy</td>
</tr>
<tr>
<td>Analysts’ Email Addresses</td>
<td>NASD Rule 2711 and NYSE Rules 351 and 472</td>
</tr>
<tr>
<td>California Keywords</td>
<td>State Data Privacy</td>
</tr>
<tr>
<td>Illinois Keywords</td>
<td></td>
</tr>
<tr>
<td>Letter/12 Num. DLN State Words</td>
<td></td>
</tr>
<tr>
<td>New Jersey Keywords</td>
<td></td>
</tr>
<tr>
<td>New York Keywords</td>
<td></td>
</tr>
<tr>
<td>Canadian Social Ins. No. Words</td>
<td>PIPEDA; Canadian Social Insurance Number</td>
</tr>
<tr>
<td>Company Name Keywords (user-defined)</td>
<td>SEC Fair Disclosure Regulation; Sarbanes-Oxley</td>
</tr>
<tr>
<td>Competitor Domains</td>
<td>Competitor Communications</td>
</tr>
</tbody>
</table>
Table 15-11  Premium dictionaries, custom dictionaries, and related templates (continued)

<table>
<thead>
<tr>
<th>Dictionary name</th>
<th>Associated templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Keywords (user-defined)</td>
<td>Confidential Documents</td>
</tr>
<tr>
<td>Internal Use Only Keywords (user-defined)</td>
<td></td>
</tr>
<tr>
<td>Proprietary Keywords (user-defined)</td>
<td></td>
</tr>
<tr>
<td>Not for Distribution Words (user-defined)</td>
<td></td>
</tr>
<tr>
<td>Confidential/Proprietary Words</td>
<td>Sarbanes-Oxley</td>
</tr>
<tr>
<td>Credit Card Number Keywords</td>
<td>Credit Card Numbers; Payment Card Industry Data Security Standard; Customer Data Protection; Employee Data Protection; PIPEDA</td>
</tr>
<tr>
<td>Design Documents Extensions</td>
<td>Design Documents</td>
</tr>
<tr>
<td>Disease Names</td>
<td>HIPAA (including PHI); Caldicott Report</td>
</tr>
<tr>
<td>EAR CCL Keywords; EAR Country Codes</td>
<td>Export Administration Regulations (EAR)</td>
</tr>
<tr>
<td>EU Country Codes</td>
<td>EU Data Protection Directives</td>
</tr>
<tr>
<td>Financial Keywords</td>
<td>Sarbanes-Oxley</td>
</tr>
<tr>
<td></td>
<td>Financial Information</td>
</tr>
<tr>
<td>Gambling Keywords, Confirmed; Gambling Keywords, Suspect</td>
<td>Gambling</td>
</tr>
<tr>
<td>GPG Encryption Keywords</td>
<td>Encrypted Data</td>
</tr>
<tr>
<td>PGP file extensions</td>
<td></td>
</tr>
<tr>
<td>PGP8 Keywords</td>
<td></td>
</tr>
<tr>
<td>Hacker Keywords; Keylogger Keywords</td>
<td>Network Security</td>
</tr>
<tr>
<td>ITAR Country Codes</td>
<td>International Traffic in Arms Regulations (ITAR)</td>
</tr>
<tr>
<td>ITAR Munition Names</td>
<td></td>
</tr>
<tr>
<td>Job Search Keywords, Education</td>
<td>Resumes</td>
</tr>
<tr>
<td>Job Search Keywords, General</td>
<td></td>
</tr>
<tr>
<td>Job Search Keywords, Work</td>
<td></td>
</tr>
<tr>
<td>M &amp; A Project Code Names (user-defined)</td>
<td>Mergers and Acquisitions Data</td>
</tr>
<tr>
<td>Mancfd. Controlled Substances</td>
<td></td>
</tr>
<tr>
<td>Street Drug Names</td>
<td>Illegal Drugs</td>
</tr>
<tr>
<td>Dictionary name</td>
<td>Associated templates</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Media Files Extensions</td>
<td>Media Files</td>
</tr>
<tr>
<td>Medical Treatment Keywords</td>
<td>HIPAA (including PHI)</td>
</tr>
<tr>
<td>NASD 2711 Keywords (user-defined)</td>
<td>NASD Rule 2711 and NYSE Rules 351 and 472</td>
</tr>
<tr>
<td>NASD 3010 General Keywords</td>
<td>NASD Rule 3010 and NYSE Rule 342</td>
</tr>
<tr>
<td>NASD 3010 Stock Keywords</td>
<td></td>
</tr>
<tr>
<td>NASD 3010 Buy/Sell Keywords</td>
<td></td>
</tr>
<tr>
<td>OFAC Country Codes</td>
<td>Office of Foreign Assets Control (OFAC)</td>
</tr>
<tr>
<td>OFAC SDN Country Codes</td>
<td></td>
</tr>
<tr>
<td>SDN List</td>
<td></td>
</tr>
<tr>
<td>Offensive Language, Explicit</td>
<td>Offensive Language</td>
</tr>
<tr>
<td>Offensive Language, General</td>
<td></td>
</tr>
<tr>
<td>Other Sensitive Information</td>
<td>US Intelligence Control Markings (CAPCO) &amp; DCID 1/7</td>
</tr>
<tr>
<td>Password Filenames</td>
<td>Password Files</td>
</tr>
<tr>
<td>Prescription Drug Names</td>
<td>HIPAA (including PHI)</td>
</tr>
<tr>
<td></td>
<td>Caldicott Report</td>
</tr>
<tr>
<td>Publishing Document Extensions</td>
<td>Publishing Documents</td>
</tr>
<tr>
<td>Racist Language</td>
<td>Racist Language</td>
</tr>
<tr>
<td>Restricted Recipients</td>
<td>Restricted Recipients</td>
</tr>
<tr>
<td>SEC Fair Disclosure Keywords</td>
<td>SEC Fair Disclosure Regulation</td>
</tr>
<tr>
<td>Secret</td>
<td>Defense Message System (DMS) GENSER Classification</td>
</tr>
<tr>
<td>Top Secret</td>
<td></td>
</tr>
<tr>
<td>Classified or Restricted</td>
<td>US Intelligence Control Markings (CAPCO) &amp; DCID 1/7</td>
</tr>
<tr>
<td>Sensitive Keywords</td>
<td>NERC Security Guidelines for Electric Utilities</td>
</tr>
<tr>
<td>Sensitive Project Code Names</td>
<td>Project Data</td>
</tr>
</tbody>
</table>
Table 15-11  Premium dictionaries, custom dictionaries, and related templates (continued)

<table>
<thead>
<tr>
<th>Dictionary name</th>
<th>Associated templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sex. Explicit Words, Confirmed</td>
<td>Sexually Explicit Language</td>
</tr>
<tr>
<td>Sex. Explicit Words, Possible</td>
<td></td>
</tr>
<tr>
<td>Sex. Explicit Words, Suspect</td>
<td></td>
</tr>
<tr>
<td>Source Code Extensions</td>
<td>Source Code</td>
</tr>
<tr>
<td>SWIFT Code Keywords</td>
<td>SWIFT Codes</td>
</tr>
<tr>
<td>TPO Email Addresses</td>
<td>HIPAA (including PHI)</td>
</tr>
<tr>
<td>UK Electoral Roll Number Words</td>
<td>UK Electoral Roll Numbers</td>
</tr>
<tr>
<td></td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td></td>
<td>Human Rights Act 1998</td>
</tr>
<tr>
<td>UK Tax ID Number Keywords</td>
<td>UK Tax ID Numbers</td>
</tr>
<tr>
<td></td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td>UK NIN Keywords</td>
<td>UK National Insurance Number</td>
</tr>
<tr>
<td></td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td></td>
<td>Caldicott Report</td>
</tr>
<tr>
<td>UK Keywords</td>
<td>UK Drivers License Numbers</td>
</tr>
<tr>
<td></td>
<td>UK Electoral Roll Numbers</td>
</tr>
<tr>
<td></td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td></td>
<td>Human Rights Act 1998</td>
</tr>
<tr>
<td>UK Passport Keywords</td>
<td>UK Passport Numbers</td>
</tr>
<tr>
<td></td>
<td>Data Protection Act 1998</td>
</tr>
<tr>
<td>UK Personal Data Keywords</td>
<td>Human Rights Act 1998</td>
</tr>
<tr>
<td>US ITIN Keywords</td>
<td>Individual Taxpayer Identification Numbers</td>
</tr>
<tr>
<td>US SSN Keywords</td>
<td>US Social Security Numbers</td>
</tr>
<tr>
<td></td>
<td>Employee Data Protection</td>
</tr>
<tr>
<td>Violence Keywords</td>
<td>Violence and Weapons</td>
</tr>
<tr>
<td>Weapons Keywords</td>
<td></td>
</tr>
<tr>
<td>Vulnerability Keywords</td>
<td>NERC Security Guidelines for Electric Utilities</td>
</tr>
</tbody>
</table>
Using patterns to detect policy violations

Symantec Messaging Gateway provides the predefined basic patterns and premium patterns that you can use in content filtering policy conditions.

Table 15-12 describes what you can do with patterns. You can perform these tasks as needed in any order.

Table 15-12 Manage patterns

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about what patterns are and how to use them. You can also learn the types of patterns that install with Symantec Messaging Gateway.</td>
<td>Symantec Messaging Gateway provides a feature that lets you use patterns to detect policy violations. Patterns are the regular expressions or system patterns that depict commonly known forms of content, such as the pattern for credit card numbers. Symantec Messaging Gateway provides predefined basic patterns and premium patterns. You can also create your own custom patterns. See “About patterns” on page 395.</td>
</tr>
<tr>
<td>Create a custom pattern.</td>
<td>You can create your own custom pattern with the syntax that you copy from a basic pattern or regular expressions. You can view, edit, and delete custom patterns. An example of a custom pattern is a pattern for non-US phone numbers. See “Creating your own custom patterns” on page 397.</td>
</tr>
<tr>
<td>Edit your custom pattern.</td>
<td>You cannot edit basic patterns and premium patterns. However, you can edit the custom patterns that you create.</td>
</tr>
<tr>
<td>Delete a custom pattern.</td>
<td>You cannot edit the basic patterns or premium patterns. However, you can delete the custom patterns that you create when you no longer need them.</td>
</tr>
</tbody>
</table>

About patterns

Symantec Messaging Gateway provides a feature that lets you use patterns to detect policy violations. Patterns are regular expressions or system patterns that depict commonly known forms of content, such as the pattern for credit card numbers. Symantec Messaging Gateway provides predefined basic patterns and premium patterns. You can also create your own custom patterns.

All of these patterns are available in the Matches pattern/does not match pattern drop-down list on the Content Filtering Policy Conditions page when you define a policy condition. Table 15-13 describes the types of patterns that you can use.
Patterns for content filtering policy conditions

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Description</th>
</tr>
</thead>
</table>
| Basic        | Basic patterns are known and performance-tested regular expressions that you can use in a policy or as examples when you create a custom pattern. You can view basic patterns, but these patterns cannot be edited or deleted. Basic credit card patterns detect only Visa, Master Card, AMEX and Discover cards. The predefined basic patterns and their syntax are as follows:  
  ■ Credit Card  
  \b(?<!-)((4\d{3})|(5\[1-5]\d{2})|(6011))(-?)\d{4}\d{4}\d{4}(?!-)\b |  
  ■ Email Address  
  \b([0-9a-zA-Z](\[-.\w\]*[0-9a-zA-Z])*@[0-9a-zA-Z]\.[w]*[0-9a-zA-Z])@([0-9a-zA-Z]\[-\w\]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,9})\b |  
  ■ Social Security Number  
  \b(?<!-)(\d{3})([ -]\d{2})\d{4}(?!-)\b |  
  ■ US Phone Number  
  \b(?<!-)((1([\s.-]?)[2-9]\d{2}\d{3}\d{3}\d{4})|([2-9]\d{2}([ -]?)(3)\d{3}\d{4})|([2-9]\d{3}\d{4})([ -]?)(4)))\b |  
  ■ US Zipcode  
  \b(?<!-)((\d{5})|((\d{5})\d{4}))\b |  
| Premium      | Premium patterns perform additional checking and validation (such as Luhn checking) beyond regular expression definitions to reduce false positives. These patterns cannot be viewed, edited, or deleted. The predefined premium patterns and the policy templates that you can use them with are as follows:  
  ■ Valid Credit Card  
  Credit Card Numbers; Customer Data Protection; Employee Data Protection; PIPEDA; State Data Privacy; Payment Card Industry Data Security Standard; Gramm-Leach-Bliley  
  ■ Valid IP Address  
  Network Diagrams  
  ■ Valid Social Security Number  
  HIPAA; Gramm-Leach-Bliley; US Social Security Numbers; Individual Taxpayer Identification Numbers (ITIN); State Data Privacy; Customer Data Protection; Employee Data Protection  
  **Note:** The Valid Credit Card and Valid Social Security Number patterns differ from the Credit Card and Social Security Number patterns that are provided in the basic patterns. The valid patterns contain a rules checking feature to help insure their completeness and accuracy. |
Table 15-13  Patterns for content filtering policy conditions (continued)

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom</td>
<td>You can create your own custom pattern with the syntax that you copy from a basic pattern or regular expressions. You can view, edit, and delete custom patterns. An example of a custom pattern is a pattern for non-US phone numbers. You should consult an advanced resource on regular expressions to construct your own patterns.</td>
</tr>
</tbody>
</table>

See “Creating a content filtering policy” on page 325.
See “Creating your own custom patterns” on page 397.
See “Editing patterns” on page 398.
See “Deleting patterns” on page 398.

Creating your own custom patterns

Symantec Messaging Gateway provides the basic patterns and premium patterns that you can reference in your policy conditions. Symantec Messaging Gateway uses these patterns to search messages for the character patterns that indicate the data that you may want to restrict.

You can copy all or any portion of a basic pattern to use in your custom pattern, or you can use regular expressions.

See “About patterns” on page 395.
See “Using regular expressions in content filtering policy conditions” on page 332.

An example of a custom pattern that you can create is for non-US telephone numbers. For example, Australia has a variety of formats for phone numbers. One such format follows the pattern: nn nnnn nnnn

To detect Australian telephone numbers that follow this format, you could create the following pattern:

```
\b((\[(0\d\])\]|0\d)\s)?\d{4}\s\d{4}\b
```

Your pattern might also include formats with country codes for international dialing.

Note: You should consult an advanced resource on regular expressions to construct your own patterns.

To create a custom pattern, you must have Full Administration rights or rights to modify policies.

See “Editing patterns” on page 398.
To create your own custom pattern

1. In the Control Center, click Content > Resources > Patterns.
2. Click the Custom tab.
3. Click Add.
4. In the Pattern name field, type a name for your custom pattern.
5. In the Regular expression field, type the regular expression.
6. Click Save.

Editing patterns

You cannot edit basic patterns and premium patterns. However, you can edit the custom patterns that you create. You can only edit one pattern at a time. To edit a custom pattern, you must have Full Administration rights or rights to modify policies.

To edit patterns

1. In the Control Center, click Content > Resources > Patterns.
2. Click the Custom tab.
3. Check the box beside the pattern that you want to edit, and then click Edit.
   
   You can also click the custom pattern name to edit the pattern.
4. In the Pattern name field, edit the pattern name as needed.
   
   If a pattern's name is changed, that name change is propagated to any policy that references the custom pattern.
5. In the Regular expression field, edit the regular expression as needed.
6. Click Save.

See “About patterns” on page 395.
See “Using regular expressions in content filtering policy conditions” on page 332.
See “Creating your own custom patterns” on page 397.
See “Deleting patterns” on page 398.

Deleting patterns

You cannot edit the basic patterns or premium patterns. However, you can delete the custom patterns that you create when you no longer need them.
To delete a custom pattern, you must first delete that pattern as a condition from any content filtering policies in which it is used. Symantec Messaging Gateway lets you know which policies use that pattern when you attempt to delete it.

To delete a custom pattern, you must have Full Administration rights or rights to modify policies.

See “About patterns” on page 395.

To delete patterns

1. In the Control Center, click **Content > Resources > Patterns**.
2. Click the **Custom** tab.
3. Check the box beside the pattern that you want to delete.
   - Check the box beside **Patterns** to select all of the patterns for deletion.
4. Click **Delete**.

A message appears at the top of the page to indicate the content filtering policies in which a condition to use this pattern occurs. Delete or modify this condition in these policies first, then repeat this procedure.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.

See “About patterns” on page 395.

Creating and managing annotations for policy violations

An annotation is the text that Symantec Messaging Gateway adds to the body of a message when the message violates a filtering policy. When you create a policy, you can select the action **add annotation**, and then choose the annotation from a drop-down menu. You can add annotations to this menu, or edit or delete existing ones, from the **Content > Resources > Annotations** page.

To add or edit an annotation, you must have Full Administration rights or rights to modify policies.

---

**Note:** Annotations are different from notifications. Annotation text is added to a message. A notification is a separate message that is sent when a policy is violated and the policy action is **Send notification**.

---

To create an annotation

1. In the Control Center, select **Content > Resources > Annotations**.
2. On the **Annotations** page, click **Add**.
3 On the Add Annotations page, enter a description for the annotation.

   This description appears in the drop-down menu when you add an annotation action to a policy.

4 Select the Encoding type.

5 In the Plain text (required) box, enter the text that you want to add to messages.

   Text for content filtering messages should not exceed 65,000 characters.

   When you select Add annotation as a policy action, you can choose to prepend the annotation to the beginning of the message body. Or you can append the annotation to the end of the message. The annotation appears on a separate line from the message body. However, you can add a blank line or a line of dashes to the beginning and end of your annotation text for better visual separation from the message body.

6 (Optional) In the HTML box, enter the text that you want to add to the HTML part of a message, if present.

   As a best practice, the plain text message and HTML message should be the same. If you do not add HTML text, the plain text annotation is added to HTML messages.

   HTML text should not exceed 128 characters. You can use HTML formatting tags, such as <b>bold text here</b>, but HTML structure tags are not supported.

7 Click Save.

   To edit an annotation, select the annotation on the Content > Resources > Annotations, and then click Edit.

   To delete an annotation, select the annotation on the Content > Resources > Annotations, and then click Delete.

   See "Policy actions and what they do" on page 333.

Using lists to detect prohibited attachments

   Table 15-14 describes how you can use attachment lists in policy conditions to identify prohibited attachments types. You can perform these tasks as needed in any order.
Table 15-14  Managing lists

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Learn more about how you can use attachment lists in policies. | An attachment list contains the file extensions and the file application types that you want Symantec Messaging Gateway to detect. You use an attachment list as a condition of a content filtering policy. When Symantec Messaging Gateway detects an attachment that has an extension that is on the file extension list, it applies the action that you specify. Symantec Messaging Gateway can determine the email attachment type based on the application that created it, regardless of its file extension.  
See “About attachment lists” on page 401. |
| Create an attachment list. | Symantec Messaging Gateway provides predefined attachment lists that you can use to create your attachment list or you can create your own custom attachment list.  
See “Creating lists to detect file attachment types” on page 411. |
| Modify an existing attachment list. | You can edit an existing attachment list as needed.  
See “Editing attachment lists” on page 413. |
| Delete a custom attachment list that you no longer need. | You can delete the attachment lists that you create when they are no longer needed. Predefined attachment lists cannot be deleted.  
See “Deleting attachment lists” on page 414. |
| View the default attachment lists. | This topic describes all of the predefined attachment lists.  
See “Default attachment lists” on page 402. |
| Learn how you can use perl-compatible regular expressions in your attachment lists. | These topics describe the Perl-compatible regular expressions that you can use in content filtering policies along with examples.  
See “Perl-compatible regular expressions” on page 414.  
See “Perl-compatible regular expression examples” on page 416. |

About attachment lists

An attachment list contains the file extensions and the file application types that you want Symantec Messaging Gateway to detect. When Symantec Messaging Gateway detects an attachment that has an extension that is on the file extension list, it applies the action that you specify. Symantec Messaging Gateway can determine the email attachment type based on the application that created it, regardless of its file extension.

You can create an attachment list with any combination of the following:
True file classes

True file classes are categories in which similar file types and applications are grouped. For example, Desktop publishing and Movie file are true file classes.

Within a true file class are the true file types. For example, FrameMaker is a true file type within the Desktop publishing true file class.

You cannot modify the list of true file types within a true file class. You must use the list as is.

True file types

True file types are contained within a true file class. True file types consist of file extensions or applications. For example, a true file type within the category Desktop publishing is FrameMaker. A true file type within the category Movie file is MPEG movie.

You can add and delete items in a true file types list.

Note: The Archive Files attachment list does not support true file type MIME. The Document Files attachment list does not support true file type HTML.

Common file extensions and MIME-types

You can specify common file extensions and MIME-types. For example, you can filter out all .jpeg file attachments, regardless of the application that created it.

For a technical description of MIME, see the following RFC:
https://www.ietf.org/rfc/rfc2045.txt

Symantec Messaging Gateway provides default attachment lists. You cannot modify default attachment lists; however, you can copy them and modify the copies as needed. Or you can create your own custom attachment lists.

See "Default attachment lists" on page 402.
See “Creating lists to detect file attachment types” on page 411.

Default attachment lists

Table 15-15 describes the default attachment lists.
### Table 15-15  Default attachment lists

<table>
<thead>
<tr>
<th>Attachment list</th>
<th>True file class</th>
<th>Predefined true file type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Files</td>
<td>Encapsulation format</td>
<td>Apple Double, Apple Single, ASCII-armored PGP encoded, ASCII-armored PGP Public Keyring, ASCII-armored PGP signed, BinHex, Compactor / Compact Pro, cpio archive (CHR Header), cpio archive (CRC Header), Disk Doubler, GZ Compress, LHA Archive, IBM Lotus Notes Database NSF/NTF, MacBinary, Microsoft Outlook, Microsoft Outlook PST, MIME, OLE Compound Document, PAK/ARC Archive, OpenPGP Message Format (with new packet format), PGP Compressed Data, PGP Encrypted Data, PGP Public Keyring, PGP Secret Keyring, PGP Signature Certificate, PGP Signed and Encrypted Data, PGP Signed Data, RAR, Serialized Object Format (SOF), SHAR, SMTP, StuffIt (MAC), SUN PEX Binary Archive, TAR, Unix Compress, UU encoded, WANG Office GDL Header, ZIP Archive, Mac Disk Copy Disk Image File, Microsoft Entourage Database Format, 7 Zip Format(7z), Bzip 2 Compressed File, ISO-9660 CD Disc Image Format, Microsoft Cabinet File (CAB), Nero Encrypted File(.nef), Legato EMailXtender Archives Format (EMX)</td>
</tr>
<tr>
<td>Design Documents</td>
<td>Vector graphic format</td>
<td>Document F97, Lotus Freelance for DOS, Lotus Freelance for OS/2, Lotus Freelance for Windows; Persuasion, Microsoft PPT 2000 XML, Microsoft PPT Macro 2007 XML, Microsoft Visio, PowerPoint 95, PowerPoint 97, PowerPoint MAC, PowerPoint PC, Extensible Forms Description Language (.xfd, .xfd), Apple iWork Keynote</td>
</tr>
<tr>
<td>Design Documents</td>
<td>Scheduling/Planning Format</td>
<td>Microsoft Project 2000, Microsoft Project 4, Microsoft Project 4.1, Microsoft Project 98, Microsoft Project Activity, Microsoft Project Calculation, Microsoft Project Resource, PlanPerfect</td>
</tr>
<tr>
<td>Attachment list</td>
<td>True file class</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Document Files</td>
<td>Ability Spreadsheet, ACT, ALIS, Apple Binary Property List Format, Apple iChat,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Apple iWork Keynote, Apple iWork Numbers, Apple iWork Pages, AppleWorks,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APPLIX ASTERIX, Applix Graphics, Applix Spreadsheets, Applix Words, BlackBerry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Activation File (etp.dat), CDA / DDIF, CEOwrite, COMET TOP, Convergent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technologies DEF Comm., Corel Presentations, CPT, CSV (Comma Separated Values),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Interchange Format (DIF), DCA-FFT (IBM Final Form), DCA-RFT (IBM Revisable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Form), DCF Script, DCS, DECdx, DG Common Data Stream (CDS), Display Write,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DocuWorks Format (.xdw), DSA101 (Honeywell Bull), EBCDIC Text, Electronic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Publication, Enable Spreadsheet, Enable Word Processing, Envoy, Extensible Forms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description Language (.xfd, .xfdl), Folio Flat File, Founder Chinese E-paper</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Basic (ceb), FrameMaker, FrameMaker Book, Harvard Graphics, Health level7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>message, HP Word PC, HWP(Arae-Ah Hangul), IBM 1403 Line Printer IBM Writing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Assistant, ICHITARO V4-10, IFilter, Interleaf, Lotus 1-2-3, Lotus 1-2-3 97,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lotus 1-2-3 Formatting, Lotus 1-2-3 Release 9, Lotus Ami Pro, Lotus Ami Pro Style</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sheet, Lotus Freelance 96, Lotus Freelance 97, Lotus Freelance for DOS, Lotus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Freelance for OS/2, Lotus Freelance for Windows, Lotus Notes CDF, Lotus Word Pro</td>
<td></td>
</tr>
<tr>
<td></td>
<td>96, Lotus Word Pro 97, Lyrix Word Processing, MacWrite, MacWrite II, Maker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Interchange Format (MIF), Maker Markup Language, MASS-11, MHT format, Microsoft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Excel, Microsoft Excel 2000, Microsoft Excel 2007 XML, Microsoft Excel 95,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Excel 97, Microsoft Excel Binary 2007, Microsoft Excel Chart, Microsoft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Excel Macro, Microsoft Excel Macro 2007 XML, Microsoft Excel XML, Microsoft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office Groove Format, Microsoft Pocket Word, Microsoft PowerPoint 2000, Microsoft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PPT 2007 XML, Microsoft PPT Macro 2007 XML, Microsoft Project 2000, Microsoft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Project 2007, Microsoft Project 4, Microsoft Project 4.1, Microsoft Project 98,</td>
<td></td>
</tr>
</tbody>
</table>
|                    | Microsoft Project Activity
#### Table 15-15 Default attachment lists (continued)

<table>
<thead>
<tr>
<th>Attachment list</th>
<th>True file class</th>
<th>Predefined true file type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment list</td>
<td>True file class</td>
<td>Predefined true file type</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Document Files</td>
<td></td>
<td>SmartWare II Spreadsheet, SmartWare II Word Processor, StarOffice Presentation XML, StarOffice Spreadsheet XML, StarOffice Text XML, Supercalc, SWF, SYLK, Symphony, Targen Word, UltraCalc, Unicode, Unicode HTML, Uniplex, Uniplex Ucalc, USENET, Verity XML, Vistaword, Volkswriter, WANG PC, WANG WITA, WANG WPS, Windows Write, Word Connection, WordERA, WordMARC, WordPerfect, WordPerfect Configuration File, WordPerfect Driver, WordPerfect Hyphenation Dictionary, WordPerfect MAC, WordPerfect Macro, WordPerfect Miscellaneous File, WordPerfect Resource File, WordPerfect Spelling Dictionary, WordPerfect Thesaurus, WordPerfect VAX, WordStar, WordStar 2000, WPS-PLUS, WriteNow MAC, Xerox 860, Xerox Writer, XHTML, XML, XYWrite / Nota Bene, Yahoo Instant Messenger History, MIME-type begins with application/ms-excel, MIME-type begins with application/msword, MIME-type begins with application/pdf, MIME-type begins with application/vnd.ms-access, MIME-type begins with application/vnd.ms-excel, MIME-type begins with application/vnd.ms-powerpoint, MIME-type begins with application/vnd.ms-project, MIME-type begins with application/vnd.ms-works, MIME-type begins with application/vnd.visio, extension is doc, extension is dot, extension is mpp, extension is pdf, extension is ppt, extension is ps, extension is rtf, extension is txt, extension is vsd, extension is wk1, extension is wks, extension is wp, extension is xls</td>
</tr>
<tr>
<td>Executable Files</td>
<td>Executable File</td>
<td>ELF Executable, MS-DOS Batch File, MSDOS Device Driver, MSDOS/Windows Program PC (.COM), Unix Executable (3B20), Unix Executable (Basic-16), Unix Executable (Bell 5.0), Unix Executable (iAPX 286), Unix Executable (MC680x0), Unix Executable (PDP-11/pre-System V VAX), Unix Executable (VAX), Unix Executable (WE32000), Unix Executable (x86)</td>
</tr>
<tr>
<td>Financial Information</td>
<td>Spreadsheet formats</td>
<td>Applix Spreadsheets, CSV (Comma Separated Values), Lotus 1-2-3, Microsoft Excel, Microsoft Excel Chart, Microsoft Excel Macro, Microsoft Excel XML, Microsoft Works for DOS Spreadsheet, Microsoft Works for MAC Spreadsheet, Microsoft Works for Windows Spreadsheet, Multiplan (Mac), Multiplan (PC), Quattro Pro for DOS, Quattro Pro for Windows, SYLK</td>
</tr>
<tr>
<td>Attachment list</td>
<td>True file class</td>
<td>Predefined true file type</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Confidential Documents</td>
<td>Spreadsheet formats</td>
<td>Applix Spreadsheets, CSV (Comma Separated Values), Lotus 1-2-3, Lotus 1-2-3 97, Lotus 1-2-3 Release 9, Microsoft Excel, Microsoft Excel 2000, Microsoft Excel 2007, Microsoft Excel 95, Microsoft Excel 97, Microsoft Excel Chart, Microsoft Excel Macro, Microsoft Excel XML, Microsoft Works for DOS Spreadsheet, Microsoft Works for MAC Spreadsheet, Microsoft Works for Windows Spreadsheet, Multiplan (Mac), Multiplan (PC), Portable Document Format, Quattro Pro for DOS, Quattro Pro for Windows, SYLK</td>
</tr>
<tr>
<td>Confidential Documents</td>
<td>Word Processing</td>
<td>Microsoft Word 2000, Microsoft Word 2007, Microsoft Word 95, Microsoft Word 97, Microsoft Word for Macintosh, Microsoft Word for PC, Microsoft Word for Windows, Microsoft Word UNIX, Microsoft Word XML</td>
</tr>
<tr>
<td>Attachment list</td>
<td>True file class</td>
<td>Predefined true file type</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Confidential Documents</td>
<td>Presentation</td>
<td>Microsoft PowerPoint 2000, PowerPoint 95, PowerPoint 97, PowerPoint MAC, PowerPoint PC</td>
</tr>
<tr>
<td>Documents Not For Distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Use Only Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proprietary Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Files</td>
<td>Animation File</td>
<td>Macromedia Director, Macromedia Flash</td>
</tr>
<tr>
<td>Media Files</td>
<td>Vector graphic Document</td>
<td>Quickdraw 3D Metafile, VRML</td>
</tr>
<tr>
<td>Media Files</td>
<td>Movie File</td>
<td>QuickTime Movie, RIFF Multimedia Movie, Video for Windows (AVI), RealMedia Streaming</td>
</tr>
<tr>
<td>Media Files</td>
<td>Sound File Format</td>
<td>Microsoft Wave, MIDI, MP3 (MPEG Audio), RealAudio, RIFF MIDI, AC3 Audio File Format (.ac3)</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td>Library</td>
<td>DOS/Windows Object Library</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td>Database Documents</td>
<td>Microsoft Access, Microsoft Access 2000, Microsoft Access 95</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td>Executables</td>
<td>MSDOS Device Driver, PC (.COM), MSDOS/Windows Program, Unix Executable (3B20), Unix</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td>Object Module Format</td>
<td>Executable (Basic-16), Unix Executable (Bell 5.0), Unix Executable (iAPX 286), Unix</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td></td>
<td>Executable (MC680x0), Unix Executable (PDP-11/pre-System V VAX), Unix Executable (VAX),</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td></td>
<td>Unix Executable (WE32000), Unix Executable (x86)</td>
</tr>
<tr>
<td>Multimedia Files</td>
<td>Movie File</td>
<td>MPEG Movie, QuickTime Movie, RIFF Multimedia Movie, Video for Windows (AVI)</td>
</tr>
<tr>
<td>Multimedia Files</td>
<td>Sound File Format</td>
<td>Amiga IFF (BSVX) Sound, Amiga MOD, Audio Interchange File Format (AIFF), Creative Voice</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(VOC), Microsoft Wave, MIDI, MPEG Audio, NeXT/Sun Audio Data, Real Audio, RIFF MIDI, AC3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audio File Format (.ac3), RealMedia Streaming Media (.rm, .ra)</td>
</tr>
<tr>
<td>Attachment list</td>
<td>True file class</td>
<td>Predefined true file type</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Diagrams with IP Address Keyword</td>
<td>Presentation Document</td>
<td>Microsoft Visio</td>
</tr>
<tr>
<td>Network Diagrams with IP Addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Diagrams with IP Address Keyword</td>
<td>Word Processor Document</td>
<td>Microsoft Visio XML</td>
</tr>
<tr>
<td>Network Diagrams with IP Addresses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Protected Files</td>
<td>Spreadsheet formats (password protected)</td>
<td>Microsoft Excel, Microsoft Excel 2000, Microsoft Excel 2007, Microsoft Excel 95, Microsoft Excel 97, Microsoft Excel Chart, Microsoft Excel XML</td>
</tr>
<tr>
<td>Password Protected Files</td>
<td>Presentation Document (password protected)</td>
<td>Microsoft PowerPoint2000, PowerPoint 95, PowerPoint 97, PowerPoint MAC, PowerPoint PC</td>
</tr>
<tr>
<td>Password Protected Files</td>
<td>Encapsulation Format (password protected)</td>
<td>ZIP Archive</td>
</tr>
<tr>
<td>PGP Files</td>
<td>Encapsulation Format</td>
<td>ASCII-armored PGP encoded, ASCII-armored PGP Public Keyring, ASCII-armored PGP signed, PGP Compressed Data, PGP Encrypted Data, PGP Public Keyring, PGP Secret Keyring, PGP Signature Certificate, PGP Signed and Encrypted Data, PGP Signed Data</td>
</tr>
<tr>
<td>Publishing Documents</td>
<td>Desktop Publishing</td>
<td>FrameMaker, FrameMaker Book, Microsoft Publisher, PageMaker for Macintosh, PageMaker for Windows, Quark Xpress MAC</td>
</tr>
</tbody>
</table>
### Table 15-15  Default attachment lists (continued)

<table>
<thead>
<tr>
<th>Attachment list</th>
<th>True file class</th>
<th>Predefined true file type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC Fair Disclosure Regulation</td>
<td>Spreadsheet format</td>
<td>Applix Spreadsheets, CSV (Comma Separated Values), Lotus 1-2-3, Lotus 1-2-3 97, Lotus 1-2-3 Release 9, Microsoft Excel, Microsoft Excel 2000, Microsoft Excel 2007, Microsoft Excel 95, Microsoft Excel 97, Microsoft Excel Chart, Microsoft Excel Macro, Microsoft Excel XML, Microsoft Works for DOS Spreadsheet, Microsoft Works for MAC Spreadsheet, Microsoft Works for Windows Spreadsheet, Multiplan (Mac), Multiplan (PC), Quattro Pro for DOS, Quattro Pro for Windows, SYLK</td>
</tr>
<tr>
<td>True Type Executable Files</td>
<td>Executables</td>
<td>ELF Executable, MS-DOS Batch File, MSDOS Device Driver, MSDOS/Windows Program, PC (.COM), Unix Executable (3B20), Unix Executable (Basic-16), Unix Executable (Bell 5.0), Unix Executable (iAPX 286), Unix Executable (MC680x0), Unix Executable (PDP-11/pre-System V VAX), Unix Executable (VAX), Unix Executable (WE32000), Unix Executable (x86)</td>
</tr>
</tbody>
</table>

There are several true file classes that are not referenced by any Attachment List. These file classes and their associated true file types, however, can be accessed from within the File classes and File types lists the same way that other file classes and types can be selected. You can add any of these file types to an existing Attachment List or create a new Attachment List.

### Table 15-16  Additional file classes and types

<table>
<thead>
<tr>
<th>True file class</th>
<th>True file types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Format</td>
<td>Ability Communications, FTP Session Data, Microsoft Works for MAC Communications, SmartWare II Communications</td>
</tr>
<tr>
<td>FAX Format</td>
<td>DCX FAX Format (PCX images)</td>
</tr>
<tr>
<td>Font Type Document</td>
<td>NeWS bitmap font, SUN vfont, Definition TrueType Font</td>
</tr>
</tbody>
</table>
Table 15-16 Additional file classes and types (continued)

<table>
<thead>
<tr>
<th>True file class</th>
<th>True file types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mixed Type Document</td>
<td>Framework, Framework II, Windows C++ Object Storage</td>
</tr>
<tr>
<td>Planning/Outline Format</td>
<td>MORE Database MAC</td>
</tr>
</tbody>
</table>

See “About attachment lists” on page 401.

Creating lists to detect file attachment types

Use attachment lists in content filtering policy conditions to detect and act on email attachment file types. For example, you can assign an attachment list that detects messages with .exe file attachments as a condition in a content filtering policy. You can then specify what action you want Symantec Messaging Gateway to take if messages with an .exe file attachment are detected.

Symantec Messaging Gateway provides default attachment lists that you can use to create your attachment list. All of the attachments lists (default and custom) appear in the Conditions section on the Email Content Filtering Policy page. So you can conveniently select the attachment list that you want to use as a condition when you configure a content filtering policy.

When you create an attachment list, you can use any combination of true file classes, true file types, and common file extensions and MIME-types.

*Note:* MIME-type and file extension-based attachment lists are ineffective for stripping the attachments that are not described in the MIME header (for example, in the case of some forwarded messages). To ensure that you strip all instances of an attachment file type, configure your attachment lists to use true file type whenever possible.

To create an attachment list, you must have Full Administration rights or rights to modify policies.

See “About attachment lists” on page 401.

See “Editing attachment lists” on page 413.

To create lists to detect file attachment types

1. In the Control Center, click Content > Resources > Attachment Lists.
2. Click Add.
3. In the Attachment list name box, type a name for the attachment list.
4. Under Add Attachment Types, do any of the following tasks:
To add a true file class to your attachment list
Do all of the following tasks:

- Above the File classes list, click the radio button beside If the.
- Click the attachment type drop-down list and select True file class.
- In the File classes list, select the class or classes that you want to add to your attachment list.
  
  You can press and hold Ctrl to select multiple, non-consecutive items. You can also press and hold Shift to select consecutive blocks of items.

When you select a true file class, you add every true file type that is within that class to your attachment list. You cannot add or remove any file types.

To add a true file type to your attachment list
Do all of the following tasks:

- Above the File classes list, click the radio button beside If the.
- Click the attachment type drop-down list and select True file type.
  
  True file type is the default option.
- In the File classes list, select the true file class that contains the true file types that you want to add to your attachment list.
  
  You can press and hold Ctrl to select multiple, non-consecutive items. You can also press and hold Shift to select consecutive blocks of items.
  
  See “Default attachment lists” on page 402.
- In the File types box, select the true file types that you want to add to your attachment list.
To add a file extension based on file names, extensions, or MIME types

Do all of the following tasks:

- To add your own extension, under the File classes list, click the radio button beside If the.
- Click the Extension drop-down list and select one of the following options:
  - File name
  - Extension
    This value is the default.
  - MIME-type
- Click the is drop-down list and select one of the following options:
  - contains
  - begins with
  - ends with
  - is
    This value is the default.
- In the adjacent text box, type only one file name, extension, or MIME type.
  Type the MIME type completely, such as image or image/gif.

5 Click Add to add the attachment type to the attachment list.

6 Repeat steps 4 and 5 to add more attachment types to the attachment list.

7 Click Save.

Editing attachment lists

You can edit the custom attachment lists that you create. The default, premium attachment lists cannot be modified.

See “Default attachment lists” on page 402.

You can modify the list name, add file extensions to the list, or remove files extensions from the list.

To edit an attachment list, you must have Full Administration rights and rights to modify policies.

See “About attachment lists” on page 401.

To edit attachment lists

1 In the Control Center, click Content > Resources > Attachment Lists.

2 On the Attachment Lists page, check the box beside the custom attachment list that you want to modify, and then click Edit.

You can also click on the name of the attachment list to edit it.
3 Do any of the following tasks:
   ■ Modify the attachment list name.
   ■ Add file classes, file extensions, or file types to the list.
     See “Creating lists to detect file attachment types” on page 411.
   ■ In the Attachment Types list, select an attachment type that you want to remove, and
     then click Delete.

4 Click Save.

Deleting attachment lists

You can delete custom attachment lists when they are no longer needed. Premium attachment
lists cannot be deleted.

To delete an attachment list, you must first delete the condition to use that attachment list from
all of the content filtering policies in which it is used. Symantec Messaging Gateway lets you
know which policies use that attachment list when you attempt to delete it.

To delete an attachment list, you must have Full Administration rights or rights to modify
policies.

See “About attachment lists” on page 401.

To delete attachment lists

1 In the Control Center, click Content > Resources > Attachment Lists.

2 On the Attachment Lists page, check the box beside the attachment list that you want
to delete.

3 Click Delete.

A message appears at the top of the page to indicate the content filtering policies in which
a condition to use this attachment list occurs. Delete or modify this condition in these
policies first, then repeat this procedure.

See “Viewing, editing, adding, and managing your content filtering policies” on page 323.

Perl-compatible regular expressions

This section describes the Perl-compatible regular expressions that can be used in content
filtering policies.
### Table 15-17  Regular expression metacharacters

<table>
<thead>
<tr>
<th>Metacharacter/construct</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Period: Matches any single character of the input sequence.</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex: Represents the beginning of the input line. For example, ^A is a regular expression that matches the letter A at the beginning of a line. The ^ character is the only special character allowed at the beginning of a regular expression or after the ( or</td>
</tr>
</tbody>
</table>
| $                       | Dollar sign: Represents the end of the input line. For example, A$ is a regular expression that matches the letter A at the end of a line. The $ character is the only special character allowed at the end of a regular expression or before the ) or | characters.  
  Note that this metacharacter cannot be used for line-by-line matching in a message body. |
| *                       | Asterisk: Matches zero or more instances of the string to the immediate left of the asterisk. For example, A* matches A, AA, AAA, and so on. It also matches the null string (zero occurrences of A). |
| ?                       | Question mark: Matches zero or one instance of the string to the immediate left of the question mark.                                         |
| +                       | Plus sign: Matches one or more instances of the string to the immediate left of the plus sign.                                                |
| \                       | Escape: Turns on or off the special meaning of metacharacters. For example, \ only matches a dot character. \ matches a literal dollar sign character.  
  Note that \ matches a literal \ character.                                                                 |
| |                        | Pipe: Matches either expression on either side of the pipe. For example, exe|com|zip matches exe, com, or zip.                                                                 |
| [string]                | Brackets: Inside the brackets, matches a single character or collating element, as in a list. Characters within brackets are not case sensitive.  
  The string inside the brackets is evaluated literally, as if an escape character (\) were placed before each character in the string.  
  If the initial character in the bracket is a circumflex (^), then the expression matches any character or collating element except those inside the bracket expression.  
  If the first character after any potential circumflex (^) is a dash (-) or a closing bracket ()), then that character matches only a literal dash or closing bracket. |
Table 15-17  Regular expression metacharacters (continued)

<table>
<thead>
<tr>
<th>Metacharacter/construct</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parentheses: Groups parts of regular expressions, which gives the string inside the parentheses precedence over the rest.</td>
<td></td>
</tr>
</tbody>
</table>

See “Perl-compatible regular expression examples” on page 416.

Perl-compatible regular expression examples

Table 15-18 gives some examples of Perl-compatible expressions.

See “Perl-compatible regular expressions” on page 414.

Table 15-18  Sample Perl-compatible regular expressions

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
<th>Sample matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Match any one character</td>
<td>j.n</td>
<td>jen, jon, j2n, j$\n</td>
</tr>
<tr>
<td>..</td>
<td>Match any two characters</td>
<td>jo..</td>
<td>john, josh, jo4#</td>
</tr>
<tr>
<td>.*</td>
<td>Match zero or more characters</td>
<td>sara.*</td>
<td>sara, sarah, sarahjane, saraabc%123</td>
</tr>
<tr>
<td>.*</td>
<td></td>
<td>s.<em>m.</em></td>
<td>sm, sam, simone, s321m$xyz</td>
</tr>
<tr>
<td>.+</td>
<td>Match one or more characters</td>
<td>sara.+</td>
<td>sarah, sarahjane, saraabc%123</td>
</tr>
<tr>
<td>.+</td>
<td></td>
<td>s.+m.+</td>
<td>simone, s321m$xyz</td>
</tr>
<tr>
<td>\</td>
<td>Match a period</td>
<td>stop.</td>
<td>stop.</td>
</tr>
<tr>
<td>*</td>
<td>Match an asterisk</td>
<td>b*b**</td>
<td>b**</td>
</tr>
<tr>
<td>+</td>
<td>Match a plus character</td>
<td>18+</td>
<td>18+</td>
</tr>
<tr>
<td>/</td>
<td>Match a forward slash</td>
<td>18/</td>
<td>18/</td>
</tr>
<tr>
<td>[0-9]({n}</td>
<td>Match any numeral n times, for example, match a social security number</td>
<td>[0-9]({3}-[0-9]({2)-[0-9]({4}</td>
<td>123-45-6789</td>
</tr>
</tbody>
</table>
Specifying where to save archived messages

Your organization can maintain copies of the messages that violate specific policies. To use the archive feature, you must specify the action **Archive the message** when you create a content filtering policy.

You can also configure your archive email destination on a per-policy basis.

See “Policy actions and what they do” on page 333.

This feature can be useful to your organization in any of the following scenarios, just to name a few:

- You want to prepare for a potential lawsuit against an employee or other organization
- You must maintain records for regulatory compliance purposes
- You want to retain records for certain groups of employees

When messages trigger a policy violation with the action to **Archive the message**, Symantec Messaging Gateway copies the messages. It sends the copy to one or both an email address that you specify or an archive server.

To archive messages, you must have Full Administration rights or rights to modify policies.

**To specify where to save archived messages**

1. In the Control Center, click **Content > Settings > Archive**.
2. In the **Archive email address** box, type a complete email address, such as kyi@symantecexample.com.
3. In the **Archive server host** field, type the name of the archive server host.
   
   This server host is the host name or IP address for the archive email address that you provided in step 2.
4. If you provided an **Archive server host**, in the **Archive server port**, type the server host’s port number.
5. If you want to route archive messages with MX Lookup to locate the information that corresponds to the archive server host, check **Enable MX Lookup**.
6. To make the archive server information available to all of your existing policies, click **Apply to all current policies**.
7. Click **Save**.
Working with content filtered incidents

This chapter includes the following topics:

- Configuring content incident folders
- Monitoring and acting on incidents
- Encrypting data with Symantec Content Encryption
- Configuring Symantec Messaging Gateway to update data with Enforce Server

Configuring content incident folders

Table 16-1 describes how you can manage content incident folders. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn what content incident folders are and how they can help you manage content filtering incidents.</td>
<td>Content incident folders help you organize, monitor, and manage the incidents of content filtering policy violations. As a best practice, you should create a content incident folder for each type of content filtering policy that you use. For example, if you use the HIPAA template to create a policy, create a HIPAA content incident folder. You can use that folder to monitor HIPAA policy incidents. See “About content incident folders” on page 419.</td>
</tr>
</tbody>
</table>
Table 16-1  Manage content incident folders (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Familiarize yourself with how to keep the size of your folders</td>
<td>Symantec Messaging Gateway provides an Expunger that can manage the</td>
</tr>
<tr>
<td>manageable.</td>
<td>size of your content incident folders. The Expunger automatically runs</td>
</tr>
<tr>
<td></td>
<td>at the frequency that you specify.</td>
</tr>
<tr>
<td></td>
<td>See “About managing the size of content incident folders” on page 420.</td>
</tr>
<tr>
<td>Create a content incident folder.</td>
<td>Create content incident folders to help you organize, monitor, and manage</td>
</tr>
<tr>
<td></td>
<td>the incidents that content policy violations generate. You can have as</td>
</tr>
<tr>
<td></td>
<td>many as 1,000 folders including the default Informational Incidents and</td>
</tr>
<tr>
<td></td>
<td>Quarantine Incidents folders.</td>
</tr>
<tr>
<td></td>
<td>See “Creating content incident folders” on page 422.</td>
</tr>
<tr>
<td>Modify an existing content incident folder.</td>
<td>You can edit any content incident folder as needed.</td>
</tr>
<tr>
<td></td>
<td>See “Editing content incident folders” on page 425.</td>
</tr>
<tr>
<td>Delete an existing content incident folder.</td>
<td>You can delete a content incident folder that you create when you no</td>
</tr>
<tr>
<td></td>
<td>longer need it. However, you cannot delete the default Informational</td>
</tr>
<tr>
<td></td>
<td>Incidents folder or the Quarantine Incidents folder.</td>
</tr>
<tr>
<td></td>
<td>See “Deleting content incident folders” on page 425.</td>
</tr>
<tr>
<td>To maximum disk space, schedule an Expunger to remove messages in</td>
<td>Symantec Messaging Gateway provides an Expunger that manages the size of</td>
</tr>
<tr>
<td>content incident folders.</td>
<td>your content incident folders. You can specify the frequency at which you</td>
</tr>
<tr>
<td></td>
<td>want the Expunger to run.</td>
</tr>
<tr>
<td></td>
<td>See “Scheduling the content incident folder Expunger” on page 426.</td>
</tr>
</tbody>
</table>

About content incident folders

Content incident folders help you organize, monitor, and manage the incidents of content filtering policy violations. As a best practice, you should create a content incident folder for each type of content filtering policy that you use. For example, if you use the HIPAA template to create a policy, create a HIPAA content incident folder. You can use that folder to monitor HIPAA policy incidents.

Create the content incident folder before you configure a content filtering policy. That way, when you create a content filtering policy, the folder is an available option when you select the action to create an incident. If you do not specify a folder in which to create an incident, messages that violate that policy are filed in the Informational Incidents folder.

See “Creating a content filtering policy” on page 325.

When you create a content filtering folder, you must choose the type of folder you want to use.

Symantec Messaging Gateway provides the following types of content incident folders:
Hold for Review (Content Quarantine) Use this type of folder for the incidents that you want to review. This folder lets you retain the messages that trigger content filtering violations so that you can review them and determine how to act on them. Any additional actions for that policy are deferred until the incident is reviewed.

Note: Messages in the Hold for Review (Content Quarantine) folder are expunged based on the settings that you specify, even if they have not been reviewed.

These folders appear in the Control Center as Quarantine Incidents.

See “About managing the size of content incident folders” on page 420.

Informational Incidents Use this type of folder to track the incidents that are at a lower priority than the ones that you want to hold for review.

You can also configure the following settings for each folder:

- Archive tag and encoding for the tag
  This setting is optional.

- Expunger settings
  The maximum content incident folder size is required. The setting for the number of days to hold an incident before it is expunged is optional.

- Notification message that indicates an incident has been logged to that folder and the people that you want to receive the notification
  This setting is optional.

Symantec Messaging Gateway supports up to 1,000 content incident folders, including the default Informational Incidents and Quarantine Incidents folders. You must have Full Administration rights or rights to modify settings to create content incident folders.

See “Creating content incident folders” on page 422.

About managing the size of content incident folders

Your content incident folders can fill up quickly and consume a lot of disk space when one or both of the following conditions exist:

- You have a large number of content filtering policies whose actions are to create incidents in content incident folders.

- You have a large number of messages that violate policies.

Symantec Messaging Gateway provides an Expunger that can manage the size of your content incident folders. The Expunger automatically runs at the frequency that you specify.

When the Expunger runs, it expunges incidents from your content incident folders based on the following criteria:
By the maximum content incident folder size

The maximum content incident folder size is the sum of the block size (the size on disk) of each message file in the folder. The actual disk usage may be higher.

When a folder reaches its maximum size, a message is sent to the BrightmailLog.log. When the folder reaches the maximum size that you specify for alerts (for example, 120% of the maximum size), then an alert is sent. Only one alert is sent if multiple folders reach their maximum size at the same time. However, you continue to receive alert emails to notify you of any subsequent folders that exceed their maximum size. The oldest incidents are deleted until the folder returns to its maximum size.

See “Configuring alerts” on page 688.

Symantec recommends that you expunge folders based on size while you fine-tune content filtering policies. Then you can modify the Expunger settings as desired.

You must specify a maximum content incident folder size. The default maximum size is 5 GB, but you can modify this setting.

By the number of days that you want to store incidents

Optionally, you can specify the number of days to store an incident before the Expunger performs one of the following actions:

- Approve
  This option is only available for content quarantine incident folders. After the Expunger approves the incident, it is deleted from the folder.

- Reject
  This option is only available for content quarantine incident folders. After the Expunger rejects the incident, it is deleted from the folder.

- Custom
  This action is the custom action that you specify when you create a policy action to create a quarantine incident. This option is only available for content quarantine incident folders. After the Expunger applies the custom action on the folder, the action that is taken on the incidents is the action that is defined in the policy.

- Delete
  This option is available for both content quarantine incident folders and informational incident folders.

See “Adding actions to a content filtering policy” on page 332.

**Note:** When this threshold is met, incidents in quarantine incident folders are expunged, even if they have not been reviewed. Symantec Messaging Gateway takes the action that you specify in the content filtering policy, starting with the oldest incidents. Symantec Messaging Gateway determines the age of an email based on the time that the message is received.
You configure your Expunger criteria when you create the content incident folder. You can specify one or both the folder size thresholds and days to store thresholds. You can also modify the settings at any time thereafter. When a threshold is met, no further incidents are created in the folder.

See “Creating content incident folders” on page 422.

The Expunger cycle applies to all content incident folders.

See “Scheduling the content incident folder Expunger” on page 426.

See “About content incident folders” on page 419.

Creating content incident folders

Create content incident folders to help you organize, monitor, and manage the incidents that content policy violations generate. You can have as many as 1,000 folders including the default Informational Incidents and Quarantine Incidents folders.

To create a content incident folder, you must have Full Administration rights or rights to modify policies.

See "About content incident folders" on page 419.

See “Editing content incident folders” on page 425.

See “Scheduling the content incident folder Expunger” on page 426.

See “Deleting content incident folders” on page 425.

To create content incident folders

1 In the Control Center, click Content > Settings > Content Incident Folders.

2 Click Add.

3 In the Content Incident folder name field, type a name for the content incident folder. As a best practice, you should use a name that reflects the type of content that you intend to collect in that folder. For example, if you want to place the messages that violate a HIPPA policy in this folder, you might name the folder HIPPA.

4 Click the Content incident folder type drop-down list to select the type of folder you want to use.

5 Optionally, in the Optional archive tag field, type the text that you want to identify this folder with for archival purposes.

When you specify an archive action on an incident in this content incident folder, that text accompanies the incident.

6 If you specified an incident archive tag, in the Encoding drop-down list, choose the character encoding set to use for the tag text.
7 Check **Enable message submission buttons within this folder** to enable submission functionality.

This option only appears if you have enabled the customer-specific spam submission feature.

See “About submitting messages for customer-specific spam rules” on page 265.

8 Under **Expunger Settings** do the following tasks:

To specify the number of days to retain incidents before they are expunged (optional)

- Check **Days to store before default action occurs**, and in the field beside it, type the number of days.
- Under **Default expunger action**, specify the action that you want to take when an incident is expunged.
  
  If the folder is an **Informational Incidents** folder, the only options available are **Delete**.

To specify a maximum folder size (required)

- Under **Thresholds**, specify the size in kilobytes, megabytes, or gigabytes.

See “About managing the size of content incident folders” on page 420.

9 Optionally, click the **Notification format** drop-down list and select the format for incident notifications.

This notification is sent to whomever you specify in step 11 and step 12 that indicates that an incident is added to this folder.

See “Creating incident notifications” on page 430.

10 Click **Edit** to view or edit the incident notification template.

11 In the **Notification recipient addresses** field, type the email addresses of the content filtering officers who should be notified of incidents in this folder.

Separate multiple addresses with commas, semicolons, or spaces.

12 In the **Administrator Notifications** list, check the names of administrators whom you want to be notified of incidents in this folder. If you do not want to have notifications sent, leave this field blank.

You can specify administrators to notify of incidents in this folder when you add administrators or modify administrator settings.

13 Click **Save**.

**Content filtering notification variables**

In the notification message text, Symantec Messaging Gateway replaces the default variable `%NEW_COMPLIANCE_MESSAGES%` with a list of incident numbers and the policies that
triggered those incidents. You can type text before or after this variable. You can also modify this variable to meet more specific needs.

For example, you can type the following text to precede the variable and replace Name with the folder name:

New incidents have been created. Please access the Name Content Incident Folder for incident details.

Table 16-2 lists the content filtering notification variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%NEW_COMPLIANCE_MESSAGES%</td>
<td>Lists the incident numbers and the policies that triggered those incidents.</td>
</tr>
<tr>
<td>%NEW_COMPLIANCE_MESSAGES_DETAILED%</td>
<td>Provides more detailed information about incidents. For example, the incident ID, to, from, subject, and attachment details and the name of the incident folder that contains the incident.</td>
</tr>
<tr>
<td>%NEW_COMPLIANCE_MESSAGES_REMEDIATION_REQUIRES_AUTHENTICATION%</td>
<td>Specifies the policy that was violated and the message's From, To, Subject, and Date details. Provides the links that users can click to remediate the quarantined incident. Also requires the user to authenticate to Symantec Messaging Gateway to remediate.</td>
</tr>
<tr>
<td>%NEW_COMPLIANCE_MESSAGES_REMEDIATION_AUTO_AUTHENTICATION%</td>
<td>Specifies the policy that was violated and the message's From, To, Subject, and Date details. Provides the links that users can click to remediate the quarantined incident. However, it does not require the user to authenticate to Symantec Messaging Gateway to remediate.</td>
</tr>
<tr>
<td>%NEW_INFORMATIONAL_INCIDENT_MESSAGES_REQUIRES_AUTHENTICATION%</td>
<td>Specifies the policy that was violated and the message's From, To, Subject, and Date details. Provides the links that users can click to remediate the informational incident. Also requires the user to authenticate to Symantec Messaging Gateway to view the incident's details.</td>
</tr>
<tr>
<td>%NEW_INFORMATIONAL_INCIDENT_MESSAGES_AUTO_AUTHENTICATION%</td>
<td>Specifies the policy that was violated and the message's From, To, Subject, and Date details. Provides the links that users can click to remediate the informational incident. However, it does not require the user to authenticate to Symantec Messaging Gateway to view the incident's details.</td>
</tr>
</tbody>
</table>

See “About remediating incidents from email notifications” on page 432.
Editing content incident folders

You can edit any content incident folder as needed. To edit a content filtering folder, you must have Full Administration rights or rights to modify policies.

See “About content incident folders” on page 419.
See “Deleting content incident folders” on page 425.
See “Creating content incident folders” on page 422.

To edit content incident folders

1. In the Control Center, click **Content > Settings > Content Incident Folders**.
2. Check the box beside the content incident folder that you want to edit, and then click **Edit**.
   
   You can also click on the content incident folder name to edit it.
3. Edit the content incident folder settings as necessary.
4. Click **Save**.

Deleting content incident folders

You can delete a content incident folder that you create when you no longer need it. However, you cannot delete the default Informational Incidents folder or the Quarantine Incidents folder.

Before you delete a folder, you may want to ensure that all of the items in the folder have been reviewed and addressed as needed. You must also delete the action to log incidents to the folder from any content filtering policies in which it is used. Symantec Messaging Gateway lets you know which policies use that folder in an action when you attempt to delete it.

To delete a content incident folder, you must have Full Administration rights or rights to modify policies.

See “About content incident folders” on page 419.
See “Editing content incident folders” on page 425.
See “Scheduling the content incident folder Expunger” on page 426.

To delete content incident folders

1. In the Control Center, click **Content > Settings > Content Incident Folders**.
2. Check the box beside the content incident folder that you want to delete.
   
   Check the box beside **Content Incident Folders** to select all of the folders.
3 Click **Delete**.

4 In the confirmation dialog, click **Delete**.

A message appears at the top of the page to indicate the content filtering policies in which an action to log incidents to this folder occurs. Delete or modify this action in these policies first, then repeat this procedure.

### Scheduling the content incident folder Expunger

Symantec Messaging Gateway provides an Expunger that manages the size of your content incident folders. You can specify the frequency at which you want the Expunger to run. The default frequency is every day at 4:00 A.M. When the Expunger runs, it takes the default actions that you specify in your content filtering policies. Then it deletes the incidents based on the threshold criteria: folder size or days to store in the folder.

See “Creating content incident folders” on page 422.

See “About managing the size of content incident folders” on page 420.

See “About content incident folders” on page 419.

You can check the status of your scheduled task from the **Status > Scheduled Tasks** page.

See “About scheduled tasks” on page 648.

You must have Full Administration or rights to modify settings to schedule the content incident folder Expunger.

See “Administrator rights” on page 661.

**To schedule the content incident folder Expunger**

1 In the Control Center, click **Content > Settings > Content Incident Folders**.

2 Under **Content Filtering Expunging Cycle**, in the **Incident expunger frequency** drop-down list, select how often you want the Expunger to run.

3 In the **Incident expunger start time** drop-down lists, specify the hour and minute in which you want the Expunger to run.

4 Click **Save**.

### Configuring message submission options to appear in quarantine incident folders

Administrators can submit messages from quarantine incident folders to Symantec for customer-specific rules. However, you must first configure these options to appear for each content quarantine incident folder in which you want this feature to be available. When you enable this option, administrators see the options **This is Spam** and **This is NOT Spam** in the details page of the incident.
**Note:** This feature is not available for informational incident folders.

You must have Full Administration rights or Manage Setting modify rights to configure this option.

**To configure message submission options to appear in quarantine incident folders**

1. In the Control Center, click **Content > Settings > Content Incident Folders**.
2. On the **Content Incident Folder Settings** page, either add a new content quarantine incident folder or edit an existing one.
3. On the **Add/Edit Content Incident Folder** page under **Submissions**, check **Enable message submission buttons within this folder**.
4. Click **Save**.

See “Creating content incident folders” on page 422.

See “Editing content incident folders” on page 425.

See “Setting up customer-specific spam submissions” on page 268.

See “Monitoring and acting on incidents” on page 427.

### Monitoring and acting on incidents

Content incident folders let you monitor incidents and determine whether a policy needs to be adjusted. They also let you manage the incidents that Symantec Messaging Gateway detects based on the policies that you configure.

**Table 16-3** describes how you can monitor incidents and manage them. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Learn more about what you can do with messages in content incident folders. | Content incident folders contain incidents of the messages that violate a policy's conditions. Information about incidents can help you understand, prevent, respond to, and audit potential violations.  
See “About monitoring and acting on incidents” on page 429. |
| Notify the content administrators that messages are in content incident folders. | Symantec Messaging Gateway can notify the persons that you specify that an incident has been added to a content incident folder. Symantec Messaging Gateway provides a default notification message that you can modify as necessary.  
See “Creating incident notifications” on page 430. |
Table 16-3  Monitor and act on incidents (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the incidents that are in content incident folders.</td>
<td>This topic describes what you can do on the Incident Management page. See “Viewing incidents in content incident folders” on page 433.</td>
</tr>
<tr>
<td>Perform the same action on multiple incidents.</td>
<td>You can perform the same action on multiple incidents at a time. For example, you might want to reject all of the incidents that are from a specific sender. See “Acting on multiple incidents at a time” on page 434.</td>
</tr>
<tr>
<td>Submit the message for a custom rule.</td>
<td>You can notify Symantec that the message was missed spam or a false positive. Based on this information, Symantec creates a custom rule that can improve spam detection and help administrators control false positive incidents.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This feature is only available for quarantine incident folders.</td>
</tr>
<tr>
<td></td>
<td>See “Submitting messages from quarantine folders for customer-specific rules” on page 443.</td>
</tr>
<tr>
<td>Familiarize yourself with the actions that you can perform within content incident folders.</td>
<td>This topic describes the actions that you can take on incidents in content incident folders. See “Content incident actions” on page 435.</td>
</tr>
<tr>
<td>Archive messages after you review them.</td>
<td>After you review incidents and take the action that you want, you can archive the message. You can archive one or more messages from the Incident Manager page or one at a time from an incident's detail page. See “Archiving incidents” on page 436.</td>
</tr>
<tr>
<td>Export an incident's history.</td>
<td>You can export all of the information about an incident's history. For example, when the incident is created, when a status changed, message review actions, and comments. You can select the encoding that you want to use for the exportation and the delimiter. See “Exporting an incident's history” on page 440.</td>
</tr>
<tr>
<td>Forward an incident.</td>
<td>You can forward incidents in incident folders for further review. When you forward an incident, you can create a comment for the person to whom you forward the message to provide instructions or deadlines. You can also specify whether you want to attach the original message. See “Forwarding incidents” on page 441.</td>
</tr>
</tbody>
</table>
Table 16-3  Monitor and act on incidents (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete an incident after you review it.</td>
<td>Symantec recommends that after you review and act on incidents, you delete them to reduce the volume of incidents in your incidents folders. When an incident is deleted, it no longer appears in the incident folder, and the incident cannot be retrieved. See “Deleting incidents” on page 442.</td>
</tr>
<tr>
<td>Act on an incident.</td>
<td>After you review an incident in a Quarantine Incidents folder, you can approve it, reject it, perform a custom action, or continue to hold it. When you remediate an incident in a Quarantine Incidents folder, Symantec Messaging Gateway takes the action that you specified in the content filtering policy actions for Message Review Approved Actions, Message Review Rejected Actions, and Message Review Custom Actions. See “Remediating quarantined incidents” on page 444.</td>
</tr>
<tr>
<td>Update an incident's status to monitor its progress.</td>
<td>You can update an incident's status to reflect changes to the incident. The incident's status lets reviewers know what stage of the review process the incident is currently in and what the results of the review are. See “Updating an incident's status” on page 445.</td>
</tr>
<tr>
<td>Modify an incident's severity level.</td>
<td>As you review an incident, you can modify its severity level. See “Changing an incident's severity level” on page 446.</td>
</tr>
<tr>
<td>View an incident's history.</td>
<td>You can view the history of an incident to see how the incident has progressed. See “Viewing an incident's history” on page 447.</td>
</tr>
</tbody>
</table>

About monitoring and acting on incidents

Content incident folders contain incidents of the messages that violate a policy's conditions. Information about incidents can help you understand, prevent, respond to, and audit potential violations. For example, you can use an incident folder to monitor content filtering policy violations at your company before you adopt permanent policies.

See “About content incident folders” on page 419.

Content incident folders store the incidents that let you do the following:
Monitor incidents in informational incidents folders

You can monitor the incidents that occur, but you do not have to act on them.

You must create a content filtering policy in which at least one action is to create an informational incident in the folder that you specify. If a policy violation occurs, an incident is created in that informational incidents folder for you to review at your convenience.

Hold incidents for review and remediation in quarantine incidents folders

You can hold messages in a quarantine incident folder for you to review and determine the action that you want to take.

The content filtering officer can perform any of the following tasks:
- Approve the incident.
- Reject the incident.
- Perform a custom action.
- Delete the incident.

You must create a policy in which at least one action is to create a quarantine incident in the folder that you specify. If a policy violation occurs, an incident is created in that folder for your review and action.

Messages that are held in content incident folders remain there until they are remediate or expunged by the Expunger.

See “Viewing incidents in content incident folders” on page 433.

See “Adding actions to a content filtering policy” on page 332.

See “Content incident actions” on page 435.

See “About managing the size of content incident folders” on page 420.

Creating incident notifications

Symantec Messaging Gateway can notify the persons that you specify that an incident has occurred. Symantec Messaging Gateway provides a default notification message that you can modify as necessary.

You can customize notification messages such that recipients can view or remediate the incident by clicking a link in the email notification message. The link takes the user to the Control Center page where they address the incident. You can also specify whether users must type their credentials to access the Control Center when they click the link or if they can auto-authenticate.

See “About remediating incidents from email notifications” on page 432.

See “Content filtering notification variables” on page 423.

See “Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway” on page 471.
You can have one notification message for each incident folder. That message can be unique or it can be the same message that you use for a different incident folder.

---

**Note:** This notification differs from the Notifications resource. The Notifications resource lets you send notification messages to the message sender, message recipient, or a third party to indicate that a policy is violated. The Notifications resource is the notification that is sent when the policy action is to Send notification.

See “About policy violation notifications” on page 377.

---

You must have Full Administration or rights to modify settings to create incident notifications.

See “Administrator rights” on page 661.

**To create incident notifications**

1. In the Control Center, click Content > Settings > Content Incident Folders.
2. In the **Content Incident Folder** list, click on the name of a content incident folder for which you want to create an incident notification message.

   Alternatively, check the box beside the name of the content incident folder, and click **Edit**.

3. On the **Content Incident Folder Settings** page under **Notification Settings**, click the **Notification format** drop-down list and select the format that you want to use the notification message.

   You can select multi-part (HTML and text), HTML only, or text only.

4. If you want to modify the notification message, click **Edit** beside **Notification template**.

5. On the **Notification template** page, under **Encoding Type**, click the drop-down list and select the character encoding for the notification message.

6. In the **Send from** box, type the address of the **From** header to appear in incident notification messages.

7. In the **Subject** box, type the **Subject** header that you want to appear on the incident notification messages.

8. In the **Notification** box, modify the text as desired.

9. Click **Save**.

10. In the **Maximum summary entries per notification** field, type the maximum number of entries that you want to appear in a notification message.

11. Click the **Notification Frequency** drop-down list and specify how frequently you want Symantec Messaging Gateway to send notifications.

12. In the **Notification Start Time**, click the drop-down menu and specify the time of day that Symantec Messaging Gateway starts to send notifications.
To specify who should receive this notification, do any of the following tasks:

To notify an administrator
Under Administrator Notifications, check the box beside the administrators that you want to receive this notification.

To notify people who are not administrators
In the Notification recipient addresses box, type the email addresses of anyone that you want to receive the notification message.
Separate multiple entries with commas.

Click Save.

About remediating incidents from email notifications
You can configure Symantec Messaging Gateway to send notifications to administrators or notification recipients to notify them that a content filtering incident was created. You can also specify how frequently you want notifications to be sent and the maximum number of incidents to include in a notification message.

See “Creating content incident folders” on page 422.

By default, the notification message contains a short description of each incident. However, you can customize the notification message to contain the links that take users to the Control Center page where they can address incidents. You can also specify whether users can auto-authenticate or if they must type their credentials to access the Control Center before they can remediate incidents.

See “Content filtering notification variables” on page 423.

If an incident is in an informational folder, the notification message contains a link to view the incident. If an incident is in a quarantine incident folder, the message contains links to view and remediate the incident. To remediate the incident, users can approve it, reject it, or apply the custom action (if a custom action is defined).

See “Adding actions to a content filtering policy” on page 332.

Users who have Control Center access rights are taken to the appropriate folder incident page in the Control Center. From this page, they can view and remediate incidents. Users who do not have Control Center access rights see a page within the Control Center that displays the summary details of the message. However, these users cannot see any other pages or navigate to any other location within the Control Center.

For users who can auto-authenticate, the link that they click in the notification is automatically applied to the incident. Users who must authenticate are taken to the Control Center login page where they must type their credentials. Upon login, those users are automatically taken to the page where they can view or remediate the incident. Both administrators and notification recipients can be permitted to auto-authenticate.
Note: You must permit users who do not have Control Center access rights to auto-authentication. Otherwise, they cannot see the details of the incident or be able to remediate quarantine incidents.

If you integrate with Enforce Server, the actions that are taken when users click remediation links are updated on the Enforce Server administration console after the next update occurs.

See “Configuring Symantec Messaging Gateway to update data with Enforce Server” on page 453.

Viewing incidents in content incident folders

You can do any of the following tasks on the Incident Management page to view your incidents:

- Use a filter to narrow or expand your search of incidents.
- View details about a particular incident from this page.
- Sort columns by ascending order or descending order.

Use the Folder Overview link for a high-level summary of all your content incident folders or a single folder at a time.

Symantec Messaging Gateway provides the following tools on the Incident Management page to help you customize your view and navigate through your incidents:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entries per page</td>
<td>This setting lets you specify how many entries you want to display per page. You can specify 10, 25, 50, 100, 200, or 500.</td>
</tr>
<tr>
<td>Display</td>
<td>This setting lets you specify which range of entries you want to display.</td>
</tr>
<tr>
<td>Forward and back arrows</td>
<td>Use the back &lt;</td>
</tr>
</tbody>
</table>

Incidents remain in content incident folders until you act on them (delete or archive) or the incidents are expunged.

To view the contents of incident folders, you must have Full Administration rights or rights to access each content incident folder separately.
To view a summary of what is in your content incident folders

1 In the Control Center, click **Content > Folder Overview**.
   By default, all of your folders appear in the **Content Incident** table.

2 In the **Content incident folder** drop-down list, select the folder for which you want to see an overview.

3 Click **Display**.
   The status appears in the **Content Incident Folders** table.

To view incidents in content incident folders

1 In the Control Center, click **Content**.

2 In the **Incident Management** task pane, select the folder that contains the incidents that you want to view.

   See “How the matching text feature is affected by upgrade for existing content” on page 449.

   See “About monitoring and acting on incidents” on page 429.

   See “About managing the size of content incident folders” on page 420.

   See “Content incident actions” on page 435.

**Acting on multiple incidents at a time**

You can perform the same action on multiple incidents at a time. For example, you might want to reject all of the incidents that are from a specific sender.

   See “Content incident actions” on page 435.

To act on incidents in incident folders, you must have Full Administration rights or rights to access each content incident folder separately.

To act on multiple incidents at a time

1 In the Control Center, click **Content**.

2 In the **Incident Management** task pane, select the folder that contains the incidents that you want to act on.

3 Check the box beside the incident ID for all of the incidents that you want to act on.

   Check the box beside the Incident ID column heading to select all of the incidents that appear on the page.
4 Click the option for the task that you want to take on all of the incidents that you selected. See “About monitoring and acting on incidents” on page 429.

5 Take the necessary steps to complete the action.

For example, if you want to export incidents, you must specify the location to where you want the files exported.

Content incident actions

Table 16-4 lists the actions that you can take on incidents in content incident folders.

Table 16-4  Content incident actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive</td>
<td>Archives incidents. You can archive a single incident at a time or multiple incidents at once. See “Archiving incidents” on page 436.</td>
</tr>
<tr>
<td>Export Incident History</td>
<td>Exports an incident's history to the location that you specify. You can export a single incident's history at a time or multiple incident histories at once. See “Exporting an incident's history” on page 440.</td>
</tr>
<tr>
<td>Forward an incident</td>
<td>Forwards an incident to the email address that you specify. You can add a subject to your email and a comment. You can also select the message encoding and specify whether you want to forward your message with the original message. You can forward a single incident at a time or multiple incidents at once. See “Forwarding incidents” on page 441.</td>
</tr>
<tr>
<td>Delete an incident</td>
<td>Deletes a single incident at a time or multiple incidents at once. See “Deleting incidents” on page 442.</td>
</tr>
<tr>
<td>RemEDIATE an incident</td>
<td>Specifies how to act on a quarantined incident. When you remEDIATE an incident in a quarantine incidents folder, Symantec Messaging Gateway takes the action that you specified for the content filtering policy actions: Message Review Approved Actions, Message Review Rejected Actions, and Message Review Custom Actions. You can remEDIATE a single incident at a time or multiple incidents at once. You can specify to hold only a single incident at a time. See “Remediating quarantined incidents” on page 444.</td>
</tr>
</tbody>
</table>
### Table 16-4  Content incident actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update incident status</td>
<td>Specifies the status of an incident. The status options are as follows: ■ New ■ Active ■ Confirmed ■ False positive You can only change the status of a single incident at a time. See “Updating an incident's status” on page 445.</td>
</tr>
<tr>
<td>Modify an incident's severity</td>
<td>Specifies the severity of an incident. The severity levels are as follows: ■ Unknown ■ High ■ Medium ■ Low You can only change the severity of a single incident at a time. See “Changing an incident's severity level” on page 446.</td>
</tr>
<tr>
<td>Review an incident's history</td>
<td>Shows the entire history of an incident. The history can include when the incident is created, when a status or severity is changed, or when an action is taken. The incident history contains the date and time that the event occurred and any comments that you create in connection with the event. You can only view the history of one incident at a time. See “Viewing an incident's history” on page 447.</td>
</tr>
</tbody>
</table>

See “About monitoring and acting on incidents” on page 429.
See “About content incident folders” on page 419.
See “Viewing the text that violated a content filtering policy” on page 447.

### Archiving incidents

After you review incidents and take the action that you want, you can archive the message. You can archive one or more messages from the Incident Manager page or one at a time from an incident's detail page.

See “About monitoring and acting on incidents” on page 429.
See "Specifying where to save archived messages" on page 417.

To archive incidents, you must have Full Administration rights or rights to view the specific content incident folder.

To archive incidents from the Incident Management page

1. In the Control Center, click **Content**.
2. Under **Incident Management**, select the folder that contains the incident that you want to review and archive.
3. Check the box beside one or more incidents that you want to archive.
4. Click **Archive**.

To archive incidents from the Incident Management details page

1. In the Control Center, click **Content**.
2. Under **Incident Management**, select the folder that contains the incident that you want to review and archive.
3. In the **Incident ID** column, click on the incident number that you want to review and archive.
4. On the **Incident Management** details page, in the right pane under **Incident Actions**, click **Archive**.

**Monitoring your spam email submissions**

You can monitor the submissions that your organization has made for customer-specific rules in the Control Center.

Below are some details that you can ascertain from spam submission details:

- Which users submit messages most often.
- Which types of messages (missed spam or false positives) are most frequently submitted.
- Whether there is an unusually high number of submissions from a specific email sender or to an intended recipient.
- Whether the message that was submitted was valid and, therefore, resulted in a custom rule. And if it was invalid, why.
- Whether the rule that was created as a result of that submission is currently active. If so, for how many messages has that rule detected violations.

The Control Center lets you filter spam submissions so that you can more easily find the information you want. Click on any item in the search results to view the **Submissions Details** page, which provides more information about the submission and the related message.

See "How rules are created and why messages may not result in custom rules" on page 267.
You must have Full Administration, Manage Spam Submissions, or Manage Status and Logs view or modify rights to view the Submissions and Submissions Detail pages.

Monitoring your spam email submissions

1. In the Control Center, click Status > Submissions > Submission Detail.

2. On the Submissions page, click the Submission type drop-down menu to specify the type of submissions that you want to filter for.
   You can select from any of the following options:
   - No restriction
   - Missed Spam
   - Misidentified as Spam

3. Click the Submitter type drop-down menu and select the category of submitter.
   You can select from the following options:
   - All
   - Admin
   - Blocked
   - End-user

4. Click the Time range drop-down menu to specify when the message was submitted.
   You can select from any of the following options:
   - Past hour
   - Past day
   - Past week
   - Past month
   - Customize
     - When you select this option you can specify the start date and time and the end date and time.

5. Click the Subject drop-down menu to specify the subject of the message.
   Specify the subject content based on the following search criteria:
   - matches/does not match
     - Specify the match/does not match criteria as follows:
       - substring (case-sensitive)
       - substring (case-insensitive)
- exactly (case-sensitive)
- exactly (case-insensitive)
- wildcard expression
  This field accepts the following punctuation characters: dot (.), at sign (@), hyphen (-), and underscore (_). The asterisk (*) is recognized as a wildcard metacharacter.
- Type the string, text, or wildcard expression in the adjacent text box.

6 Specify a specific submitter email address based on the following search criteria:
- matches/does not match
- Specify the match/does not match criteria as follows:
  - substring (case-sensitive)
  - substring (case-insensitive)
  - exactly (case-sensitive)
  - exactly (case-insensitive)
  - wildcard expression
  This field accepts the following punctuation characters: dot (.), at sign (@), hyphen (-), and underscore (_). The asterisk (*) is recognized as a wildcard metacharacter.
- Type the string, text, or wildcard expression in the adjacent text box.

7 Specify a specific sender based on the following search criteria:
- matches/does not match
- Specify the match/does not match criteria as follows:
  - substring (case-sensitive)
  - substring (case-insensitive)
  - exactly (case-sensitive)
  - exactly (case-insensitive)
  - wildcard expression
  This field accepts the following punctuation characters: dot (.), at sign (@), hyphen (-), and underscore (_). The asterisk (*) is recognized as a wildcard metacharacter.
- Type the string, text, or wildcard expression in the adjacent text box.

8 Specify the intended recipient based on the following search criteria:
- matches/does not match
- Specify the match/does not match criteria as follows:
■ substring (case-sensitive)
■ substring (case-insensitive)
■ exactly (case-sensitive)
■ exactly (case-insensitive)
■ wildcard expression
   This field accepts the following punctuation characters: dot (.), at sign (@), hyphen (-), and underscore (_). The asterisk (*) is recognized as a wildcard metacharacter.
■ Type the string, text, or wildcard expression in the adjacent text box.

9 Select either of the following options:

Clear Filters  Clears the current filtering criteria from memory.
Display Filtered  Searches for and display the messages that fit your criteria.
   When you select this option, the matching submissions appear in the table.

10 To view more information about a specific submission, click the item to view the Submission Details page.

11 Optionally, if you want to export the results of your search, do all of the following steps:
   ■ Click Export CSV.
   ■ In the Export Submission Status dialog box, click the File Encoding drop-down list and specify the type of encoding that you want to use.
   ■ Click the CSV Delimiter drop-down list and select the delimiter type.
   ■ Click Export.

See “About submitting messages for customer-specific spam rules” on page 265.

Exporting an incident's history

You can export all of the information about an incident's history. For example, when the incident is created, when a status changed, message review actions, and comments. You can select the encoding that you want to use for the exportation and the delimiter.

You can export one or more incident histories at a time. To export an incident's history, you must have Full Administration rights or rights to view the specific content incident folder.

See “About monitoring and acting on incidents” on page 429.
See “Viewing an incident's history” on page 447.
To export an incident's history

1. In the Control Center, click Content.
2. Under Incident Management, select the folder that contains the incident history that you want to export.
3. Check the box beside one or more incidents whose histories you want to export.
4. Click the Encoding drop-down list to select the encoding.
5. Click the Delimiter drop-down list to select the delimiter that you want to use.
6. Click Export Incident History to export an incident history.
7. Select whether you want to save the file or open it. If you save the file, browse and select the desired location.

Forwarding incidents

You can forward incidents in incident folders for further review. When you forward an incident, you can create a comment for the person to whom you forward the message to provide instructions or deadlines. You can also specify whether you want to attach the original message.

You can forward one or more messages from the Incident Management page or one incident at a time from an incident's detail page.

To forward incidents, you must have Full Administration rights or rights to modify the specific content incident folder.

See “About monitoring and acting on incidents” on page 429.

To forward incidents from the Incident Management page

1. In the Control Center, click Content.
2. Under Incident Management, select the folder that contains the incident that you want to review and forward.
3. Check the box beside one or more incidents that you want to forward.
4. Click Forward Incident.
5. On the Forwarding Message page, under Encoding, click the drop-down list to select the encoding type.
6. Under Message Content, in the Forward to text box, type the email address.
7. In the Subject text box, type a subject name.
8. Check Forward with original message if you want to forward the message without any modifications.
   This action forwards the message in its original state with no policy-based actions that can affect the message (for example, removing or cleaning attachments).
To forward incidents from the Incident Management details page

1. In the Control Center, click **Content**.
2. Under **Incident Management**, select the folder that contains the incident that you want to review and forward.
3. In the **Incident ID** column, click on the incident number that you want to review and forward.
4. On the **Incident Management** details page, in the right pane under **Incident Actions**, click **Forward**.
5. On the **Forwarding Message** page, under **Encoding**, click the drop-down list to select the encoding type.
6. Under **Message Content**, in the **Forward to** text box, type the email address.
7. In the **Subject** text box, type a subject name.
8. Check **Forward with original message** if you want to forward the message without any modifications.
   
   This action forwards the message in its original state with no policy-based actions that can affect the message (for example, removing or cleaning attachments).
9. In the **Comments** text box, type the message that you want to accompany the email.
10. Click **Send**.

Deleting incidents

Symantec recommends that after you review and act on incidents, you delete them to reduce the volume of incidents in your incidents folders. When an incident is deleted, it no longer appears in the incident folder, and the incident cannot be retrieved.

Incidents that meet expunger thresholds are automatically deleted.

See “About managing the size of content incident folders” on page 420.

You can delete one or more messages from the Incident Manager page or one incident at a time from an incident's detail page.

To delete an incident, you must have Full Administration rights or rights to view the specific content incident folder.

See “About monitoring and acting on incidents” on page 429.
To delete incidents from the Incident Management page

1. In the Control Center, click **Content**.

2. Under **Incident Management**, select the folder that contains the incident that you want to review and delete.

3. Check the box beside one or more incidents that you want to delete.

4. Click **Delete**.

   Optionally, you can click **Delete All** to delete all of the incidents on the page, and in the confirmation dialog box, click **OK**.

To delete incidents from the Incident Management details page

1. In the Control Center, click **Content**.

2. Under **Incident Management**, select the folder that contains the incident that you want to review and delete.

3. In the **Incident ID** column, click on the incident number that you want to review and delete.

4. On the **Incident Management** details page, in the right pane under **Incident Actions**, click **Delete**.

Submitting messages from quarantine folders for customer-specific rules

You can submit the messages that are in content quarantine incident folders to Symantec for customer-specific rules. However, an administrator must have first configured these options to appear in the content incident folder.

---

**Note:** This option is not available for informational incident folders.

See “Configuring message submission options to appear in quarantine incident folders” on page 426.

You must have Full Administration rights or Manage Spam Submissions modify rights to submit messages. You must also have modify or view rights to access that specific content incident folder.

To submit messages from quarantine folders for customer-specific rules

1. In the Control Center, click **Content**.

2. Under **Incident Management**, select the content quarantine incident folder that contains the message that you want to submit for a custom rule.
3  Do one of the following tasks:

To submit one or more messages from the Quarantine Incidents page:

- In the Incident ID column, check the box beside the message or messages that you want to submit, and click This is Spam or This is NOT Spam.

To view the details of the incident first, then submit the message:

- In the Incident ID column, double-click on the incident number to view its details, and on the Content Incident Management page, click This is Spam or This is NOT Spam.

4  In the confirmation dialog box, click This is Spam or This is NOT Spam, as appropriate.

If submission is successful, the submission type appears in the Submission Status column for the message that you selected.

See “About submitting messages for customer-specific spam rules” on page 265.
See “Monitoring and acting on incidents” on page 427.

Remediating quarantined incidents

After you review an incident in a quarantine incidents folder, you can remediate it (approve it, reject it, or apply a custom action). Or you can continue to hold it.

When you remediate incidents in quarantine incident folders, Symantec Messaging Gateway takes the action that you specified in the content filtering policy for the following:

- Message Review Approved Actions
- Message Review Rejected Actions
- Message Review Custom Actions

See “Adding actions to a content filtering policy” on page 332.

For example, assume that you create a content filtering policy whose actions is to create an incident in the Quarantine Incidents folder. The Message Review Approved Actions is deliver the message. The Message Review Rejected Actions is to delete the message. The Message Review Custom Actions is to archive the message. Assume that this policy is violated, and an incident is created in the Quarantine Incidents folder. If you approve the incident, the message is delivered. If you reject the incident, the message is deleted. If you select the custom action, the message is archived.

If you integrate with the Enforce Server, you can remediate incidents through either the Symantec Messaging Gateway Control Center or the Enforce Server administration console. When you remediate through the Enforce Server administration console, the status is immediately updated on both Symantec Messaging Gateway and the Enforce Server. However, the remediation actions that are taken through notification message links or through the Control
Center are only updated on the Enforce Server administration console when Symantec Messaging Gateway updates its data with the Enforce Server.

See “Configuring Symantec Messaging Gateway to update data with Enforce Server” on page 453.

See “Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway” on page 471.

You can remediate one or more messages from the Incident Management page. You can remediate or continue to hold one incident at a time from an incident’s detail page.

See “About monitoring and acting on incidents” on page 429.

To remediate incidents, you must have Full Administration rights or rights to modify the specific content incident folder.

To remediate quarantined incidents from the Incident Management page

1 In the Control Center, click Content.

2 Under Incident Management, select the quarantine incident folder that contains the incident that you want to review and remediate.

3 Check the box beside one or more incidents that you want to remediate.

4 Click Approve, Reject, or Custom.

To remediate quarantined incidents from the Incident Management details page

1 In the Control Center, click Content.

2 Under Incident Management, select the quarantine incident folder that contains the incident that you want to remediate or continue to hold.

3 In the Incident ID column, click on the incident number that you want to review, remediate, or continue to hold.

4 On the Incident Management details page, in the right pane, click the Message review action drop-down list and select the action that you want to take.

5 Optionally, in the Comment box, type a comment about the action.

6 Click Update.

Updating an incident’s status

You can update an incident’s status to reflect changes to the incident. The incident’s status lets reviewers know what stage of the review process the incident is currently in and what the results of the review are.

The status options are as follows:
The incident occurred, but the status has not yet been updated.
This setting is the default status that is assigned to the incident when it is initially created.

Active
The incident is under review.

Confirmed
The incident is valid.

False positive
The incident is not valid.

You can only change the status of a single incident at a time.

See “About monitoring and acting on incidents” on page 429.

To update an incident's status, you must have Full Administration rights or rights to view the specific content incident folder.

To update an incident's status

1 In the Control Center, click Content.
2 Under Incident Management, select the quarantine incident folder that contains the incident that you want to review, remediate, or continue to hold.
3 In the Incident ID column, click on the incident number that you want to review, remediate, or continue to hold.
4 On the Incident Management details page, in the right pane, click the Update status to drop-down list and select the new status.
5 Optionally, in the Comment box, type a comment.
6 Click Update.

Changing an incident's severity level

As you review an incident, you can modify its severity level.

The severity levels are as follows:

- Unknown
  This setting is the default severity when an incident is created.
- High
- Medium
- Low

You can only change the severity of a single incident at a time.

See “About monitoring and acting on incidents” on page 429.
To update an incident's severity, you must have Full Administration rights or rights to view the specific content incident folder.

To update an incident's severity

1. In the Control Center, click **Content**.
2. Under **Incident Management**, select the folder that contains the incident whose severity you want to change.
3. In the **Incident ID** column, click on the incident number whose severity you want to change.
4. On the **Incident Management** details page, in the right pane, click the **Update severity** drop-down list and select the new status.
5. Optionally, in the **Comment** box, type a comment.
6. Click **Update**.

Viewing an incident's history

You can view the history of an incident to see how the incident has progressed.

You can only view the history of a single incident at a time.

See “About monitoring and acting on incidents” on page 429.

To view an incident's history, you must have Full Administration rights or rights to view the specific content incident folder.

See “Exporting an incident's history” on page 440.

To view an incident's history

1. In the Control Center, click **Content**.
2. Under **Incident Management**, select the folder that contains the incident history that you want to review.
3. In the **Incident ID** column, click on the incident number whose history you want to review.
   The incident history appears on the **Incident Management** details page under **Incident History**.

Viewing the text that violated a content filtering policy

Symantec Messaging Gateway can identify the text that violated a content filtering policy. It also specifies in which message part the text is contained (for example, the subject line or message body). You can see this information when you view the details of a specific incident. You can use this information to help you fine-tune and troubleshoot your content filtering policies.
The only content filtering conditions that let you view the text that violated a policy are as follows:

- Contains
- Matches regular expression
- Matches pattern
- Starts with
- Ends with
- Matches exactly

For each message, Symantec Messaging Gateway can display a maximum of 50 matching strings per policy group. Each matching string displays only the first 100 bytes of the text.

**Note:** This feature is not available for any incidents that existed before you upgraded to Symantec Messaging Gateway 9.5.

To view the contents of incident folders, you must have Full Administration rights or rights to access each content incident folder separately.

**To view the text that violated a content filtering policy**

1. In the Control Center, click **Content**.
2. In the **Incident Management** task pane, select the content incident folder that contains the incident that you want to view.
3. In the **Incident ID** column, click on the incident ID number for the incident in which you want to view the details.
4. Under **Incident Details**, click the hyperlink beside **Message scan results: <policy name>** to view the content that violated the policy. The hyperlink is the name of the policy.

   The text that violated the policy and the message part that contains the text appears in the **<policy name> Policy Match Text** window.

   For example, a policy named 'XYZ' is a content filtering policy. When an email message violates this policy, under **Incident Details**, click 'XYZ' in **Message scan results: XYZ** which is hyperlinked. You can view the content that violated policy 'XYZ'. The text that violated the policy and the message part that contains the text, appears in the **XYZ Policy Match Text** window.

5. Click **Close** to close the **<policy name> Policy Match Text** window.

   The **<policy name>** that appears in this window is the name of the policy which caused the message to go to the incident folder.

See “**How the matching text feature is affected by upgrade for existing content**” on page 449.
How the matching text feature is affected by upgrade for existing content

When you upgrade from Symantec Brightmail Gateway version 9.0.x or earlier, your previous settings and the behavior for the settings are retained. However, the matching text feature is unavailable for any messages that existed in the Message audit log before your upgrade to Symantec Messaging Gateway 9.5 or later. It is also unavailable for any incidents in your content incident folders before your upgrade.

When you choose to view the matching text information for a pre-existing message, the following message appears in the `<policy name>` Policy Match Text window:

Policy Match Text information is not available.

See “Viewing the text that violated a content filtering policy” on page 447.

See “How the Message Audit Log helps to fine-tune and troubleshoot content filtering policies” on page 351.

See “Content filtering condition match criteria” on page 330.

Encrypting data with Symantec Content Encryption

Symantec Messaging Gateway uses Symantec Content Encryption, powered by Symantec Email Security.Cloud, to encrypt outbound messages for greater security.

You must purchase a Symantec Content Encryption license, configure your system for encryption, and provision an encryption account before you can use Symantec Content Encryption. You then create and assign policies that encrypt outbound messages.

You can track encrypted message statistics in the Status dashboard of the Control Center and view message logs in the Message Audit Log reports.

Table 16-5 describes the process for how to set up and configure Symantec Content Encryption to provide encryption for outbound messages.

Table 16-5 Encrypt outbound message data

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Purchase a Symantec Content Encryption license.</td>
<td>You can find licensing information on the following page: Content &gt; Settings &gt; Content Encryption See &quot;Licensing your product&quot; on page 714.</td>
</tr>
</tbody>
</table>
### Encrypt outbound message data (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2: Configure your appliance.</td>
<td>Purchase and install an SSL certificate from a supported Certificate Authority and configure your hosts for content encryption. See “Preparing your system for content encryption” on page 450.</td>
</tr>
<tr>
<td>Step 3: Configure the host and port.</td>
<td>Next you must configure the host information and port information for an encryption account. See “Managing host and port information for content encryption” on page 451.</td>
</tr>
<tr>
<td>Step 4: Provision your encryption account.</td>
<td>To apply content encryption to your messages, you must work with Symantec to provision an encryption account. See “Provisioning a content encryption account” on page 452.</td>
</tr>
<tr>
<td>Step 5: Create a content policy with the action <strong>Deliver message with content encryption.</strong></td>
<td>When you complete setting up and configuring the appliance for content encryption, you can create content filtering policies to use outbound message encryption. See “Creating a content filtering policy” on page 325.</td>
</tr>
</tbody>
</table>

### Preparing your system for content encryption

Once you have obtained a content encryption license, you must provision your account through Symantec and then also configure your system for content encryption. To configure your system for content encryption, you must complete the tasks described in this topic before or after you begin the provisioning process with Symantec. These tasks must be completed before you use your new encryption account.

See “Encrypting data with Symantec Content Encryption” on page 449.

### Preparing your certificates

1. Secure a domain, if necessary, and purchase a certificate for your domain

   You must use a Certificate Authority (CA) that is listed in the provisioning form that is provided by Symantec. If you already have a certificate, but it is not on the list of approved CAs, you will need to replace your certificate with one from a CA in the list.

2. In Symantec Messaging Gateway, click **Administration > Settings > Certificates** and click the **TLS & HTTP Certificates** tab to request and create a new certificate.

   See “Requesting a Certificate Authority signed certificate” on page 176.
3 Import the certificate that is issued by your CA. The certificate’s Subject Common Name must match the fully-qualified domain name of your Symantec Messaging Gateway host. For example, if “update5.brightmailtest.info” is the name of the Symantec Messaging Gateway host that you use to accept mail, then the Subject Common Name “update5.brightmailtest.info” must be used by the certificate and by SMTP clients that connect to that host.

See “Importing a Certificate Authority signed certificate” on page 177.

4 Add the CA certificate or the CA certificate bundle to your system.

See “Adding a CA or an intermediate certificate” on page 175.

Configuring your hosts for content encryption

1 Click Administration > Hosts > Configuration.

2 Select the first host and click Edit then click the SMTP tab.

3 Under Mail Filtering, make sure that you have selected either Inbound mail filtering only or Inbound and outbound mail filtering.

4 Under Inbound Mail Settings, check Accept TLS encryption and select the new certificate.

5 Optionally, you can check Request client certificate.

This option adds information about the client certificate verification transaction into the Received header. This information is potentially useful for building policies.

6 If your host uses only one IP address, click Save to save your changes and then repeat steps 2 through 5 to enable TLS for the next host.

If your host uses more than one IP address, go to step 7.

7 Click Advanced Settings at the bottom of the page to display the SMTP configuration page.

8 On the Delivery tab, under SMTP Delivery Bindings, set Dynamically routed messages to Auto.

9 Click Continue to return to the Edit Host Configuration page.

10 Click Save to save your changes for this host.

Use this procedure to configure all of your hosts for TLS encryption.

Managing host and port information for content encryption

The host information for your provisioned encryption account is determined by your Symantec provisioning representative, who will determine the host and port that is most appropriate for your system.
This section describes how to manage host and port information for an encryption account. To provision an encryption account you must obtain a license, configure your system for encryption, work with your provisioning representative to provision the account and then create policy groups that direct the system to encrypt outbound messages.

See “Encrypting data with Symantec Content Encryption” on page 449.

**Editing host and port information for content encryption**

1. To view your Content Encryption host and port information, click **Content > Settings > Content Encryption**, then click **Show Advanced**.

2. To change the host information, provide the new Email Security.cloud encryption host name in the **Host** field.

3. To change the port information, provide the new port in the **Port** field.

4. Click **Save** to save your new host and port information.

**Provisioning a content encryption account**

To apply content encryption to your messages, you must work with Symantec to provision an encryption account.

This section describes how to provision an existing license. If you have not acquired a Symantec Content Encryption license, you can learn more about the service by clicking **Content > Settings > Content Encryption**. In addition to provisioning your account, you must also configure your system for encryption and create policy groups that direct the system to encrypt outbound messages.

See “Encrypting data with Symantec Content Encryption” on page 449.

To provision your content encryption license

1. Select **Content > Settings > Content Encryption**.

   - If you have not yet purchased a Symantec Content Encryption license, you can learn more about the service via the Content Encryption page. Click **click here**. Once you have purchased a license, go to step 2.

   - If you have not already provisioned your encryption account, the **Content Encryption** page provides a link to facilitate the provisioning process. Go to step 2.

   - If you have already provisioned your encryption account, the **Content Encryption** page displays your licensing information and provides your host and port setting defaults. If you want to edit your connection information at this time, click **Show Advanced**.
See “Managing host and port information for content encryption” on page 451.

2 In the Content Encryption page, click **click here**.

A page provides a downloadable provisioning form along with instructions for provisioning your content encryption account.

3 Complete the Content Encryption Provisioning form as directed. For encryption to be fully effective, you must include information for all domains and Scanners in the provisioning form.

If you add a new domain or Scanner at a later date, you must inform your Symantec provisioning representative. For more information, see the Symantec Content Encryption Provisioning page by clicking **Content > Settings > Content Encryption** and then clicking the **click here** link.

New hosts must also be configured for encryption.

See “Preparing your system for content encryption” on page 450.

4 When you are finished, email the provisioning form to the provided email address.

Once you have mailed your completed form, a Symantec employee on the Email Security.cloud team will contact you to facilitate the provisioning of your account and will notify you when your account is active.

See “Managing host and port information for content encryption” on page 451.

## Configuring Symantec Messaging Gateway to update data with Enforce Server

Symantec Messaging Gateway can update information about content filtering incidents and their statuses with the Enforce Server. Synchronization lets administrators view the current details about Symantec Messaging Gateway incidents from the Enforce Server administration console.

See “About integrating Symantec Data Loss Prevention with Symantec Messaging Gateway” on page 470.

You must provide Symantec Messaging Gateway with proper Enforce Server credentials and specify the number of incidents and frequency of the incident data updates. The credentials that you specify must already exist on the Enforce Server.

For more information, see the chapters about how to manage users and roles and about stored credentials in the *Symantec Data Loss Prevention Administration Guide*.

You must have Full Administration rights or rights to modify Manage Settings to configure these options.
To configure Symantec Messaging Gateway to update data with Enforce Server

1. In the Control Center, click **Content > Settings > DLP Connect**.
2. Click the **Enforce Server Access** tab.
3. Check **Enable connection with Enforce Server**.
4. In the **Registered Enforce Server administration console host or IP address** field, specify the host name or IP address of the server upon which your Enforce Server resides.
5. In the **User name** field, type the user name.
6. In the **Password** field, type the password.
7. In the **Maximum number of incidents for status update** field, specify the number of incidents that can be sent in each update.
   The default value is 5000.
8. In **Synchronize with Enforce Server every (minutes)**, specify how often the Enforce Server and Symantec Messaging Gateway should synchronize incident data.
   The minimum amount of time you can select and the default value is every 5 minutes.
9. Click **Save**.

See “Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway” on page 471.
Threat defense scanning with Symantec Content Analysis

This chapter includes the following topics:

- About threat defense scanning
- Preparing Symantec Content Analysis for connection to Symantec Messaging Gateway
- Connecting Symantec Messaging Gateway to a Content Analysis appliance
- Configuring threat defense scan settings
- Default and sample threat defense policies
- Creating new threat defense policy sets
- Selecting threat defense policies for a policy group
- Viewing the Content Analysis queue

About threat defense scanning

With Symantec Messaging Gateway version 10.6.3 and later, you can connect to Symantec Content Analysis version 2.1 or later to provide threat defense scanning. Content Analysis offers deep content inspection to deliver next-generation malware detection, and On-box Sandboxing to provide true on-premises analyses. Through threat defense integration, you can add these capabilities to your existing Symantec Messaging Gateway protections.

Threat defense scans the HTML body of a message and the message attachments. If an attachment is a plain text file, an XML file, or an empty file, the threat defense scan ignores
the file. The text body of a message is also ignored. If an attachment is an email message, threat defense scans the attached message in the same way that it scans any other message.

The following tables summarize what you need to do on Symantec Content Analysis and Symantec Messaging Gateway to set up threat defense scanning.

See “Connecting Symantec Messaging Gateway to a Content Analysis appliance” on page 457.

Table 17-1 Setup steps for Symantec Messaging Gateway

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Generate an API key, enable HTTPS Administration, and configure a port on each Symantec Content Analysis appliance. See “Preparing Symantec Content Analysis for connection to Symantec Messaging Gateway” on page 456.</td>
</tr>
<tr>
<td>2</td>
<td>Use the API key and port information when you configure the Content Analysis connection settings on the <strong>Threat Defense &gt; Settings &gt; CA Connect</strong> page. See “Connecting Symantec Messaging Gateway to a Content Analysis appliance” on page 457.</td>
</tr>
<tr>
<td>3</td>
<td>Configure Scan Settings on the <strong>Threat Defense &gt; Settings &gt; Scan Settings</strong> page. See “Configuring threat defense scan settings” on page 458.</td>
</tr>
<tr>
<td>4</td>
<td>Make any necessary changes to threat defense policies on the <strong>Threat Defense &gt; Policies &gt; Email</strong> page. See “Default and sample threat defense policies” on page 460.</td>
</tr>
<tr>
<td>5</td>
<td>Enable Content Analysis for each policy group, and choose the policies that apply to the group on the <strong>Administration &gt; Users &gt; Policy Groups &gt; Edit Policy Group &gt; Threat Defense</strong> tab. See “Selecting threat defense policies for a policy group” on page 467.</td>
</tr>
</tbody>
</table>

Preparing Symantec Content Analysis for connection to Symantec Messaging Gateway

Before you can connect Symantec Messaging Gateway to a Content Analysis appliance, you must perform certain steps on the Content Analysis appliance.
To set up a Symantec Content Analysis appliance for threat defense scanning

1. Generate the API key for the interface between Content Analysis and Symantec Messaging Gateway.

You generate the API key in the command line interface of the Content Analysis appliance. For instructions, refer to the Developer's Guide for Content Analysis File Submission REST API.

2. Enable HTTPS Administration and specify the HTTPS port

In the Content Analysis Control Center, select Settings > Web Management. In the Web Server panel, select Enable HTTPS Administration and enter a Port number.

3. Make sure the Content Analysis appliance has a valid certificate.

The Content Analysis web interface requires a certificate. Each Content Analysis appliance installs with a default certificate. The default certificate or a valid replacement certificate must be installed on the Content Analysis appliance.

4. Enable On-box Sandboxing on the Content Analysis appliance, if you licensed this option.

For instructions, refer to the Symantec Content Analysis 2.1 WebGuide.

Connecting Symantec Messaging Gateway to a Content Analysis appliance

After you generate an API key and configure a port on the Content Analysis appliance, use the following procedure to configure the connection in the Symantec Messaging Gateway Control Center.

To configure Content Analysis connection settings in Symantec Messaging Gateway

1. On the Threat Defense > Settings > CA Connect > Symantec Content Analysis Setup page, enter the host name or IP address, HTTPS port number, and API key for the Content Analysis appliance.

2. Specify a Preference for this appliance. The Preference value directs Symantec Messaging Gateway to access one or more appliances as primary servers, and access others only if the primary servers are unavailable or busy.

   - Lower numbers are higher preference. For example, Symantec Messaging Gateway tries to connect to a Content Analysis appliance with a preference of 1 before it attempts to connect to an appliance with a preference of 2.

   - If two Content Analysis appliances have the same preference number, Symantec Messaging Gateway attempts to use each appliance equally. A Content Analysis appliance with a higher preference number is used only if both hosts with the lower preference number are unavailable.
Configuring threat defense scan settings

Threat defense scan settings help you manage the queue of messages that are sent to Content Analysis for scanning.

Other factors affect the Content Analysis queue, such as:

- The amount of incoming traffic
- The amount of outgoing traffic, if your policies include threat defense scanning of outgoing messages
- The capacity and availability of the connected Content Analysis appliances
- Network performance

After you connect a Content Analysis appliance to SMG, you may want to evaluate the results at the default settings and then adjust as needed.

To edit threat defense scan settings

1. In the Control Center, select **Threat Defense > Settings > Scan Settings > Threat Defense Scan Settings**.

2. On the **General** tab > **Result cache TTL**, enter a value from 7 to 90 minutes to specify how many minutes a result or verdict from Content Analysis is cached.

   - The result cache stores the verdicts that Content Analysis sends for each file hash it analyzes. The hash values of the files in incoming emails are compared to the cached results. If there is a match, SMG uses the cached result and does not send the file to Content Analysis for scanning. Any files that do not match cached results are sent to Content Analysis for scanning.

   - After the TTL (time to live) limit expires, the cached result is deleted. The next file with a matching hash is sent to Content Analysis for an updated result, and the TTL timer resets.

   - A short **Result cache TTL** increases the load on the Content Analysis appliances, but gives your organization faster updates if a threat verdict changes. For example, a threat verdict may change when Content Analysis receives results from sandbox analyses. However, a short TTL may cause SMG to send many copies of a non-malicious file to Content Analysis for scanning. The repeated scans increase the queue size and the load on Content Analysis appliances with no added security benefits.

   - A long **Result cache TTL** means that possibly malicious files may be delivered while SMG waits to update a cached verdict. However, a long TTL prevents SMG from sending the same non-malicious files to Content Analysis. For example, a file attachment that is sent to a distribution list does not go to Content Analysis for repeated scanning.
The Result cache TTL must be at least 6 minutes longer than the Scan timeout that you specify in step 3.

3 For the Scan timeout, enter a value from 1 to 60 minutes.

The Scan timeout specifies how many minutes SMG waits for the Content Analysis appliance to return a result. If the Scan timeout is exceeded, the message is processed according to the policy for the condition Is unscannable for advanced threats.

- A short Scan timeout may increase the number of Unscannable results.
- A long Scan timeout may increase the size of the CA queue and cause delayed delivery when Inline policies are applied.

See “Selecting threat defense policies for a policy group” on page 467.

4 For the Maximum number of messages in Content Analysis queue, enter a value between 1 and 1,000,000.

The Maximum number of messages in Content Analysis queue value is the upper limit of messages that can wait in the queue for Content Analysis scanning. If SMG already started to process a message, this limit does not block the message from entering the CA queue.

5 Enable or disable Bypass scanning when Content Analysis queue is full to specify what SMG does if the queue exceeds the limit.

- When Bypass scanning when Content Analysis queue is full is enabled, SMG does not send files and attachments to Content Analysis for scanning. SMG still scans messages with the other enabled filters. The messages are then processed according to the policies for the other filters.

- When Bypass scanning when Content Analysis queue is full is disabled, SMG defers inbound mail.

When Content Analysis processes more messages and the queue size falls below the maximum, normal operations resume.

6 If you do not want to send certain file types to Content Analysis for scanning, click the Exclude Scanning tab and add the file types to the list.

Although the Exclude Scanning lists are entirely separate for Content Analysis and malware scanning, you maintain the lists in a similar way. You can exclude files by type or class. You cannot exclude files from Content Analysis scanning by file name or file extension.

7 Click Save.
Excluding file types from threat defense scanning

Symantec Messaging Gateway lets you create lists of the file types that you do not want to send to Content Analysis for threat defense scanning. You can create a single list or you can create multiple lists to help you categorize the file types.

To help you create your lists, Symantec Messaging Gateway provides file classes that group similar file types. You can choose every file type in a file class, or you can select individual file types to exclude from threat defense scanning. You can also select All File Classes to create a list of every file class that SMG provides.

To exclude file types from threat defense scanning

1. In the Control Center, click Threat Defense > Settings > Scan Settings.
2. On the Exclude Scanning tab, click Add.
3. In the Exclude scanning list name box, type a name for the list.
4. In the File classes list, select the file class that you want to exclude from scanning.
   - To select multiple classes, hold down the Ctrl key while you click the names of file classes.
   - To select every file class in the File classes list, click All File Classes.
5. The File Types list displays all the file types that are associated with your selected file classes.
   - To exclude every file type in the File Types list from threat defense scanning, click Add File Classes.
   - To remove file types from the exclusion list, hold down the Ctrl key while you deselect the file types. Then click Add File Classes to add the remaining, selected file types.
6. Click Save.

The names of the file types appear in the Description list.

When you create a new list, it is enabled by default. An exclude scanning list must be enabled if you want SMG to use the list during scans. When a message contains an attachment that matches an excluded file type, SMG does not send the file to Content Analysis for scanning. You can edit, delete, disable, enable, or export an exclude scanning list on the Threat Defense > Scan Settings > Exclude Scanning tab.

Default and sample threat defense policies

The Threat Defense > Policies > Email > Email Threat Defense Policies page displays the sample policies that Symantec Messaging Gateway provides for threat defense scanning by Symantec Content Analysis. These threat defense policies are grouped into sets to achieve specific results under all scanning conditions and threat defense verdicts. The policy names
begin with **Inline**, **Monitor**, and **Secure Preview** to indicate which policies you should assign as a set to individual policy groups.

- **Inline** policies ensure that all messages are scanned before they are delivered.
- **Monitor** policies ensure that messages are delivered promptly. Malware may be discovered after messages are delivered.
- **Secure Preview** policies deliver copies of each message, stripped of attachments. The original messages and attachments are delivered after Content Analysis scanning determines that the attachments are not malicious.

Inline policies are assigned to all policy groups by default. However, you must enable the Inline policies, or apply different sets of threat defense policies to your groups, from the Administration > Policy Groups page.

**Default threat defense policies for Inline mode**

The default Inline policy set supports a workflow where security is the most important consideration. Recipients may experience a short delay before messages are delivered.

When you enable the default Inline policies for a group, no message should be delivered before it is scanned. However, Inline policies contain a notification action to ensure that recipients are aware of an unexpected condition or error that triggers an early release. Early release means that recipients receive a copy of a message before Content Analysis scans the message. For example, if a recipient moves from a group with Monitor policies to a group with Inline policies, SMG may deliver an infected message before the Inline policy takes effect.

Table 17-2 describes the settings for each Inline policy.

**Table 17-2** Inline threat defense policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on messages that trigger this policy before an early release</th>
<th>Actions to take on messages that trigger this policy after an early release</th>
</tr>
</thead>
</table>
| Inline - Advanced threat: Delete message (default) | Content Analysis detected a threat in the message | Delete the message | Send the notification "Threat Defense - Advanced Threat delivered"  
Delete the copy of the message that was sent for Content Analysis scanning |
Table 17-2 Inline threat defense policies (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on messages that trigger this policy before an early release</th>
<th>Actions to take on messages that trigger this policy after an early release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline - Unscannable: Modify subject line with &quot;[Message not scanned by Threat Defense]&quot; (default)</td>
<td>Content Analysis cannot scan the message</td>
<td>Prepend the subject line with &quot;[Message not scanned by Threat Defense]&quot; and send the message</td>
<td>Send the notification &quot;Threat Defense - Message Unscannable&quot; Delete the copy of the message that was sent for Content Analysis scanning</td>
</tr>
<tr>
<td>Inline - Not malicious: Deliver normally (default)</td>
<td>Content Analysis did not detect a threat in the message</td>
<td>Deliver the message normally</td>
<td>Delete the copy of the message that was sent for Content Analysis scanning</td>
</tr>
</tbody>
</table>

The Inline policies are labeled (default). These default policies are assigned to all policy groups automatically, but you must explicitly enable these policies for each group. You cannot delete a default policy.

Sample threat defense policies for Monitor mode

The Monitor policy set supports a workflow where any delay in email delivery is unacceptable. Monitor mode is also useful to evaluate the effect of enabling Content Analysis scanning for test groups before you deploy to your full organization.

When you assign all the sample Monitor policies to a group:

- Messages are delivered to recipients immediately.
- If the results cache does not contain a verdict for an attachment or a file in a message, Symantec Messaging Gateway sends a copy to Content Analysis for scanning.
- If Content Analysis returns an advanced threat or unscannable verdict, SMG sends a notification to the recipient.
- If Content Analysis returns a result of no threat detected, no further action is taken because the message was already delivered.
- If the results cache contains verdicts for all the attachments and files in a message, there is no need to send copies to Content Analysis for scanning. Symantec Messaging Gateway executes the **Actions to take on messages that trigger this policy before an early release** immediately.

The following tables describe the settings for each Monitor policy.
### Table 17-3  Monitor mode early release policy

<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on the released copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor – Early release: Deliver immediately with no delay</td>
<td>If Content Analysis inspection time exceeds 0 seconds</td>
<td>Deliver the message normally. An additional implied action is to send a copy to Content Analysis for scanning</td>
</tr>
</tbody>
</table>

### Table 17-4  Monitor mode policies by threat defense scanning result

<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on messages that trigger this policy before an early release</th>
<th>Actions to take on messages that trigger this policy after an early release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor - Advanced threat: Send notification &quot;Threat Defense - Advanced Threat delivered&quot;</td>
<td>Content Analysis detected a threat in the scanned copy of the message.</td>
<td>Delete message</td>
<td>Send the notification &quot;Threat Defense - Advanced Threat delivered&quot; Delete the copy of the message that was sent for Content Analysis scanning</td>
</tr>
<tr>
<td>Monitor - Unscannable: Send notification &quot;Threat Defense - Message unscannable&quot;</td>
<td>Content Analysis cannot scan a copy of the message.</td>
<td>Prepend subject line with &quot;[Message not scanned by Threat Defense] &quot; and send message</td>
<td>Send the notification &quot;Threat Defense - Message unscannable&quot; Delete the copy of the message that was sent for Content Analysis scanning</td>
</tr>
<tr>
<td>Monitor - Not malicious: Take no action, message already delivered</td>
<td>Content Analysis did not detect a threat in the scanned copy of the message.</td>
<td>Deliver the message normally</td>
<td>Delete the copy of the message that was sent for Content Analysis scanning</td>
</tr>
</tbody>
</table>

### Sample threat defense policies for Secure Preview

The Secure Preview policy set supports a workflow where recipients can tolerate a short delay while their mail is scanned for threats. However, recipients need a secure way to receive details of their messages immediately.

When you assign all the sample Secure Preview policies to a group:
Attachments are stripped from copies of each message and Symantec Messaging Gateway adds the annotation "Threat Defense - Secure Preview" to each subject line. These copies are then delivered to recipients immediately.

Symantec Messaging Gateway sends the full message, with attachments, to Content Analysis for scanning.

If Content Analysis returns an advanced threat or unscannable verdict, Symantec Messaging Gateway sends a notification to the recipient.

If Content Analysis scanned the message and did not detect malware, the original message is delivered to the recipients.

If the results cache contains verdicts for all the attachments and files in a message, there is no need to send copies to Content Analysis for scanning. Symantec Messaging Gateway executes the **Actions to take on messages that trigger this policy before an early release** immediately.

Table 17-6 describes the settings for Monitor policies.

**Table 17-5**  Secure Preview threat defense policy that triggers immediate delivery

<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on the released copy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Preview – Early release: Strip all attachments and deliver immediately with no delay</td>
<td>If Content Analysis inspection time exceeds 0 seconds</td>
<td>Strip all attachments from the message. Add the annotation &quot;Threat Defense - Secure Preview&quot; and deliver the modified message.  An additional implied action is to send a copy of the full message, with attachments, to Content Analysis for scanning.</td>
</tr>
</tbody>
</table>

**Table 17-6**  Secure Preview threat defense policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on messages that trigger this policy before an early release</th>
<th>Actions to take on messages that trigger this policy after an early release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Preview - Advanced threat: Delete message</td>
<td>Content Analysis scanning determined that the message contained advanced threats</td>
<td>Delete the original message</td>
<td>Delete the original message</td>
</tr>
</tbody>
</table>

Table 17-6 describes the settings for Monitor policies.
<table>
<thead>
<tr>
<th>Policy name</th>
<th>If the following condition is met</th>
<th>Actions to take on messages that trigger this policy before an early release</th>
<th>Actions to take on messages that trigger this policy after an early release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Preview - Unscannable: Modify subject line with &quot;[Message not scanned by Threat Defense]&quot; and redeliver message with attachments</td>
<td>Content Analysis could not scan one or more attachments</td>
<td>Prepend the subject line with &quot;[Message not scanned by Threat Defense] &quot; and deliver the original message, with attachments</td>
<td>Prepend the subject line with &quot;[Message not scanned by Threat Defense] &quot; and deliver the original message, with attachments</td>
</tr>
<tr>
<td>Secure Preview - Not malicious: Modify subject line with &quot;[Threat Defense scanning complete, no threats found]&quot; and redeliver message with attachments</td>
<td>Content Analysis scanning determined that the message did not contain malicious content</td>
<td>Prepend the subject line with &quot;[Threat Defense scanning complete, no threats found] &quot; and deliver the original message, with attachments</td>
<td>Prepend the subject line with &quot;[Threat Defense scanning complete, no threats found] &quot; and deliver the original message, with attachments</td>
</tr>
</tbody>
</table>

Creating new threat defense policy sets

The sample threat defense policies have names that indicate to which set a policy belongs. When you add new threat defense policies, you should create sets to ensure that SMG takes appropriate actions under all of the following conditions:

- **Early Release**
  An Early Release policy has the condition **If Content Analysis inspection time exceeds X seconds**. If you enter 0, SMG delivers the message immediately. When you create an Early Release policy, all other policies in the policy set must coordinate with the Early Release policy. For example, if an Early Release policy sends the full message, the corresponding Advanced Threats Detected policy must specify the actions to take when malware is delivered.

- **Advanced Threats Detected**
  An Advanced Threats Detected policy determines how SMG processes messages for the condition **If a message contains advanced threats**.

- **Unscannable**
  An Unscannable policy determines how SMG processes messages for the condition **If a message is unscannable for advanced threats**. While the vast majority of unscannable files are not malicious, some may be.

- **Not Malicious**
A Not Malicious policy determines how SMG processes messages for the condition **if a message does not contain advanced threats**.

**Best practices for creating threat defense policies**

The threat defense policies that you assign to a policy group must process messages correctly for every condition and verdict in this list. To avoid unexpected results, Symantec recommends that you create new threat defense policy sets from copies of the sample policy sets and follow these guidelines:

- Choose a unique name to include in the names of all policies in the set, to identify which policies belong to the set. The sample policies, for example, begin with Inline, Monitor, or Secure Preview. This naming convention reduces the chance of errors when you assign the policies to a policy group.

- Copy every policy in the sample policy set, even if you only want to modify one or two of the policies. This practice lets you apply the same naming convention to the entire set.

- Choose a name for each policy that describes the policy’s purpose. Prepend this name with the policy set name. For example, the Monitor policy for an unscannable verdict is named **Monitor - Unscannable: Send notification "Threat Defense - Message unscannable"**.

**Creating a new threat defense policy from a copy**

To create a threat defense policy from an existing policy

1. In the Control Center, select **Threat Defense > Policies > Email**.
2. On the **Email Threat Defense Policies** page, click the box next to a sample policy that you want to use as a starting point and click **Copy**.
   
   See “**Default and sample threat defense policies**” on page 460.
3. On the **Add Email Threat Defense Policy** page that appears, type a name for the policy. Follow the guidelines to include the policy set name and the policy purpose.
4. Change the policy conditions and actions as needed. For example, you can:
   - Choose a notification action and then choose a notification from the list. The notification is sent as a separate email. The original message is processed according to the policy.
     You can add a notification to the list or edit an existing notification on the **Content > Resources > Notifications** page.
     See “**About policy violation notifications**” on page 377.
   - Choose an annotation action and then choose an annotation to append to an email message.
     You can add or edit an annotation on the **Content > Resources > Annotations** page.
     See “**Creating and managing annotations for policy violations**” on page 399.
   - Choose a Disarm action.
You can view and change Disarm settings on the Malware > Settings > Email Scan Settings > Disarm tab. The same Disarm settings apply to malware scanning and threat defense scanning. See “About Disarm” on page 207.

5 Do not change anything in the Apply to the following policy groups panel. Symantec recommends that you assign threat defense policies from the Administration > Users > Policy Groups page after you create all your new policies. This practice ensures that you apply a consistent set of policies to a policy group. See “Selecting threat defense policies for a policy group” on page 467.

6 Click Save.

7 Repeat steps 2 through 6 to create the next policy in the set. Continue to create policies until the set is complete.

## Selecting threat defense policies for a policy group

Threat defense policies specify how to process the email that is sent to Symantec Content Analysis for scanning. Symantec Messaging Gateway includes sets of sample policies that support Inline, Monitor, and Secure Preview modes, to ensure that Symantec Messaging Gateway processes messages correctly for every condition and verdict. You must assign sets of threat defense policies to your policy groups to enable threat defense scanning for the group.

---

**Warning:** Do not mix policies from different sets or you may get undesirable results. For example, if you mix the sample Secure Preview - Early Release policy with the default Inline - Not malicious policy, recipients receive the Secure Preview message without attachments. When Content Analysis returns a verdict of not malicious, the Inline - Not malicious policy tells SMG to delete the message. The result is that recipients never receive the original message with attachments.

---

To select threat defense policies for a policy group

1 In the Control Center, click Administration > Users > Policy Groups.

2 On the Policy Groups page, click the policy group for which you want to select threat defense policies.

3 On the Edit Policy Group page, click the Threat Defense tab.

4 If you want Content Analysis to scan inbound mail, click Enable inbound Content Analysis for this policy group, and then select policies for the group. You can click View to see the characteristics of the selected policy.
- **Inbound advanced threat policy** defines what SMG should do with messages that contain advanced malware.

- **Inbound unscannable policy** defines what SMG should do with messages that Content Analysis could not scan. (There may be encrypted attachments, for example.)

- **Inbound not malicious policy** defines what SMG should do with messages that do not contain advanced threats.

- **Inbound early release policy** defines what SMG should do when it delivers messages before Content Analysis returns a verdict.

5 If you want Content Analysis to scan outbound mail, click **Enable outbound Content Analysis for this policy group**, and then select policies for the group.

By default, only Inline policies are enabled for outbound mail. If you want to assign Monitor or Secure Preview policies to a group, you must edit the policies to enable them for outbound mail.

6 Click **Save**.

See "Default and sample threat defense policies" on page 460.

See "Creating new threat defense policy sets" on page 465.

**Viewing the Content Analysis queue**

The Content Analysis queue for each Scanner contains the messages that currently wait for threat defense scanning.

To view the Content Analysis queue for a Scanner

1 In the Control Center, select **Threat Defense > SMTP > CA Queue**.

2 On the **Content Analysis Queue** page, from the **Host** menu, select the Scanner.

3 From the **Direction** menu, select whether you want to view **Inbound** or **Outbound** messages.

4 Optionally, in the **To** field, type the email address of a recipient. You can enter multiple email addresses, separated by semicolons.

5 Optionally, in the **From** field, type the email address of a sender.

6 Click **Display Filtered** to view the search results. You can click the **Date** heading to sort the results by the date each message first entered the queue.

To start a new search, click **Clear Filters**.
This chapter includes the following topics:

- About integrating Symantec Data Loss Prevention with Symantec Messaging Gateway
- Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway
- About Data Loss Prevention Network Prevent
- Required ports for Data Loss Prevention Network Prevent integration
- How Symantec Messaging Gateway and Data Loss Prevention Network Prevent interact
- Common Data Loss Prevention Network Prevent actions
- Supported Data Loss Prevention Network Prevent delivery modes
- About failure behavior with Data Loss Prevention Network Prevent
- How to resolve a delivery queue back up to Symantec Network Prevent
- Enabling or disabling bypass for Data Loss Prevention Network Prevent
- How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled
- About Data Loss Prevention Network Prevent reports
- About performance implications for Data Loss Prevention Network Prevent integration
- About Data Loss Prevention Network Prevent preference order
- Troubleshooting Data Loss Prevention Network Prevent integration: messages bounce
About integrating Symantec Data Loss Prevention with Symantec Messaging Gateway

Symantec Messaging Gateway integrates with the following Symantec Data Loss Prevention components:

**Data Loss Prevention Network Prevent for Email**
Outbound traffic can be routed from Symantec Messaging Gateway through a Data Loss Prevention Network Prevent server. Network Prevent modifies messages, routes, or block them based on the policies that you configure. Messages that violate content filtering policies are held in Symantec Messaging Gateway incident folders for review and remediation.

See "About Data Loss Prevention Network Prevent" on page 474.

See "Configuring email connections to and from Data Loss Prevention Network Prevent" on page 486.

**Enforce Server**
Enforce Server provides a centralized Web-based management console and incident repository.

This integration lets you remediate quarantined messages from either Symantec Messaging Gateway Control Center or from the Enforce Server administration console. If remediation occurs from Enforce Server, it writes the status to Symantec Messaging Gateway so the incident status stays synchronized. You can also synchronize status updates from Symantec Messaging Gateway to Enforce Server.

See "Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway" on page 471.

See "Configuring Symantec Messaging Gateway to update data with Enforce Server" on page 453.

For additional information, see the Symantec Data Loss Prevention SMG Release from Quarantine FlexResponse Plug-In Implementation Guide, which is available with the Data Loss Prevention Server FlexResponse plug-ins.
Integrating Symantec Data Loss Prevention Enforce Server and Symantec Messaging Gateway

Before you integrate Symantec Messaging Gateway with Symantec Data Loss Prevention Enforce Server, ensure that both products are licensed.

See “About integrating Symantec Data Loss Prevention with Symantec Messaging Gateway” on page 470.

Table 18-1 describes the steps that you must take to integrate Symantec Messaging Gateway with Symantec Data Loss Prevention Enforce Server. It also describes in which product or product component you must perform the configuration.

Table 18-1  Steps to integrate Symantec Messaging Gateway with Enforce Server

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Product or component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Ensure that Data Loss Prevention Network Prevent is configured appropriately for message routing.</td>
<td>Symantec Messaging Gateway</td>
<td>Route outbound email to Data Loss Prevention Network Prevent and configure Data Loss Prevention Network Prevent to route email back to Symantec Messaging Gateway. If you have multiple outbound Scanners, you can route outbound mail to Data Loss Prevention Network Prevent servers differently for each Scanner. Alternatively, you can apply the same settings to all outbound Scanners.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Install and configure the Email Quarantine Connect plug-in and configure the plug-in properties.</td>
<td>Enforce Server</td>
<td>See the section on how to install the plug-in in the Symantec Data Loss Prevention SMG Release from Email Quarantine Connect Plug-In Implementation Guide.</td>
</tr>
</tbody>
</table>
### Table 18-1  Steps to integrate Symantec Messaging Gateway with Enforce Server (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Product or component</th>
<th>Description</th>
</tr>
</thead>
</table>
|      |                                                  | Symantec Messaging Gateway     | Export the same certificate that you use for the Control Center HTTPS interface. This certificate lets the Enforce Server authenticate to Symantec Messaging Gateway.  
See "Exporting a TLS and HTTPS certificate" on page 184.  
See “Requesting a Certificate Authority signed certificate” on page 176.  
See "Assigning a user interface HTTPS certificate to the Control Center" on page 186. |
| Step 3| Export the Control Center HTTPS certificate.     | Enforce Server                 | Import the Symantec Messaging Gateway certificate into the Enforce Server truststore.  
See the section on importing certificates in the Symantec Data Loss Prevention Installation Guide for Windows or the Symantec Data Loss Prevention Installation Guide for Linux. |
| Step 4| Import the Symantec Messaging Gateway certificate.| Enforce Server                 | Create a client certificate and truststore with a server certificate from Symantec Messaging Gateway from the Enforce Server command line.  
See the section on how to install the plug-in in the Symantec Data Loss Prevention SMG Release from Quarantine FlexResponse Plug-In Implementation Guide. |
| Step 5| Create a client certificate.                     | Enforce Server                 | See the section on creating credentials in the Symantec Data Loss Prevention Installation Guide for Windows or the Symantec Data Loss Prevention Installation Guide for Linux. |
| Step 6| Create a user and role.                          | Enforce Server                 |                                                                                                                                                                                                            |
Table 18-1  Steps to integrate Symantec Messaging Gateway with Enforce Server (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Product or component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 7 | Import the Enforce Server certificate. | Symantec Messaging Gateway | Import the Enforce Server certificate into Symantec Messaging Gateway Control Center.  
See “Importing an application certificate” on page 180. |
| Step 8 | Configure the Enforce Server connection details. | Symantec Messaging Gateway | Specify the Enforce Sever credentials and configure the synchronization settings.  
Ensure that the account that you use to access the Enforce Server has the appropriate roles to remediate incidents.  
See the section on managing roles and users in the Symantec Data Loss Prevention Administration Guide for Windows or the Symantec Data Loss Prevention Administration Guide for Linux.  
See “Configuring Symantec Messaging Gateway to update data with Enforce Server” on page 453. |
| Step 9 | Configure policies and their detection rules. | Enforce Server | Configure response policies and rules to insert headers into the messages that violate policies.  
See the sections on implementing policy detection and policy responses in the Symantec Data Loss Prevention Administration Guide for Windows or the Symantec Data Loss Prevention Administration Guide for Linux. |
| Step 10 | Create incident folders to capture the messages that violate content filtering policies and hold for remediation or review. | Symantec Messaging Gateway | Select the folder type Hold for Review (Content Quarantine) to hold incidents for remediation. Or you can choose Informational Incidents to hold incidents for review.  
See “Creating content incident folders” on page 422. |
Table 18-1  Steps to integrate Symantec Messaging Gateway with Enforce Server (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Product or component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 11</td>
<td>Create content filtering policies to detect the header that Data Loss Prevention response rules add.</td>
<td>Symantec Messaging Gateway</td>
<td>Create the policies that scan for the header that Data Loss Prevention (Network Prevent for Enforce) inserts into email messages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Symantec Messaging Gateway filters messages for these headers. Based on the policy actions that you specify, it creates incidents in quarantine incident folders or informational incident folders.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specify the policy action <strong>Create a quarantine incident</strong> to hold these incidents for remediation. Or you can specify the policy action to <strong>Create an informational incident</strong> to hold these incidents for review.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>See “Creating a content filtering policy” on page 325.</td>
</tr>
</tbody>
</table>

### About Data Loss Prevention Network Prevent

Symantec Messaging Gateway integrates with Data Loss Prevention Network Prevent to deliver, route, hold, or block email traffic. Data Loss Prevention Network Prevent is a component of Symantec Data Loss Prevention that discovers, monitors, and protects confidential data wherever it is stored or used. You install Data Loss Prevention Network Prevent on a separate server. You must have at least one Scanner configured for outbound mail filtering to route email to Data Loss Prevention Network Prevent.

**Note:** You cannot route inbound mail through Data Loss Prevention Network Prevent.

You can configure Data Loss Prevention Network Prevent policies to perform the following actions on messages, depending on the type of data that is detected:

- **Block**  Block messages and return a customized bounce message back to senders.
- **Redirect**  Route the messages to different recipients.
- **Tag**  Modify the subject line or add a new header to messages.
Based on message modification by Data Loss Prevention Network Prevent, you can also configure policies on Symantec Messaging Gateway to perform actions such as the following:

- **Archive**: Send the messages to a specific email address for archiving.
- **Create an incident**: Route messages to a content filtering folder and review them before they are delivered. You can optionally configure notification for the messages that are routed to content filtering folders.
- **Encrypt**: Government regulations or your own policies may require that you encrypt sensitive messages.

See “How Symantec Messaging Gateway and Data Loss Prevention Network Prevent interact” on page 476.

### Required ports for Data Loss Prevention Network Prevent integration

**Table 18-2** describes the default ports to use to route email to one or more Data Loss Prevention Network Prevent servers.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Origin</th>
<th>Destination</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Internal mail servers</td>
<td>Scanners</td>
<td>Outbound email</td>
<td>—</td>
</tr>
<tr>
<td>10025</td>
<td>SMTP</td>
<td>Scanner</td>
<td>Data Loss Prevention Network Prevent</td>
<td>Outbound email for processing by Data Loss Prevention Network Prevent</td>
<td>—</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Data Loss Prevention Network Prevent</td>
<td>Scanners</td>
<td>Outbound email that was processed by Data Loss Prevention Network Prevent</td>
<td>By default, Data Loss Prevention Network Prevent returns email to port 10026. You may need to change the Remote SMTP Listener Port setting on Data Loss Prevention Network Prevent to match the port that Symantec Messaging Gateway expects, such as port 25.</td>
</tr>
</tbody>
</table>

See “Configuring email connections to and from Data Loss Prevention Network Prevent” on page 486.
How Symantec Messaging Gateway and Data Loss Prevention Network Prevent interact

If you configure Symantec Messaging Gateway to route email to Data Loss Prevention Network Prevent, email is typically routed in the following order:

- Symantec Messaging Gateway accepts outbound messages at the gateway on port 25, by default.
- Symantec Messaging Gateway passes outbound messages to Data Loss Prevention Network Prevent on port 10025, by default.
- Data Loss Prevention Network Prevent scans messages and blocks, redirects, or tags messages for further action by the MTA.
- See “Common Data Loss Prevention Network Prevent actions” on page 477.
- Data Loss Prevention Network Prevent passes messages back to Symantec Messaging Gateway on port 25 (default) unless Data Loss Prevention Network Prevent rejects the message. In that case, Symantec Messaging Gateway returns the message back to the sender with an SMTP 5xx failure response code. The message includes the text that you specify.
- Symantec Messaging Gateway processes messages as configured. Symantec Messaging Gateway can process messages based on subject or header markup of messages by Data Loss Prevention Network Prevent. Redirected messages are delivered to the alternate recipient or recipients.

The port numbers that are listed are suggested. Actual port numbers may differ at your site.

See “Required ports for Data Loss Prevention Network Prevent integration” on page 475.

If you have multiple outbound Scanners, you can route outbound mail to Data Loss Prevention Network Prevent servers differently for each Scanner, on the Symantec Data Loss Prevention Setup page, or you can apply the settings to all outbound Scanners.

Each Scanner routes email to all Data Loss Prevention Network Prevent servers configured for that Scanner, according to the preference order as follows:

Reflecting mode  
If Data Loss Prevention Network Prevent is configured in reflecting mode, then each Data Loss Prevention Network Prevent server returns each message to the Scanner from which it received the message.

Forwarding mode  
If Data Loss Prevention Network Prevent is configured in forwarding mode, then Data Loss Prevention Network Prevent servers pass messages to the next destination. v19465700

See “About Data Loss Prevention Network Prevent preference order” on page 484.
See “Configuring email connections to and from Data Loss Prevention Network Prevent” on page 486.

Symantec Messaging Gateway integrates with Data Loss Prevention Network Prevent through SMTP Client IP Address-based Routing.

Common Data Loss Prevention Network Prevent actions

Symantec Messaging Gateway and Data Loss Prevention Network Prevent interoperate by exchanging SMTP messages. Through response rules and policies, Data Loss Prevention Network Prevent can modify, reroute, and reject messages. Some actions that you configure Data Loss Prevention Network Prevent to take on email require no further action by Symantec Messaging Gateway. Other actions require you to configure Symantec Messaging Gateway.

Table 18-3 Common Data Loss Prevention Network Prevent actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>Bounces the message back to the sender</td>
</tr>
<tr>
<td>Redirect</td>
<td>Sends the message to different recipients</td>
</tr>
<tr>
<td></td>
<td>You can configure Data Loss Prevention Network Prevent to redirect messages to a new recipient, such as an administrator email address.</td>
</tr>
<tr>
<td>Tagging - Header markup</td>
<td>Adds a custom email header to messages</td>
</tr>
<tr>
<td></td>
<td>You can add a header to an email message, such as X-Sensitive-Data: SSN. You can configure Symantec Messaging Gateway to search for the custom header and act on the message. Symantec Messaging Gateway can delete, archive, create an incident, and hold the message for review.</td>
</tr>
<tr>
<td></td>
<td>You can also run reports on the actions that Symantec Messaging Gateway takes on matching messages.</td>
</tr>
<tr>
<td></td>
<td>See “Creating an incident based on Symantec Network Prevent header markup” on page 488.</td>
</tr>
<tr>
<td>Tagging - Subject modification</td>
<td>Changes the subject line</td>
</tr>
<tr>
<td></td>
<td>Like header markup, you can configure Symantec Messaging Gateway to search for the specific text in the subject line and act on matching messages.</td>
</tr>
</tbody>
</table>
Supported Data Loss Prevention Network Prevent delivery modes

You can integrate Data Loss Prevention Network Prevent into your network architecture. Data Loss Prevention Network Prevent does not make its own on-disk copies of messages. Messages are retained in memory only. The incoming message transaction is not committed until the outbound message transaction succeeds.

You can integrate Data Loss Prevention Network Prevent into your network architecture through the following methods:

Reflecting
After it processes messages, Data Loss Prevention Network Prevent returns the message to the Scanner from which it came.

Forwarding
After it processes messages, Data Loss Prevention Network Prevent passes messages to the MTA that you specify.

The method that you choose depends on the particular requirements at your site.

About failure behavior with Data Loss Prevention Network Prevent

If Data Loss Prevention Network Prevent is unreachable, email may bypass Data Loss Prevention Network Prevent or wait in a mail queue. The behavior depends on how many Data Loss Prevention Network Prevent servers are unreachable and whether bypass is enabled. By default, bypass is enabled.

See “Enabling or disabling bypass for Data Loss Prevention Network Prevent” on page 481.

Data Loss Prevention Network Prevent servers may be unreachable because of the following reasons:

- Failures in the network
- Failures on the hardware on which Data Loss Prevention Network Prevent is running
- The network bandwidth, hardware speed, or number of Data Loss Prevention Network Prevent servers are not adequate for the mail flow
Table 18-4  Failure behavior with Data Loss Prevention Network Prevent

<table>
<thead>
<tr>
<th>Bypass status</th>
<th>Data Loss Prevention Network Prevent server status</th>
<th>System behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass disabled or enabled</td>
<td>One unreachable of two or more</td>
<td>The unavailable Data Loss Prevention Network Prevent server is bypassed. Email is routed to the next Data Loss Prevention Network Prevent server according to the preference list, MX record, or both.</td>
</tr>
</tbody>
</table>
| Bypass disabled       | All unreachable                                 | Email is stored in Symantec Messaging Gateway's delivery queue. No outbound email is delivered. If the Data Loss Prevention Network Prevent servers continue to be unavailable, the delivery queue grows larger as time passes. Messages can get stuck in Symantec Messaging Gateway if the following conditions are met:  
  ■ The Maximum number of messages in the delivery queue limit is reached.  
  ■ The option Defer new connections when delivery queue is full is enabled.  
  New inbound connections and outbound connections are deferred when the delivery queue becomes full.  
  See “How to resolve a delivery queue back up to Symantec Network Prevent” on page 479.  
  See “Configuring SMTP advanced settings” on page 54. |
| Bypass enabled        | All unreachable                                 | Email is not routed to Data Loss Prevention Network Prevent servers, but Symantec Messaging Gateway does process it. Sensitive data can leave your site unscanned unless you configure Symantec Messaging Gateway appropriately.  
  See “How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled” on page 482. |

How to resolve a delivery queue back up to Symantec Network Prevent

If you disable bypass to the Symantec Network Prevent servers and the servers are unreachable, messages back up in the delivery queue. Normally when the Symantec Network Prevent servers become reachable again, the delivery queue automatically drains as the servers process the messages.
The delivery queue may not automatically drain for any of the following reasons:

- The amount of free hard disk space on Symantec Messaging Gateway is too low.
- The amount of free memory on Symantec Messaging Gateway is too low.
- The following conditions on Symantec Messaging Gateway are met:
  - The maximum number of messages in the delivery queue limit is reached.
  - The **Defer new connections when delivery queue is full** option is enabled.

See “About failure behavior with Data Loss Prevention Network Prevent” on page 478.

If Symantec Network Prevent servers continue to be unavailable, the queue may grow to a large size and consume large amounts of disk space. This lowered disk space can impact Symantec Messaging Gateway’s ability to deliver messages.

### Table 18-5  Process to resolve delivery queue backups

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Correct the issue with the Symantec Network Prevent servers. Confirm that the Symantec Network Prevent servers are running, have sufficient capacity for processing the given email volumes, and network paths are reachable.</td>
</tr>
<tr>
<td>2</td>
<td>If disk space is low on the Symantec Messaging Gateway Scanners, free disk space. Examples of ways to free disk space are to delete report data or logs. See <a href="#">delete on page 752</a>.</td>
</tr>
<tr>
<td>3</td>
<td>Temporarily or permanently enable bypass. Sensitive data can leave your site unscanned unless you configure Symantec Messaging Gateway appropriately. See “How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled” on page 482. See “Enabling or disabling bypass for Data Loss Prevention Network Prevent” on page 481.</td>
</tr>
<tr>
<td>4</td>
<td>Temporarily divert incoming message flow to a different Scanner.</td>
</tr>
</tbody>
</table>
| 5    | In the Control Center, access **Administration > Hosts > Configuration**. Select a Scanner, access the **SMTP** tab, and then select **Advanced Settings**. Temporarily change the following settings:  
  - **Maximum number of messages in delivery queue**: Increase.  
  - **Defer new connections when delivery queue is full**: Uncheck. See “Configuring SMTP advanced settings” on page 54. |
| 6    | Optionally, in the Control Center, click **Status > SMTP > Messages Queues**, and flush all of the queues. The MTA flushes queues automatically, but this manual action expedites queue processing. |
Enabling or disabling bypass for Data Loss Prevention Network Prevent

By default, outbound email bypasses Data Loss Prevention Network Prevent if all Data Loss Prevention Network Prevent servers are unavailable. Bypass is triggered only if a connection cannot be established with the Data Loss Prevention Network Prevent servers.

Bypass is not triggered in the following cases:

- The connection to Data Loss Prevention Network Prevent server is established but the connection is deferred.
- The email results in an SMTP 4xx temporary failure. The Symantec Messaging Gateway MTA attempts to redeliver the message later.
- The email results in an SMTP 5xx permanent failure. The Symantec Messaging Gateway MTA sends a bounce message to the sender.
- The Data Loss Prevention Network Prevent server is slow in processing the SMTP connection. However, if the SMTP connection times out, bypass is triggered if no other Data Loss Prevention Network Prevent servers are available.

Sensitive data can leave your site unscanned if Data Loss Prevention Network Prevent servers are unreachable. If you disable bypass and Data Loss Prevention Network Prevent is unavailable, all outbound email waits in the delivery queue which prevents timely delivery.

See “About failure behavior with Data Loss Prevention Network Prevent” on page 478.

See “How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled” on page 482.

To enable or disable bypass for Data Loss Prevention Network Prevent

1. In the Control Center, click Content > Settings > DLP Connect.
2. To choose the outbound Scanner you want to configure, check Enable DLP for the outbound Scanner host, and then choose the scanner from the drop down.
3. To enable bypass, check Enable bypass when all DLP servers are unreachable. To disable bypass, uncheck Enable bypass when all DLP servers are unreachable.
4. To apply the setting to all outbound Scanners, check Apply to all outbound Scanner hosts.
5. Click Save.
How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled

By default, outbound email bypasses Symantec Network Prevent if Symantec Network Prevent is unavailable. Sensitive data can leave your site unscanned if Symantec Network Prevent servers are unreachable. However, you can configure a policy on Symantec Messaging Gateway to prevent unscanned messages from leaving your site.

You can prevent unscanned messages from leaving your site when you create a content filtering policy for unscanned messages. In this policy configuration, the administrator of the content filtering folder receives notification if an unscanned message is detected. Unscanned messages are held in the content incident folder for review.

Table 18-6 describes the process that you can follow to prevent bypassed email from leaving your site.

Table 18-6: Process to create a content filtering policy to prevent bypassed email from leaving your site

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that the Symantec Network Prevent server adds a header to messages it processes. By default, Symantec Network Prevent adds the header <strong>X-CFilter-Loop:</strong> to messages it processes.</td>
</tr>
<tr>
<td>2</td>
<td>In Symantec Messaging Gateway, create a content filtering folder for unscanned messages, and configure email notification for the content filtering folder.</td>
</tr>
</tbody>
</table>
| 3    | In Symantec Messaging Gateway, create an email content filtering policy with the following characteristics:  
  - Policy template: Blank  
  - Apply to: Outbound messages  
  - Condition - Text in this specific part of the message: Message header  
  - Condition - Header name: X-Cfilter-Loop  
  - Condition - The message header: does not exist  
  - Perform the following action: Create an incident. Add additional actions for approved and rejected.  
  - In content incident folder: The folder that you created  
  - Hold message for review: checked  
  
  See "Creating a content filtering policy" on page 325. |

Alternatively, you may not need to store unscanned messages but want to be notified if messages are unscanned. You can create an email content filtering policy on Symantec Messaging Gateway to send an email notification if unscanned messages are detected.
See “About policy violation notifications” on page 377.

About Data Loss Prevention Network Prevent reports

Symantec Messaging Gateway does not provide reports specifically for Data Loss Prevention Network Prevent activity. Use Data Loss Prevention Network Prevent for reports on its activity. Some activity that is related to Data Loss Prevention Network Prevent may be part of reports on Symantec Messaging Gateway. For example, you can create an incident for the messages that are marked up by Data Loss Prevention Network Prevent. That incident activity is reflected in some content filtering reports.

About performance implications for Data Loss Prevention Network Prevent integration

Due to the additional processing that is involved, the integration with Data Loss Prevention Network Prevent may add latency to the outbound email delivery speed.

The amount of latency depends on the following factors:

- The volume of outbound email at your site
- The number and complexity of content filtering policies in Data Loss Prevention Network Prevent
- Message content and size
- The number of Data Loss Prevention Network Prevent servers compared to the volume of mail

You may be able to decrease latency and increase throughput by doing any of the following tasks:

- Add additional Data Loss Prevention Network Prevent servers
- Tune the **Maximum number of connections** and **Maximum number of connections from a single IP address** setting for outbound SMTP and SMTP delivery. This setting is a Symantec Messaging Gateway Scanner setting. See “Configuring SMTP advanced settings” on page 54.
- Tune the **NumThreads** setting on the Data Loss Prevention Network Prevent server to optimize throughput depending on the volume of outbound email at your site.

See “Configuring email connections to and from Data Loss Prevention Network Prevent” on page 486.
About Data Loss Prevention Network Prevent preference order

If you have multiple Data Loss Prevention Network Prevent servers, you can configure the order in which Symantec Messaging Gateway employs Data Loss Prevention Network Prevent servers. You can set the preference in the Control Center or in MX records.

Table 18-7 describes the preference types and where you set them.

<table>
<thead>
<tr>
<th>Preference type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preference on Symantec Data Loss Prevention Setup</td>
<td>You configure this type of preference on the <strong>Content &gt; Settings &gt; DLP Connect &gt; Symantec Data Loss Prevention Setup</strong> page in the Control Center. See &quot;Configuring email connections to and from Data Loss Prevention Network Prevent&quot; on page 486.</td>
</tr>
<tr>
<td>MX record preference</td>
<td>You configure MX record preference in the DNS records for Data Loss Prevention Network Prevent with your DNS software. You must configure MX record preference if the host name that you specify routes to more than one Data Loss Prevention Network Prevent server. The valid MX preference range is 0 - 65535. Typical values are every 10 digits between 10 and 100.</td>
</tr>
</tbody>
</table>

- Choose a lower preference number for Data Loss Prevention Network Prevent servers that run on high network bandwidth computers with ample CPU and hard disk resources. Choose a higher preference number for Data Loss Prevention Network Prevent servers that run on lower network bandwidth computers with fewer CPU and hard disk resources.
- For both types of preference, lower numbers are attempted before higher numbers. If a Data Loss Prevention Network Prevent server is unreachable, the server with the next higher preference number is tried. For example, a Data Loss Prevention Network Prevent server with a preference of 1 is tried before a Data Loss Prevention Network Prevent server with a preference of 2.
- In the Control Center, if you assign a Preference value of 1 to two Data Loss Prevention Network Prevent servers, Symantec Messaging Gateway randomly picks one of them. If that server becomes unavailable the other server with Preference 1 becomes the primary server. When that server becomes unavailable, Symantec Messaging Gateway attempts to reconnect with the first server. A Data Loss Prevention Network Prevent server with a higher Preference is used only if both hosts with Preference 1 become unavailable.
- You can use both types of preference in combination. The preference settings on the **Symantec Data Loss Prevention Setup** page are compared before the preference is checked in the MX record for the chosen host name.
Troubleshooting Data Loss Prevention Network Prevent integration: messages bounce

If you have recently enabled routing to Data Loss Prevention Network Prevent and email messages bounce, check the following:

- **Accept Scanned Mail from DLP Servers** IP address is configured correctly on the Symantec Data Loss Prevention Setup page.
- The Prevent Server is correctly configured with the reflected port setting that points to the Scanner port.


See “About Data Loss Prevention Network Prevent” on page 474.

See “Configuring email connections to and from Data Loss Prevention Network Prevent” on page 486.

Troubleshooting Data Loss Prevention Network Prevent integration: deferred messages

If outbound email returns with the following error:

421 Forwarding agent unavailable. Closing connection.

the **Remote SMTP Listener Port** for Data Loss Prevention Network Prevent does not match the inbound email port on Symantec Messaging Gateway.

See “How to configure Symantec Network Prevent to return email to Symantec Messaging Gateway” on page 486.

This message describes the error that is seen in Symantec Data Loss Prevention from Symantec Version 8.1. Future versions may produce different errors.
How to configure Symantec Network Prevent to return email to Symantec Messaging Gateway

You must configure Symantec Network Prevent server to return email to Symantec Messaging Gateway on the expected port. The default outbound email port for Symantec Messaging Gateway is 25. The default Remote SMTP Listener Port in Symantec Network Prevent is 10026. Change the Symantec Network Prevent port to match the Symantec Messaging Gateway outbound email port.

See “Configuring email connections to and from Data Loss Prevention Network Prevent” on page 486.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check the default outbound email port on Symantec Messaging Gateway.</td>
<td>The outbound mail IP address port appears on the <strong>SMTP</strong> tab of the <strong>Host Configuration</strong> page in the Control Center.</td>
</tr>
<tr>
<td>2</td>
<td>Set the <strong>Remote SMTP Listener Port</strong> for Symantec Network Prevent.</td>
<td>Set the <strong>Remote SMTP Listener Port</strong> for Symantec Network Prevent to the outbound email port that Symantec Messaging Gateway uses. See the Symantec Network Prevent documentation for configuration details.</td>
</tr>
</tbody>
</table>

Configuring email connections to and from Data Loss Prevention Network Prevent

If you have one or more Data Loss Prevention Network Prevent servers, you can route email to them from Symantec Messaging Gateway. You also must configure Data Loss Prevention Network Prevent to route email back to Symantec Messaging Gateway. If you have multiple outbound Scanners, you can route outbound mail to Data Loss Prevention Network Prevent servers differently for each Scanner, or you can apply the same settings to all outbound Scanners.

See “How to configure Symantec Network Prevent to return email to Symantec Messaging Gateway” on page 486.
To configure email connections to and from Data Loss Prevention Network Prevent

1 In the Control Center, click Content > Settings > DLP Connect.

2 Click Enable DLP for the outbound Scanner host to choose the outbound Scanner you want to configure.

   You can skip this step if you have only one outbound Scanner. If you want to apply the same settings to all outbound Scanners, choose one and you can later check Apply to all outbound Scanner hosts.

3 Under Route Outbound Mail to DLP servers, click Add to add a blank row.

4 Under Host or IP Address, specify the domain name or IP address of a Data Loss Prevention Network Prevent server.

   The domain name can be of the form server1.symantecexample.com or symantecexample.com. Specify a domain name (not IP address) if MX records are configured for the Data Loss Prevention Network Prevent server.

5 Under Port, specify the port number on the Data Loss Prevention Network Prevent server to which the outbound email should be routed.

   The default port is 10025. Ensure that the Local SMTP Listener Port on the Data Loss Prevention Network Prevent server is set to the same port number.

6 Check MX Lookup to enable MX lookup for the Data Loss Prevention Network Prevent server.

   If you check MX Lookup, ensure that you have specified a domain name (not IP address) in the form server1.symantecexample.com or symantecexample.com.

7 Under Preference (1 - 100), specify the preference of this Data Loss Prevention Network Prevent server as compared to all the defined Data Loss Prevention Network Prevent servers.

   See “About Data Loss Prevention Network Prevent preference order” on page 484.

   Enable bypass when all DLP servers are unreachable is described in another section.
   See “Enabling or disabling bypass for Data Loss Prevention Network Prevent” on page 481.

8 Under TLS Encryption, check Optional delivery encryption to attempt or require TLS encryption on mail delivered to Data Loss Prevention Network Prevent. If you enable delivery encryption, you must choose one of three certificate options:

   ■ Attempt TLS encryption: attempt, but do not require, TLS encryption. Requires either self-signed or Certificate Authority-signed certificates on both the Symantec Messaging Gateway and Data Loss Prevention Network Prevent servers.

   ■ Require TLS encryption and don't verify certificate: requires either self-signed or Certificate Authority-signed certificates on both the Symantec Messaging Gateway and Data Loss Prevention Network Prevent servers.
- **Require TLS encryption and verify certificate**: requires a valid certificate signed by a Certificate Authority installed on both the Symantec Messaging Gateway and Data Loss Prevention Network Prevent servers.

For greater security, you can disable support for early encryption protocols on the Protocols > SMTP > Settings > SMTP tab. The SSL Restrictions setting affects the protocols that SMG can use to encrypt the communications that it exchanges with Data Loss Prevention Network Prevent.

See “Specifying SSL restrictions for TLS communications” on page 96.

If a Certificate Authority other than the defaults provided with Symantec Messaging Gateway is needed to sign the certificates used for TLS encryption, you can import it on the Administration > Settings > Certificate Settings page.

9. Under **Accept Scanned Mail from DLP servers**, click **Add** to add a blank row.

10. Specify an IP address from which Symantec Messaging Gateway should expect email from Data Loss Prevention Network Prevent.

Add additional rows to specify the IP addresses of all Data Loss Prevention Network Prevent servers from which Symantec Messaging Gateway should expect email. For example, you may have only one host name specified under **Route Outbound Mail to DLP servers**. But if that host name resolves to multiple Data Loss Prevention Network Prevent servers, add the IP addresses of all of those servers.

11. If you want the settings to apply to all outbound Scanners, check **Apply to all outbound Scanner hosts**.

12. Click **Save**.

### Creating an incident based on Symantec Network Prevent header markup

Below is a sample method to handle any sensitive data that Symantec Network Prevent detects. This method requires that you configure both Symantec Network Prevent and Symantec Messaging Gateway.

In this example, Symantec Network Prevent adds a custom header to matching messages. Symantec Messaging Gateway creates an incident for messages with the custom header and holds the messages for review. So messages are not delivered to the original recipient but are instead routed to a content filtering folder on Symantec Messaging Gateway. An administrator can approve, reject, forward, archive, delete, and manage the messages in the content incident folder.

Table 18-9 describes the process to create an incident based on Symantec Network Prevent header markup.
Table 18-9

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure Symantec Network Prevent to add a custom header to the messages that it detects with sensitive data on the <strong>Add/Edit Response Rule</strong> screen under <strong>Create a Modify SMTP Message response</strong> rule. You can add up to three RFC 2822 header lines. Symantec recommends that you use the header <strong>X-Cfilter:</strong> with different values depending upon the wanted action on Symantec Messaging Gateway or scan verdict. For example, you can specify <strong>X-Cfilter: Symantec Incident</strong> to mark messages for a content incident folder or <strong>X-Cfilter: SSN</strong> for any messages that contain social security numbers.</td>
</tr>
<tr>
<td>2</td>
<td>In Symantec Messaging Gateway, create a content filtering folder, such as &quot;Symantec Incidents&quot;. You may want to enable email notification for the content filtering folder. See &quot;About content incident folders&quot; on page 419.</td>
</tr>
</tbody>
</table>
| 3    | In Symantec Messaging Gateway, create an email content filtering policy with the following characteristics:  
  - **Policy template:** Blank  
  - **Apply to:** Outbound messages  
  - **Condition - Text in this specific part of the message:** Message header  
  - **Condition - Header name:** The header you configured, such as **X-Cfilter: Symantec Incident**  
  - **Condition - The message header:** exists  
  - **Perform the following action:** Create an incident. Add additional actions for approved and rejected.  
  - **In content incident folder:** The folder that you created  
  - **Hold message for review:** checked |

About taking Data Loss Prevention Network Prevent servers offline for maintenance

Occasionally you may need to take one or more Data Loss Prevention Network Prevent servers offline to perform maintenance, such as to install a new software release.

Table 18-10 describes the effect on mail flow for the options available.
## Options for taking Data Loss Prevention Network Prevent servers offline for maintenance

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| If you have multiple Data Loss Prevention Network Prevent servers, perform maintenance on one server at a time | You can perform maintenance on one server at a time if either of the following conditions are true:  
- You have configured multiple Data Loss Prevention Network Prevent servers in Symantec Messaging Gateway  
- The address that you specify for Data Loss Prevention Network Prevent in Symantec Messaging Gateway resolves to multiple Data Loss Prevention Network Prevent servers using MX records  
The Data Loss Prevention Network Prevent server that is not available is ignored and the next available Data Loss Prevention Network Prevent server in the preference list is used. |
| Disable routing to Data Loss Prevention Network Prevent | Outbound email bypasses Data Loss Prevention Network Prevent servers.  
You must manually re-enable routing to Data Loss Prevention Network Prevent servers when they become available again. Sensitive data can leave your site unscanned by Data Loss Prevention Network Prevent servers.  
See “How to create a policy to detect unscanned email if Symantec Network Prevent bypass is enabled” on page 482.  
See “Enabling or disabling bypass for Data Loss Prevention Network Prevent” on page 481. |
Table 18-10  Options for taking Data Loss Prevention Network Prevent servers offline (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable bypass</td>
<td>Outbound email bypasses Data Loss Prevention Network Prevent servers if none are available. Sensitive data can leave your site unscanned by Data Loss Prevention Network Prevent servers. When Data Loss Prevention Network Prevent servers are available again, Symantec Messaging Gateway automatically routes outbound email to them. Bypass is enabled by default. If you disable bypass, outbound email remains in the delivery queue. When you later activate Data Loss Prevention Network Prevent servers, the delayed email is scanned for sensitive data. However, outbound email may be bounced back to the senders if the connection is not reestablished in time. Messages are queued up for three days by default before they are bounced. If bypass is disabled, you can perform maintenance on Data Loss Prevention Network Prevent servers when you do the following tasks: ■ Enable bypass in the Control Center of Symantec Messaging Gateway. ■ Perform maintenance on the Data Loss Prevention Network Prevent servers. ■ When work on the servers is complete, bring the Data Loss Prevention Network Prevent servers online again. ■ Disable bypass in the Control Center of Symantec Messaging Gateway. Ensure that your organization's policies let you enable bypass temporarily. See &quot;Enabling or disabling bypass for Data Loss Prevention Network Prevent&quot; on page 481.</td>
</tr>
<tr>
<td>Stop outbound message queue</td>
<td>No outbound messages are delivered while the queue is stopped. Data Loss Prevention Network Prevent servers and Symantec Messaging Gateway eventually scan all outbound messages. You must manually reenable the outbound message queue when Data Loss Prevention Network Prevent servers become available again. See “MTA and message queue behavior” on page 74.</td>
</tr>
<tr>
<td>Enable routing to Data Loss Prevention Network Prevent but disable bypass</td>
<td>Outbound messages back up in the delivery queue. See “Enabling or disabling bypass for Data Loss Prevention Network Prevent” on page 481.</td>
</tr>
</tbody>
</table>
Configuring Directory Data integration

This chapter includes the following topics:

- About using the directory data service
- Configuring Directory Data integration
- Creating a data source
- Adding a data source
- Enabling functions on a new data source
- About data source queries

About using the directory data service

The directory data service lets you use the information that is stored in your Lightweight Directory Access Protocol (LDAP) directories for features in the Symantec Messaging Gateway.

Symantec Messaging Gateway provides four functions that you can enable for your data source: authentication, address resolution, routing, and recipient validation. You enable one or a combination of these functions for each data source.

See “About data sources and functions” on page 499.

To use your directory data for these features, you configure data sources for desired functionality, and also configure additional features in Symantec Messaging Gateway.

See “Creating a data source” on page 496.

You can use these functions to support feature configuration within Symantec Messaging Gateway.
Table 19-1 describes the functionality in Symantec Messaging Gateway that relies on directory data service configurations.

Table 19-1  Features in Symantec Messaging Gateway that use configured data sources

<table>
<thead>
<tr>
<th>Feature</th>
<th>Data source function to enable</th>
<th>Additional setup tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject or drop invalid recipients.</td>
<td>Recipient validation</td>
<td>Configure invalid recipient handling and enable recipient validation for at least one domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Setting up invalid recipient handling” on page 99.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding or editing domains” on page 82.</td>
</tr>
<tr>
<td>Use directory harvest attack recognition.</td>
<td>Recipient validation</td>
<td>Configure directory harvest attack and domains.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding or editing domains” on page 82.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring directory harvest attack recognition” on page 149.</td>
</tr>
<tr>
<td>Participate in the Symantec Probe Network.</td>
<td>Recipient validation</td>
<td>Enable recipient validation for at least one domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding or editing domains” on page 82.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating probe accounts from invalid recipient email addresses” on page 318.</td>
</tr>
</tbody>
</table>
Table 19-1  Features in Symantec Messaging Gateway that use configured data sources (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Data source function to enable</th>
<th>Additional setup tasks</th>
</tr>
</thead>
</table>
| Implement end-user quarantine and allow end-users access to spam quarantine messages. | Authentication | Configure at least one policy group to quarantine spam messages, configure quarantine settings, and configure spam filtering.  
  See “About selecting filtering policies for policy groups” on page 196.  
  See “About quarantining spam” on page 280.  
  See "About filtering email spam and unwanted messages" on page 248.  
  See “About quarantining spam” on page 280. |
| Let authenticated end users remotely send email messages using the SMTP authentication protocol. | Authentication | Set up SMTP authentication.  
  See "About using SMTP authentication" on page 103. |
| Use LDAP groups and distribution lists to apply policies. | Address resolution | Add an LDAP group or distribution list as a member of a policy group.  
  See “About selecting filtering policies for policy groups” on page 196. |
| Allow end users to configure email language preferences and Good and Bad Senders lists. | Address resolution and authentication  
  User preference functionality requires that a data source is enabled for both authentication (to let the user log in and set preferences) and for address resolution (to replicate the preferences to the Scanner). | Enable at least one policy group for end-user settings.  
  See “About selecting filtering policies for policy groups” on page 196. |
Table 19-1  Features in Symantec Messaging Gateway that use configured data sources (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Data source function to enable</th>
<th>Additional setup tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-route user email to an alternate address or alternate mail host based on directory information.</td>
<td>Routing</td>
<td>Configure domains.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding or editing domains” on page 82.</td>
</tr>
</tbody>
</table>

Configuring Directory Data integration

Table 19-2  Processes for setting up a directory data service

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a new data source.</td>
<td>See “Creating a data source” on page 496.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding a data source” on page 496.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enable functions for your new data source.</td>
<td>See “Enabling functions on a new data source” on page 498.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a recipient validation data source” on page 500.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating an authentication data source” on page 502.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating a routing data source” on page 506.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating an address resolution data source” on page 508.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Customize and test data source queries.</td>
<td>See “Creating and testing a custom recipient validation query” on page 517.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and testing a custom routing query” on page 524.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Creating and testing a custom address resolution query” on page 527.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set directory data cache.</td>
<td>See “About preloading your directory data cache” on page 564.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Preloading your data cache” on page 564.</td>
</tr>
</tbody>
</table>
Creating a data source

Symantec Messaging Gateway provides a wizard that guides you through the process of creating a new data source.

Table 19-3 describes the process to create a data source.

Table 19-3 How to create a data source

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Provide details for the LDAP server hosting your directory data.</td>
<td>Such details include host settings, bind DN, credentials, and SSL status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding a data source” on page 496.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Optionally, adjust your connection settings and cache settings.</td>
<td>You can choose to use the default values, or you can edit the cache settings and connection settings to suit your needs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Configuring data source advanced settings” on page 566.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable and configure the functions that you want your data source to provide.</td>
<td>You can configure one or more functions for a single data source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Enabling functions on a new data source” on page 498.</td>
</tr>
</tbody>
</table>

Once you save your new data source, you can modify it as needed.

See “Editing a data source” on page 539.

Adding a data source

The Add Directory Data Source wizard guides you through the tasks necessary to create and configure new data sources. The first step in this process is to configure the LDAP server that provides data for your directory source.

See “Creating a data source” on page 496.
For authentication, address resolution, or routing data sources, the results that are returned must be unique. Therefore you cannot have identical or overlapping (where two data sources can potentially return the same result) data sources. If the Directory data integrity errors alert is configured on the Alerts page, that alert is triggered when this condition is detected. See “Configuring alerts” on page 688.

When the directory data service cannot properly communicate with an LDAP server (for example, if the network link to the LDAP server is down or when a data integrity problem is encountered) message processing and user authentication can be affected. See “About data sources and functions” on page 499.

To add a data source

1. Click Administration > Settings > Directory Integration.
2. On the Directory Integration Settings - Directory Data Sources page, click Add.
   The LDAP Server Configuration page appears.
3. In the Data source name field, provide a unique name for the data source.
4. Select the Directory type that your LDAP source uses. Available choices are as follows:
   - Active Directory
   - Active Directory Global Catalog
   - iPlanet/Sun ONE/Java Directory Server
   - Domino
   - Other (can be any LDAPv3 compliant directory)
   Though Symantec Messaging Gateway is compatible with any LDAPv3 directory, it is specifically designed to support configurations with the four specific directory types listed. If you select "other" for your directory type, you might need to consult your directory documentation to ensure proper functionality.
5. In the Host name field, type the host name or IP address of the LDAP server.
6. The Port is used to access the LDAP server. The port is automatically populated based on your directory type and SSL settings but can be modified by typing a new value into this field.
7. Check Enable SSL if you want to enable SSL on all connections to the LDAP server host. Encryption is provided regardless of the certificate authority that is used to sign the LDAP server x.509 certificate. If you change this checkbox, the port is automatically updated to the default ports for your directory type. Confirm the port if modifying this setting.
8. Check Anonymous bind if you want to let the directory data service connect to the LDAP server without providing specific user ID and password information. Or check Use the Following to provide the directory data service with specific authentication credentials.
9 If you checked **Use the following**, provide the bind credentials in the following fields:

- **Name (Bind DN)**
  The distinguished name (DN) that is used for authenticating to the LDAP server.
  For Active Directory or Global Catalog server, you can optionally use the full DN, the NetBIOS and logon name (NetBIOS\SAM Account Name), or the User Principal Name.

- **Password**
  Password to be used to authenticate to the LDAP server.

10 Click **Test login** to validate your authentication to the LDAP server.

This test only verifies that the LDAP server can be reached and that the account has read access to the root of the directory data tree on a directory server. Therefore, a successful test result does not guarantee that the credentials can succeed elsewhere in the directory. This is particularly true for anonymous access. You should verify access before deployment by using the Test Query function when configuring individual functions for your data source.

11 Click **Show Advanced Settings** if you want to configure optional LDAP server and cache settings.

See “Configuring data source advanced settings” on page 566.

12 When you are finished, click **Next** to configure the functions for the data source.

See “Enabling functions on a new data source” on page 498.

### Enabling functions on a new data source

The second step in the **Add Directory Data Source** wizard is to enable and configure functions for your data source. Before you can enable functions for your data source, you must complete the first step in the wizard and confirm or configure the LDAP connection settings for that source on the **LDAP Server Configuration** page.

See “Adding a data source” on page 496.

Functions enable certain behaviors for your data sources and let you take advantage of many Symantec Messaging Gateway features. You can configure your data source for one or multiple functions.

See “About data sources and functions” on page 499.

**To enable functions on a new data source**

1 Add your data source and configure your server integration settings in the **Directory Integration Settings - LDAP Server Configuration** page then click **Next**.

   See “Adding a data source” on page 496.

2 In the **Add Directory Data Source - Directory Data Source Functions** page do the following tasks:
To enable and configure your data source for end-user authentication, quarantine address resolution, or SMTP authentication, check **Authentication**.
See “Creating an authentication data source” on page 502.
See “About using SMTP authentication” on page 103.
To customize your authentication, quarantine address resolution, or SMTP authentication query, check **Customize Query**.
See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.

To enable and configure your data source for address resolution, check **Address resolution**.
See “Creating an address resolution data source” on page 508.
To customize your address resolution configuration, click **Customize Query**.
See “Creating and testing a custom address resolution query” on page 527.

To enable and configure your data source for routing, check **Routing**.
See “Creating a routing data source” on page 506.
To customize your routing configuration, click **Customize Query**.
See “Creating and testing a custom routing query” on page 524.

To enable and configure your data source for recipient validation, check **Recipient validation**.
See “Creating a recipient validation data source” on page 500.
To customize your recipient validation configuration, click **Customize Query**.
See “Creating and testing a custom recipient validation query” on page 517.

3 When you have configured all of the functions for your new data source, click **Next** and verify your configuration.

4 When you are satisfied with your configuration, click **Save** to save and deploy your data source.

**About data sources and functions**

To integrate your LDAP directories with Symantec Messaging Gateway you must first configure data sources. A data source is a set of configuration data that allows your system to easily connect to and use your LDAP server.

When you configure a data source, you configure the parameters for connecting to your LDAP server and the functions that each data source provides.

Symantec Messaging Gateway supports redundant data sources only for the recipient validation function as there is no uniqueness requirement for email addresses or user names. Other DDS functions such as Authentication, Routing, and Address Resolution have uniqueness requirements and do not support redundant data sources.

See “Creating a data source” on page 496.
Once you have configured your directory data sources, you can configure other features across Symantec Messaging Gateway.

For example, if you want to use your new data source to apply a policy using an LDAP group, you must enable the address resolution function for that data source and configure an address resolution query.

See “About using the directory data service” on page 492.

You can configure one or more of the following functions for each of your data sources:

- **Authentication**
  Use the authentication function to securely authenticate end-user login to the Control Center and to authenticate users wishing to send email. The authentication function includes quarantine address resolution, which lets you better manage spam quarantine through improved handling of aliases, distribution lists, and invalid addresses.
  See “About using the authentication function with your data source” on page 510.

- **Recipient validation**
  Use the recipient validation function to validate email addresses against directory data and drop messages or reject connections for invalid recipients.
  See “About using the recipient validation function with your data source” on page 513.

- **Routing**
  Use the routing function to route messages to alternate addresses or mail hosts on a per-user basis using directory data.
  See “About using the routing function with your data source” on page 511.

- **Address resolution**
  Use the address resolution function to apply policies to users and groups consistently.
  See “About using the address resolution function with your data source” on page 512.

### Creating a recipient validation data source

Recipient validation works with other features within Symantec Messaging Gateway to help you identify and manage invalid recipients and the messages sent to those recipients. Symantec Messaging Gateway supports redundant data sources only for the recipient validation function as there is no uniqueness requirement for email addresses or user names. Other DDS functions such as Authentication, Routing, and Address Resolution have uniqueness requirements and do not support redundant data sources.

See “About using the recipient validation function with your data source” on page 513.

Enabling your functions is the second step in the Add Directory Data Source wizard. Before you perform the task described in this topic, you must confirm or configure the LDAP connection settings for that source on the LDAP Server Configuration page.

See “Adding a data source” on page 496.
See “Enabling functions on a new data source” on page 498.

If you want to use invalid recipient handling functionality you must also configure invalid recipient handling and enable recipient validation for at least one domain.

See “Setting up invalid recipient handling” on page 99.

See “Adding or editing domains” on page 82.

---

**Note:** Be sure that your data sources do not produce overlapping results to prevent directory data service errors. If the directory data service cannot properly communicate with the LDAP directory server (for example, if the network link to the LDAP server is down) when it attempts to determine the validity of a message recipient, the MTA returns an error indicating that the delivery attempt should be retried later. See “About data sources and functions” on page 499.

---

To configure recipient validation for a new data source

1. Add your data source and configure your server integration settings in the Directory Integration Settings - LDAP Server Configuration page then click Next.

   See “Adding a data source” on page 496.

2. On the Add Directory Data Source - Directory Data Source Functions page, check Recipient validation.

3. In the Test email address field, type an email address that can be used to test and validate your recipient validation configuration. Symantec recommends that you test at least one valid and one invalid address. If the test produces unexpected results, use Customize Query to verify your settings and directory data.

4. If you want to examine or modify the default settings for your queries, click Customize Query. Create custom queries to more accurately reflect your system's configuration.

   See “Creating and testing a custom recipient validation query” on page 517.
5 Click Test Query to validate your query using the test email address provided.

This test is conducted against the directory data service instance that is running on the Control Center host. It cannot be used to verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source being tested. Test results do not provide information about the effects of other data sources or system settings such as aliasing and masquerading.

6 You can configure your data source for multiple functions or click Next to review your changes and save your deployment.

---

Note: On the Protocols > SMTP > Settings page, on the SMTP tab under Address Validation, check Remove subaddress in recipient validation directory query, if you need support for subaddressing.

Subaddressing consists of additional text in the local portion of an email address (the part before the @), that follows a plus sign or a minus sign. When checked, Symantec Messaging Gateway removes the +detail or -detail portion of the email address prior to completing an LDAP recipient validation query.

If you use plus or minus signs in email addresses for any purpose other than subaddressing, enabling this feature can cause recipient validation errors.

---

See "Enabling functions on a new data source" on page 498.

Creating an authentication data source

Authentication lets end users authenticate to the LDAP server and configure user preferences. It also lets you configure SMTP authentication.

See “About using the authentication function with your data source” on page 510.

See “About using SMTP authentication” on page 103.

Enabling your functions is the second step in the Add Directory Data Source wizard. Before you can enable functions for your data source, you must confirm or configure the LDAP connection settings for that source on the LDAP Server Configuration page.

See “Adding a data source” on page 496.

To prevent directory data service errors, be sure that your data sources do not produce overlapping results. Table 19-4 describes how directory data service processes authentication errors for the most common conditions.

See “About data sources and functions” on page 499.
Table 19-4 Common directory data service authentication errors

<table>
<thead>
<tr>
<th>Authentication error</th>
<th>System behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The directory data service cannot properly communicate with the LDAP directory server when it attempts to authenticate a user to either Control Center or SMTP server. This can happen, for example, if the network link to the LDAP server is down.</td>
<td>The error &quot;service is temporarily unavailable&quot; appears. If the proper alerts are enabled on the Alerts page, a Directory data access errors alert is triggered.</td>
</tr>
<tr>
<td>The directory data service cannot uniquely determine the identity of the user from the user name provided.</td>
<td>The error &quot;service is temporarily unavailable&quot; appears. If the proper alerts are enabled on the Alerts page, a Directory data access errors alert is triggered.</td>
</tr>
<tr>
<td>The directory data service cannot properly communicate with the LDAP directory server when it attempts to resolve the recipient of a quarantined message to the recipient's primary email address or uniquely determine the primary email address of the recipient.</td>
<td>The message is kept in the delivery queue. If the alerts are enabled on the Alerts page, the appropriate alert is triggered.</td>
</tr>
</tbody>
</table>

See “Configuring alerts” on page 688.

To configure authentication for a new data source

1. Add your data source and configure your server integration settings in the Directory Integration Settings - LDAP Server Configuration page then click Next.

   See “Adding a data source” on page 496.

2. On the Add Directory Data Source - Directory Data Source Functions page, check Authentication.

3. In the Authentication type pull-down menu, choose one of the following:

   - Control Center authentication only To authenticate end users for accessing quarantine or setting end-user preferences only.
   - SMTP authentication only To enable remote users to use Symantec Messaging Gateway to send email using SMTP authentication.
   - Control Center and SMTP authentication To enable both Control Center and SMTP authentication.
4 If you selected **Control Center authentication only** or **Control Center and SMTP authentication** as the authentication type, confirm or configure the following test data or click **Customize Query** to view or customize your query.

See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.

**Test user name**
Type a user name that can be used to test and validate your authentication configuration.
Symantec recommends that you verify your settings using a variety of input designed to produce both successful authentication and unsuccessful authentication. If the test produces unexpected results, use **Customize Query** to verify your settings and directory data.

**Test password**
Type the password for the test user name.

**Test domain (optional)**
Type a NetBIOS domain for the provided test credentials.
You only need supply the test domain if you use Active Directory or the Active Directory Global Catalog and the provided **Test user name** is domain-specific.

**Test Query**
Click to validate your query using the test information provided.
This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot verify connectivity from attached scanners to your LDAP server.
Test results reflect only the data source being tested. The results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.

**Customize Query**
Click **Customize Query** if you want to examine or modify the default settings for your queries. You can create custom queries to more accurately reflect your system’s configuration.
See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.

**Test email address**
Type an email address that can be used to test and validate your quarantine address resolution configuration. Symantec recommends that you test your data source using a combination of addresses, including a user address, distribution list address, alias address, and an invalid address.
### Test Query
Click to validate the defined quarantine address resolution query using the provided test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source being tested. Test results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.

### Customize Query
Click **Customize Query** if you want to examine or modify the default settings for your queries.

See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.
If you selected **SMTP authentication only** or **Control Center and SMTP authentication** as the authentication type, configure the following fields or click **Customize Query** to view or customize your query.

See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.

If you selected **Control Center and SMTP authentication**, you can also check **Share Control Center and SMTP Authentication query details** to populate your SMTP details with those provided for the Control Center and skip this step.

- **Test user name**: Type a user name that can be used to test and validate your SMTP authentication configuration.
  
  Symantec recommends that you verify your settings using a variety of input designed to produce both successful authentication and unsuccessful authentication. If the test produces unexpected results, click **Customize Query** to verify your settings and directory data.

- **Test password**: Type the password for the test user name.

- **Test Query**: Click to validate the defined SMTP Authentication query using the provided test user name and password.
  
  This test is conducted against the directory data service instance that is running on the Control Center host. It cannot be used to verify connectivity from attached scanners to your LDAP server.

  Test results reflect only the data source being tested and. The results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.

- **Customize Query**: Click **Customize Query** to create a customer query, or to examine the default settings for your query.
  
  You can create custom queries to more accurately reflect your system’s configuration.

  See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.

You can configure your data source for multiple functions or click **Next** to review your changes and save your deployment.

See “Enabling functions on a new data source” on page 498.

### Creating a routing data source

The routing function uses the information provided by your data source to route messages to addresses and domains.
See “About using the routing function with your data source” on page 511.

Each domain can be configured to route messages based on directory data source, destination hosts, or MX lookup. This section talks about routing that uses a directory data source. For the other types of routing, you should consult the domain documentation.

See “Adding or editing domains” on page 82.

Enabling your functions is the second step in the Add Directory Data Source wizard. Before you can enable functions for your data source you must configure the LDAP connection settings for that source on the LDAP Server Configuration page.

See “Creating a data source” on page 496.

Be sure that your data sources do not produce overlapping results to prevent directory data service errors. Table 19-5 describes how directory data service processes routing errors for the most common conditions.

See “About data sources and functions” on page 499.

**Table 19-5** Directory data service routing errors

<table>
<thead>
<tr>
<th>Directory data service routing process error</th>
<th>System behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The directory data service cannot properly communicate with the LDAP directory server when it attempts to determine the routing information for a message recipient. This can happen, for example, if the network link to the LDAP server is down.</td>
<td>The MTA queues the message and periodically retries to perform the operation. A Directory data access errors alert is triggered.</td>
</tr>
<tr>
<td>The directory data service cannot uniquely determine the LDAP entry that corresponds to the recipient.</td>
<td>The message is delivered without any attempt to apply routing information. If the proper alerts are enabled on the Alerts page, a Directory data integrity errors alert is triggered.</td>
</tr>
</tbody>
</table>

See “Configuring alerts” on page 688.

To configure routing for a new data source:

1. Add your data source and configure your server integration settings in the Directory Integration Settings - LDAP Server Configuration page then click Next.

   See “Adding a data source” on page 496.

2. In the Add Directory Data Source - Directory Data Source Functions page, check Routing.
In the Test email address field, type an email address that can be used to test and validate your routing configuration. If the test produces unexpected results, use Customize Query to verify your settings and directory data.

The wizard provides a set of default attribute values for an LDAP configuration that uses the SunOne directory type. If your configuration uses a different directory type, or if you want to route mail using a different routing attribute, click Customize Query to configure your query.

See “Creating and testing a custom routing query” on page 524.

Click Test Query to validate your query data using the provided test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot be used to verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source tested. The test does not provide information about the effects of other data sources or system settings such aliasing and masquerading.

You can configure your data source for multiple functions or click Next to review your changes and save your deployment.

See “Enabling functions on a new data source” on page 498.

Creating an address resolution data source

The address resolution function resolves alias and distribution list data. This lets you apply policies on a per-user basis by using LDAP-based group memberships to define policies.

See “About using the address resolution function with your data source” on page 512.

Enabling your functions is the second step in the Add Directory Data Source wizard. Before you perform the task described in this topic you must confirm or configure the LDAP connection settings for that source on the LDAP Server Configuration page.

See “Adding a data source” on page 496.

Be sure that your data sources do not produce overlapping results to prevent directory data service errors. Table 19-6 describes how the directory data service processes address resolution errors for the more common error conditions.

See “About data sources and functions” on page 499.
### Table 19-6  Directory data service processes address resolution errors

<table>
<thead>
<tr>
<th>Address resolution error condition</th>
<th>System behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>The directory data service cannot properly communicate with the LDAP directory server or uniquely</td>
<td>The MTA returns a &quot;451 Requested action aborted: error in processing&quot; error. Assuming that the directory data service alerts are enabled on the</td>
</tr>
<tr>
<td>determine the LDAP entry that corresponds to the recipient, when it attempts to resolve the</td>
<td><strong>Alerts</strong> page, the appropriate directory data service alert is triggered.</td>
</tr>
<tr>
<td>recipient of a message for BATV purposes.</td>
<td></td>
</tr>
<tr>
<td>An example of this condition is if the network link to the LDAP server is down.</td>
<td></td>
</tr>
<tr>
<td>The directory data service cannot properly communicate with the LDAP directory server when it</td>
<td>The message is placed in the inbound deferred queue and periodically retried. If the alert is enabled, a <strong>Directory data access errors</strong> alert is</td>
</tr>
<tr>
<td>attempts to resolve the recipient of a message for scanning purposes.</td>
<td>triggered.</td>
</tr>
<tr>
<td>The directory data service cannot uniquely determine the LDAP entry that corresponds to the</td>
<td>The message is delivered with no attempt to apply address resolution information. Policy groups are applied according to the original recipient</td>
</tr>
<tr>
<td>recipient.</td>
<td>address only. If the alert is enabled, a <strong>Directory data integrity errors</strong> alert is also triggered.</td>
</tr>
<tr>
<td>See “Configuring alerts” on page 688.</td>
<td></td>
</tr>
</tbody>
</table>

**To configure address resolution for a new data source**

1. Add your data source and configure your server integration settings in the **Directory Integration Settings - LDAP Server Configuration** page then click **Next**.
   
   See “Adding a data source” on page 496.

2. On the **Add Directory Data Source - Directory Data Source Functions** page, check **Address resolution**.

3. In the **Test email address** field, type an email address that can be used to test and validate your configuration.

   Symantec recommends that you test a variety of addresses that include a primary address, an alias address, a distribution list address, and an invalid address. If the test produces unexpected results, click **Customize Query** to verify your settings and directory data.

   Since test lookups are conducted as real-time queries (as opposed to cached queries) Symantec recommends that you test with one of your smaller distribution lists.
4 Click **Test Query** to validate your address resolution query data using the test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot verify connectivity from attached scanners to your LDAP server.

If your query is successful, you can click the icon next to the **Test Query** option to display all query results. This test reports all email addresses and user preferences that are associated with the test email address. If the recipient is a distribution list, this information is provided for all users belonging to that distribution list.

Test results reflect only the data source being tested. The test does not provide information about the effects of other data sources or system settings such aliasing and masquerading.

5 If you want to examine or modify the default settings for your queries, click **Customize Query**. Create custom queries to more accurately reflect your system’s configuration.

See “Creating and testing a custom address resolution query” on page 527.

6 Click **Test Query** to validate your group listing query data using the test email address.

Test results reflect only the data source being tested. Test results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.

7 If you want to examine or modify the default settings for your group listing query, click **Customize Query**.

See “Creating and testing a custom address resolution query” on page 527.

8 You can configure your data source for multiple functions or click **Next** to review your changes and save your deployment.

See “Enabling functions on a new data source” on page 498.

---

**About using the authentication function with your data source**

An authentication data source provides end-user functions such as end-user preferences, end-user access to spam quarantine, and SMTP authentication.

See “About using the directory data service” on page 492.

When a data source is enabled for authentication, the system can do the following tasks:

- Enable and authenticate end-user access to Spam Quarantine.
  
  You must also configure at least one policy group to quarantine spam messages and configure quarantine settings and spam filtering.

  See “About selecting filtering policies for policy groups” on page 196.

  See “About quarantining spam” on page 280.

  See “About filtering email spam and unwanted messages” on page 248.
Let end users configure User Preferences, including personal good and bad sender lists and personal language settings (address resolution must also be enabled).

See "About using the address resolution function with your data source" on page 512.
See "Enabling and disabling end user settings for policy groups" on page 201.

Let authenticated end users remotely send email messages using the SMTP authentication protocol.

You must also set up SMTP authentication.

See "About using SMTP authentication" on page 103.

When authentication is enabled, quarantine address resolution is automatically enabled as well. This query obtains information from inbound messages and uses that information to resolve email aliases to a primary email address for recipients of quarantined messages. As a result, the user can access all of their quarantined messages regardless of which alias the message was originally sent to.

See "About quarantining spam" on page 280.

See "Creating an authentication data source" on page 502.

### About using the routing function with your data source

The routing function lets you configure per-user routing based on directory data. For example, you can use this function to route email messages addressed to users who have specified (as attributes associated with their own accounts) an alternate email address or mail host.

Each domain can be configured to route messages based on a directory data source, destination hosts, or MX lookup. This section talks about routing that uses a directory data source. For the other types of routing, consult the domain documentation.

See "Adding or editing domains" on page 82.

When a data source is enabled for directory-based routing, you can configure the directory data service to route email messages to alternate email addresses and mail hosts.

See "Creating a routing data source" on page 506.

If you configure both an **Alternate address attribute** and an **Alternate mailhost attribute**, the directory data service resolves all alternate email addresses first and then resolves the alternate mailhost. If an alternate address attribute is found, the data service attempts to assess the new address. If the address is local, the data service then attempts to find the new alternate address.

Once all local alternate addresses are resolved, the rules for that final address are then applied for purposes of alternate mail host routing.

The following is an example of what might happen if you send mail to a routing user who has both an alternate mailhost and an alternate address value:
1 Mail sent to this user resolves to the alternate address and is forwarded to the new address.

2 If the new address is local and that user also has an associated alternate address established, then mail is forwarded to that next address.

3 If the user associated with the last address only has an alternate mailhost value established, then the mail is delivered through the defined mailhost to the last email address.

**Note:** If an LDAP entry has multiple alternate mailhost attribute values, the MTA randomly chooses one of the values to use each time a message is delivered to that recipient. When an alternate email address attribute is supplied, mail that is bound for the original user is rerouted to the new email address. If there is more than one alternate address value provided, the message is rerouted to all of them.

To route messages to alternate addresses or mail hosts you must associate the desired domains with the routing data source.

See “Adding or editing domains” on page 82.

See “About email domains” on page 80.

See “Creating a routing data source” on page 506.

### About using the address resolution function with your data source

The address resolution function resolves alias and distribution list data to let you apply policies on a per-user basis. You accomplish this using LDAP-based group memberships to define policies.

Enabling a data source for address resolution offers the following benefits:

- The system can resolve directory group and distribution-list membership so that scanners can apply filter policies to policy groups. Please note that distribution list expansion must be enabled to apply policies to users in distribution lists.
  
  See “About selecting filtering policies for policy groups” on page 196.
  
  See “About expanding distribution lists and preserving recipient addresses” on page 532.

- The system can rewrite alias email addresses to primary email addresses to ensure that policies are applied consistently.

- You can let end users configure User Preferences, such as personal language settings and good and bad sender lists based on email address. Please note that authentication must also be enabled.
  
  See “About using the authentication function with your data source” on page 510.
  
  See “Enabling and disabling end user settings for policy groups” on page 201.
When address resolution is enabled an optional group listing query is enabled automatically. This function lets you more easily define policy group membership by selecting from a list of LDAP users and groups. When you configure the group listing query, the groups list in the Add Policy Groups page is populated with a list of all LDAP groups (including LDAP distribution lists) retrieved by the query. You may select groups from this list to add to policies or add groups by entering the LDAP group distinguished name yourself. If you have a large number of groups in your organization, you may want to disable this query when configuring your data source.

See “Creating an address resolution data source” on page 508.

About using the recipient validation function with your data source

Recipient validation determines whether your recipient addresses are valid. A valid address is an address that is found in at least one data source that is enabled for recipient validation. If a lookup address is valid and caching is enabled, the corresponding recipient entry is cached for later use (the cache is enabled by default). If a lookup address is not valid, it is cached in the invalid recipient cache.

Recipient validation works with other features within Symantec Messaging Gateway to help you identify and manage invalid recipients and messages that are sent to those recipients.

See “About using the directory data service” on page 492.

Enabling a data source for recipient validation offers the following benefits:

- Validate email recipients and reject connections or drop messages for invalid recipients. You must also properly configure invalid recipient handling to enable this behavior.
  See “Setting up invalid recipient handling” on page 99.

- Perform directory harvest attack recognition. You must also configure directory harvest attack recognition to enable this behavior.

- Capture invalid recipient email addresses for use as probe accounts by the Symantec Probe Network.
  See “About probe accounts” on page 314.

See “Creating a recipient validation data source” on page 500.

Once invalid recipient handling has been enabled to reject or drop messages to invalid recipients, that source cannot be deleted or disabled. To delete or disable such a data source, you must reconfigure invalid recipient handling to accept all messages.

Symantec Messaging Gateway supports redundant data sources only for the recipient validation function as there is no uniqueness requirement for email addresses or user names for this function.

See “Setting up invalid recipient handling” on page 99.
About data source queries

Symantec Messaging Gateway provides a default query for each function that is suitable for most common mail system configurations. Use the **Customize Query** option on the function pages to view and confirm those settings. If your LDAP schema requires unique queries you can create queries for any enabled function to change scope and support custom directory schemas.

First, you can use the **Base DN** field to set the scope of directory searches.

You provide the distinguished name (DN) for the subset of the directory you want to search. The smaller the subset of your directory, the more quickly the system can return data.

For example, the default query for your global company might be: `dc=company, dc=com`. If you need to limit searches to your New York office, you can set your base DN to limit the search to that sub-container in the directory. In this case your custom Base DN might be: `ou=NewYork, dc=company, dc=com`.

**Note:** The **Base DN** cannot be provided in this field for all directory types but is not applied to Domino or Active Directory Global Catalog queries.

In the **Query filter** field, you can define the rules the directory data service uses to search for entries in the directory. Use custom query filters that direct the directory data service to return data by using attributes and tokens to describe a specific LDAP query syntax.

The query filter is specified in standard LDAP query syntax. For example, `email=%s` describes a filter that finds all records with an attribute named "email" that matches the provided email address in it's entirety (as indicated by the %s query filter token).

At least one token is required for the **Query filter**. Table 19-7 describes the tokens that you can use to construct your query filters. The tokens you use are also dependent upon your directory type. Consult the documentation for your directory type for information about which of the following tokens your directory supports.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Instructs the directory data service to look for the following information when it retrieves an entry:</th>
<th>Returns entries with the following types of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>%s</td>
<td>Email address to find, including user ID and fully-qualified domain name.</td>
<td><a href="mailto:joe_smith@example.com">joe_smith@example.com</a></td>
</tr>
<tr>
<td>%u</td>
<td>Local portion of the email address to find.</td>
<td>joe_smith</td>
</tr>
<tr>
<td>%d</td>
<td>Domain portion of the email address to find.</td>
<td>example.com</td>
</tr>
</tbody>
</table>
Table 19-7  Query filter tokens supported by the Symantec Messaging Gateway (continued)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Instructs the directory data service to look for the following information when it retrieves an entry:</th>
<th>Returns entries with the following types of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>%n</td>
<td>Full name to find. Periods and underscores are replaced with space characters. Consecutive periods or underscores are replaced with a single space. This benefits quarantine address resolution by consolidating multiple versions of the same addresses into a single entry in the cache. This token is particularly useful if using Domino, since Domino can be configured to consider the FullName (cn) attribute as a deliverable email address.</td>
<td>joe smith</td>
</tr>
</tbody>
</table>

You can combine attributes with and without tokens to refine returned data. For example, if you use the query filter mail=%s with a recipient validation function and want to only return individual users (as opposed to distribution lists) you can use the following filter: 

```
(&(objectClass=person)(mail=%s)).
```

Table 19-8 describes the operators that you can use to construct you query filters.

Table 19-8  Query filter operators supported by Symantec Messaging Gateway

<table>
<thead>
<tr>
<th>Operator</th>
<th>Indicates the value is</th>
<th>Example</th>
<th>Data returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equal to</td>
<td>o=symantec</td>
<td>Entries for which the organization name is Symantec.</td>
</tr>
<tr>
<td>~=</td>
<td>Approximately equal to</td>
<td>(sn~=&lt;Johnson)</td>
<td>Entries with a name that is similar to &quot;Johnson&quot;. Looks for entries that resemble the name provided. For example, the directory server might return entries with the surnames &quot;Jonson&quot; and &quot;Johnsen&quot;. Rules for approximate matches vary based on directory type, and not all directory types support this operator. Consult your directory documentation for more information.</td>
</tr>
<tr>
<td>Operator</td>
<td>Indicates the value is</td>
<td>Example</td>
<td>Data returned</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------</td>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
<td>(st&lt;=ca)</td>
<td>Entries that occur before or at the location in the alphabet for the information provided. In this case the name &quot;ca&quot; and names appearing before &quot;ca&quot; in an alphabetical state attribute list, for example, &quot;ak&quot; can be returned.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to</td>
<td>(st&gt;=ca)</td>
<td>Entries that occur after or at the location in the alphabet for the information provided. In this case the name &quot;ca&quot; and names appearing after &quot;ca&quot; in an alphabetical state attribute list, for example, &quot;va&quot; can be returned.</td>
</tr>
<tr>
<td>&amp;</td>
<td>AND</td>
<td>(&amp;(o=symantec)(co=france))</td>
<td>Entries in which the organization name is Symantec and the country is France.</td>
</tr>
<tr>
<td>*=</td>
<td>Exists</td>
<td>(&amp;(mail=%s)(mailboxFile=*))</td>
<td>Entries that have a mail attribute that exactly matches the full recipient address, and have any mailboxFile attribute value to indicate that the user has an active email mailbox.</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td>((o=symantec)(sn=simpson) (cn=simpson))</td>
<td>Entries for the organization Symantec, the surname is Simpson, or the common name is Simpson.</td>
</tr>
<tr>
<td></td>
<td>NOT</td>
<td>(!((STREET=*))</td>
<td>Entries that do not contain a StreetAddress attribute. Note that when using the ! operator, you must use it outside of the parenthesis as follows: (!(&lt;filter&gt;)).</td>
</tr>
<tr>
<td></td>
<td>Wildcard</td>
<td>(o=<em>yma</em>)</td>
<td>Organization names that contain the string &quot;yma&quot;, such as &quot;Symantec&quot; as well as the exact string match &quot;yma&quot; if present.</td>
</tr>
</tbody>
</table>

Finally, you can customize attributes such as the **Primary email attribute** and object classes such as **Distribution list object classes** as necessary to meet your unique needs.
Be sure that the administrator credentials used to connect to the LDAP server has access to the attribute you provide. If the account does not have proper access, or if the provided attribute does not exist or is misspelled, the query results indicate that no data is associated with the attribute.

See “Creating a data source” on page 496.

See “Creating and testing a custom authentication and quarantine address resolution query” on page 518.

See “Creating and testing a custom recipient validation query” on page 517.

See “Creating and testing a custom routing query” on page 524.

See “Creating and testing a custom address resolution query” on page 527.

Creating and testing a custom recipient validation query

You can view your default query information or customize your queries by configuring custom attributes and filters to change query scope and support unique directory schemas.

See “About data source queries” on page 514.

Symantec recommends that you test all queries before deploying a new data source.

To configure a custom recipient validation query for a new data source:

1. Add your data source and configure your server integration settings in the Directory Integration Settings - LDAP Server Configuration page then click Next.

   See “Adding a data source” on page 496.

2. On the Add Directory Data Source - Directory Data Source Functions page, check Recipient validation, and then click Customize Query.

   See “Enabling functions on a new data source” on page 498.
3 Provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base DN</strong></td>
<td>Provide a Base DN for the query. A default value is provided, select &quot;Customize&quot; to provide your own values in the Custom query start field.</td>
</tr>
<tr>
<td><strong>Custom query start</strong></td>
<td>If you select &quot;Customize&quot; for the Base DN field, provide a Custom query start. You can customize the base DN to refocus the search to a specific part of the directory tree. Custom query start lets you configure the query to fit your particular needs and return data more quickly.</td>
</tr>
<tr>
<td><strong>Query filter</strong></td>
<td>Provide a Query filter for the query. The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.</td>
</tr>
<tr>
<td><strong>Restore Defaults</strong></td>
<td>Click Restore Defaults if you want to remove your edits to the recipient validation query configuration fields and replace them with the default values.</td>
</tr>
<tr>
<td><strong>Test email address</strong></td>
<td>Provide a Test email address that can be used to test and validate your recipient validation configuration. Symantec recommends that you test at least one valid and one invalid address.</td>
</tr>
<tr>
<td><strong>Test Query</strong></td>
<td>Click Test Query to validate the defined query using the provided test email address. This test is conducted against the directory data service instance that is running on the Control Center host. This test cannot be used to verify connectivity from attached scanners to your LDAP server. Test results reflect only the data source being tested. Test results and do not provide information about the effects of other data sources or system settings such as aliasing and masquerading.</td>
</tr>
</tbody>
</table>

4 Click **Save** to return to the Add Directory Data Source - Directory Data Source Functions page. See “Enabling functions on a new data source” on page 498.

Creating and testing a custom authentication and quarantine address resolution query

You can customize your queries by configuring custom attributes and filters to suit your system’s configuration. Use the custom query to change scope and support unique directory schemas. See “About data source queries” on page 514.
To customize the authentication query for a new data source

1. Add your data source and configure your server integration settings in the Directory Integration Settings - LDAP Server Configuration page then click Next.

   See “Adding a data source” on page 496.

2. On the Add Directory Data Source - Directory Data Source Functions page, check Authentication, select the type of authentication you want to use, and then click Customize Query.

   You can also click Customize Query to examine the default settings for your query.

   See “Enabling functions on a new data source” on page 498.

3. In the Authentication Type drop-down list, select the type of authentication you want to configure for your data source.

   Control Center authentication only: To authenticate end users for accessing quarantine or setting end-user preferences only.
   
   You must configure Control Center authentication and quarantine address resolution queries.

   SMTP authentication only: To enable remote users to use Symantec Messaging Gateway to send email using SMTP authentication.
   
   You must configure the SMTP authentication query.

   Control Center and SMTP authentication: To allow all of the capabilities of both Control Center and SMTP authentication.
   
   You must configure Control Center authentication, quarantine address resolution, and SMTP authentication queries. You can check Share Control Center and SMTP Authentication query details if you want to share your query details.

4. If you have selected Control Center and SMTP authentication you can check Share Control Center and SMTP Authentication query details if you want to use the Control Center authentication information as your SMTP authentication information.

5. Provide the following information for the Control Center authentication query if you selected Control Center authentication only or Control Center and SMTP authentication as the authentication type:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetBIOS domain name (optional)</td>
<td>Provide a list of NetBIOS domain names that the system can use to resolve login ambiguities. This field is optional but recommended if all of the following are true: ■ Your directory type is Active Directory or Active Directory Global Catalog ■ Your directory uses more than one NetBIOS domain ■ User name uniqueness is not guaranteed</td>
</tr>
<tr>
<td>Base DN</td>
<td>Provide a Base DN for the routing query. A default value is provided, if customize is selected, a custom query start can be provided in the Custom query start field.</td>
</tr>
<tr>
<td>Custom query start</td>
<td>If you select &quot;Customize&quot; for the Base DN field, provide a Custom query start.</td>
</tr>
<tr>
<td>Query filter</td>
<td>Modify the default Query filter for the authentication query, if desired. The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.</td>
</tr>
<tr>
<td>Primary email attribute</td>
<td>This field is not relevant to SMTP authentication but is required for Control Center authentication. Type the attribute in your LDAP schema that is used to store the primary email address information for the authentication query. If you specify a primary email attribute of &quot;proxyAddresses,&quot; the directory data service automatically identifies the attribute value that is prepended with &quot;SMTP&quot; as the address. You do not need to specify this prefix in the Primary email attribute field.</td>
</tr>
</tbody>
</table>
Choose your **Authentication Method**.

Click **Simple bind** to attempt login using the password provided by the user.

Or, you can use password fetching, which fetches the password from the data source and compares it to the password provided by the user. Click **Password attribute** to choose password fetching.

You can optionally specify a **Default hash type** for password fetching. If you choose **none**, your directory data must prepend the password attribute with a prefix indicating the scheme, such as `{PLAIN}`. If you choose **plaintext**, a scheme prefix is not needed.

Symantec Messaging Gateway supports SMTP authentication via LDAP using simple bind for all supported LDAP directory types. For SMTP authentication via LDAP using password fetching, all supported directory types except Active Directory, Active Directory Global Catalog, and Domino are supported.

**Test user name**

Type a user name that can be used to test and validate your authentication configuration.

Symantec recommends that you verify your settings using a variety of input intended to produce both successful authentication and unsuccessful authentication. If the test produces unexpected results, use **Customize Query** to verify your settings and directory data.

**Test password**

Type the password for the test user name.

**Restore Defaults**

Click **Restore Defaults** to restore the settings to the default settings.

**Test domain (optional)**

Type a NetBIOS domain for the provided test credentials.

You only need supply the test domain if you use Active Directory and the provided **Test user name** is domain-specific.

**Test Query**

Click to validate the defined quarantine address resolution query using the provided test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. It does not verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source tested. Results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.
6. Provide the following information for the quarantine address resolution query if you selected **Control Center authentication only** or **Control Center and SMTP authentication** as the authentication type:

**Query filter**
In the Query filter field under Quarantine Address Resolution Query, modify the default filter if desired. The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.

**Distribution list object classes**
In the Distribution list object classes field, type the object classes in your LDAP schema that should be used to identify distribution list entries.

**Restore Defaults**
Click Restore Defaults to restore the settings to the default settings.

**Test email address**
In the Test email address field, type an address that can be used to test and validate your quarantine address resolution configuration. Symantec recommends that you test your data source using a combination addresses including a user address, distribution list address, alias address, and an invalid address.

**Test Query**
Click Test Query to validate the defined quarantine address resolution query using the provided test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. It does not verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source being tested. Results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.
Provide the following information for the SMTP authentication query if you selected **SMTP authentication only** or **Control Center and SMTP authentication**.

If configuring both Control Center and SMTP authentication, you can check **Share Control Center and SMTP Authentication query details** to populate your SMTP details with those provided for the Control Center and skip this step.

- **Base DN**
  
  Provide a **Query start** for the routing query.
  
  A default value is provided, select "Customize" to provide your own values in the **Custom query start** field.

- **Custom query start**
  
  If you select "Customize" for the **Base DN** field, provide a **Custom query start**.
  
  You can customize the base DN to refocus the search to a specific part of the directory tree. This lets you configure the query to fit your particular needs and return data more quickly.

- **Query filter**
  
  Provide a **Query filter** for the SMTP authentication query, if desired.
  
  The login query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.

- **Primary email attribute**
  
  This field is not relevant to SMTP authentication. It is required for Control Center authentication.
  
  In the **Primary email attribute** field, type the attribute in your LDAP schema that is used to store the primary email address information for the SMTP authentication query.

- **Authentication Method**
  
  Choose your **Authentication Method**.
  
  Click **Simple bind** to attempt login using the password provided by the user.
  
  Or, you can use password fetching, which fetches the password from the data source and compares it to the password provided by the user. Click **Password attribute** to choose password fetching. You can use the default password attribute or change it.
  
  You can optionally specify a **Default hash type** for password fetching. If you choose **none**, your directory data must prepend the password attribute with a prefix indicating the scheme, such as `{PLAIN}`. If you choose plaintext, a scheme prefix is not needed.
  
  Symantec Messaging Gateway supports SMTP authentication via LDAP using simple bind for all supported LDAP directory types. For SMTP authentication via LDAP using password fetching, all supported directory types except Active Directory, Active Directory Global Catalog, and Domino are supported.
Creating and testing a custom routing query

You can customize your queries by configuring custom attributes and filters to suit your system's configuration. Use the custom query page to customize your routing query to change scope and support custom directory schemas. Depending on the directory type selected, your routing attribute names may not be prepopulated with defaults. If your attribute names are not populated you cannot save your routing query until you provide at least one attribute for your LDAP schema.

See “About data source queries” on page 514.

This section covers directory based routing. For information about the other routing methods of destination host routing or MX lookup, consult the domain documentation.

See “Adding or editing domains” on page 82.

Symantec recommends that you test all queries before deploying a new data source.
To configure a custom routing query for a new data source:

1. Add your data source and configure your server integration settings in the Directory Integration Settings - LDAP Server Configuration page then click Next. See “Adding a data source” on page 496.

2. In the Add Directory Data Source - Directory Data Source Functions page, check Routing, and then click Customize Query. See “Enabling functions on a new data source” on page 498.

3. Provide the following information:

   **Base DN** Provide a Base DN for the query. A default value is provided, or you can select "Customize" to provide your own values in the Custom query start field.

   **Custom query start** If you select "Customize" for the Base DN field, you must provide a Custom query start. You can customize the base DN to refocus the search to a specific part of the directory tree. The Custom query start lets you configure the query to fit your particular needs and return data more quickly.

   **Query filter** Provide a Query filter for the routing query, if desired. The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.

   **Alternate address attribute** If you want to enable per-user, directory-based, alternate-address routing, provide an Alternate address attribute. When an alternate email address attribute is supplied, mail bound for the original user is rerouted to the new email address. If there is more than one alternate address, the message is rerouted to all of them.

   **Note:** To save your routing source, you provide an Alternate address attribute, an Alternate mailhost attribute, or both. If you configure both an Alternate address attribute and an Alternate mailhost attribute, the directory data service resolves all alternate email addresses before it resolves the alternate mailhost.

   See “About using the routing function with your data source” on page 511.
Alternate mailhost attribute

If you want to enable directory-based alternate mail host routing, provide an **Alternate mailhost attribute** that corresponds to the attribute in the directory schema that you have selected to store this information.

The mail host should be specified as either an IP address or a fully qualified host name. A port can be specified by using a colon followed by the port, for example ":25". By default, the SMTP protocol uses port 25 for email transmission.

You can use the following valid attributes:

- 10.32.100.64
- 10.32.100.64:25
- myothermailserver.mycompany.com
- myothermailserver.mycompany.com:25

If an LDAP entry has multiple alternate mailhost attribute values, the MTA randomly selects one of the values to use each time a message is delivered to that recipient.

**Note:** To save your routing source, you provide an **Alternate address attribute**, an **Alternate mailhost attribute**, or both. If you configure both an **Alternate address attribute** and an **Alternate mailhost attribute**, the directory data service resolves all alternate email addresses before it resolves the alternate mailhost.

See “About using the routing function with your data source” on page 511.

Perform MX Lookup on alternate mailhost

Check **Perform MX Lookup on alternate mailhost** to allow MX lookup for the specified alternate mailhost. MX Lookup performs a directory lookup for the domain and returns the hosts responsible for accepting mail destined to that domain.

Restore Defaults

Click **Restore Defaults** if you want to remove your edits to the routing query configuration fields and replace them with the default values.

Test email address

Provide a **Test email address** that can be used to test and validate your routing configuration.
Test Query

Click **Test Query** to validate the defined routing query using the provided test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. It does not verify connectivity from attached scanners to your LDAP server. Test results reflect only the data source being tested. It does not provide information about the effects of other data sources or system settings such as aliasing and masquerading.

4. Click **Save** to return to the **Add Directory Data Source - Directory Data Source Functions** page.

See “Enabling functions on a new data source” on page 498.

Creating and testing a custom address resolution query

You can customize your queries by configuring custom attributes and filters to suit your system’s configuration. Use the custom query to change scope and support unique directory schemas.

See “About data source queries” on page 514.

Symantec recommends that you test all queries before deploying a new data source.

To configure a custom address resolution query for a new data source:

1. Add your data source and configure your server integration settings in the **Directory Integration Settings - LDAP Server Configuration** page then click **Next**.

   See “Adding a data source” on page 496.

2. In the **Add Directory Data Source - Directory Data Source Functions** page, check **Address resolution**, and then click **Customize Query**.

   See “Enabling functions on a new data source” on page 498.
3 Provide the following information:

**Base DN**
Provide a **Base DN** for the custom query.

A default value is provided, select "Customize" to provide your own values in the **Custom query start** field.

**Custom query start**
If you select "Customize" for the **Base DN** field, provide a **Custom query start**.

You can customize the base DN to refocus the search to a specific part of the directory tree. **Custom query start** lets you configure the query to fit your particular needs and return data more quickly.

**Primary email attribute**
Provide a **Primary email attribute** for the address resolution query, if desired.

The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.

**Primary email attribute**
In the **Primary email attribute** field, provide the attribute in your LDAP schema that is used to store the primary email address information for the query.

If you provide multiple primary email attributes, the system selects the first attribute (based on alphabetical order) to use as the primary attribute for query purposes. The subsequent values appear as aliases, but only if the primary attribute and alias attribute names defined for the data source function are the same.

If you specify a primary email attribute of "proxyAddresses", the directory data service automatically identifies the attribute value that is prepended with "SMTP:" as the address. You do not need to specify this prefix in the field.

**Email alias attribute (optional)**
In the **Email alias attribute** field, the attribute in your LDAP schema that is used to store the email alias address information.

**Distribution list object classes**
In the **Distribution list object classes** field, list the object classes in your LDAP schema to be used to identify distribution list entries.

**Child membership attributes**
In the **Child membership attributes** field, provide the names of the attributes, separated by semicolons, that are in your schema used to define members of a group.

If you do not provide a child membership attribute, distribution lists, and groups are not expanded. Choosing not to expand groups does create a performance benefit. It also means, however, that policies can only be applied to the email address of the recipient since LDAP group membership are not evaluated. Indirect policy groups through email aliases are still honored.
Click **Restore Defaults** to remove your edits to the address resolution query fields and replace them with the default values.

**Test email address**

Provide a **Test email address** that can be used to test and validate your query.

**Test Query**

To validate the defined address resolution query against the data source click **Test Query**.

This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot verify connectivity from attached scanners to your LDAP server.

If your query is successful, you can click the icon next to the **Test Query** option to display all query results. This test reports all email addresses and user preferences that are associated with the test email address. If the recipient is a distribution list, this information is provided for all users belonging to that distribution list.

Test results reflect only the data source being tested. Test results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.

**Query filter (optional)**

Provide a **Query filter (optional)** for the group listing query, if desired.

The attribute describes the email address or attribute element to be searched and the token describes the parameters that are used to return data.

For example, for a SunONE data source, you might use the following query filter to identify all groups within the directory:

```
(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames))
```

If this field is left blank, then groups are not listed on the Add Policy Groups page.

In the **Group name attribute (optional)** field, provide the attribute from your schema that is used as the display name for the groups that are returned. A representative sample of groups is returned.

If this field is left blank, then the groups created for association with policy groups are listed on the **Add Policy Groups** page by the DN name only.

See “**About policy groups**” on page 188.

**Restore Defaults**

Click **Restore Defaults** to remove your edits to the group listing query configuration fields and replace them with the default values.
Click **Test Query** to validate the defined group listing query against the data source instance that is running on the Control Center host.

Test results reflect only the data source tested. The query returns a representative sample of groups found in the directory and is conducted against the directory data service instance that is running on the Control Center host. It cannot be used to verify connectivity from attached scanners to your LDAP server.

**Distribution List Secondary Query Filter**

Applies a secondary filter for distribution lists.

This query filter is applied to the distribution lists that are obtained from the directory server as a result of distribution list expansion. The default value of \(\text{objectclass}=^*\) results in any distribution list that is a child member of a recipient distribution list that is included in the result set. This list occurs regardless of whether that distribution list would have been excluded by the primary query filter that you applied on the initial search.

**Note:** If you modify this value from the default with attributes that are not indexed by the directory server, it may result in performance degradation.

**Group Secondary Query Filter**

Applies a secondary filter to groups.

This query filter is applied to groups that are obtained from the directory server as a result of group membership expansion. The default value of \(\text{objectclass}=^*\) results in any group that is a child member of a group listed in a policy group membership that is included in the result set.

**Note:** If you modify this value from the default with attributes that are not indexed by the directory server, it may result in performance degradation.

4. Click **Save** to return to the Add Directory Data Source - Directory Data Source Functions page.

See “Enabling functions on a new data source” on page 498.
Managing Directory Data Integration

This chapter includes the following topics:
- Expanding distribution lists and preserving recipient addresses
- Modifying an existing data source
- Setting the directory data cache
- Configuring data source advanced settings
- Best practices for security
- Best practices for scalability
- Improving messaging and system load when using the directory data service
- Troubleshooting your LDAP connection

Expanding distribution lists and preserving recipient addresses

You can expand distribution lists to resolve addresses and apply filter policies to policy group members within distribution lists. You can preserve recipient address to stop the rewrite from alias to primary that occurs with address resolution and quarantine address resolution.

Table 20-1 describes how to expand distribution lists and preserve recipient addresses. You can perform these tasks as needed in any order.
Table 20-1 How to expand distribution lists and preserve recipient addresses

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Familiarize yourself with how to expand</td>
<td>Distribution list expansion lets you resolve addresses and apply filter policies to policy group members within distribution lists. Preserving recipient address stops the rewrite from alias to primary that occurs with address resolution and quarantine address resolution.</td>
</tr>
<tr>
<td>how to expand distribution lists and</td>
<td>See “About expanding distribution lists and preserving recipient addresses” on page 532.</td>
</tr>
<tr>
<td>preserve recipient addresses.</td>
<td></td>
</tr>
<tr>
<td>Enable or disable distribution list expansion.</td>
<td>Distribution list expansion lets the system use your LDAP directories to resolve addresses within distribution lists and apply filter policies to policy groups more consistently. This field is enabled by default. If you disable this feature, you cannot apply policies to individuals within distribution lists when distribution lists are used as members of policy groups. See “Enabling distribution list expansion for your data sources” on page 533.</td>
</tr>
<tr>
<td>Preserve recipient addresses.</td>
<td>Recipient address preservation retains addresses by stopping the system from rewriting addresses from alias to primary, as normally occurs when address resolution is enabled. Enabling this field affects your address resolution functionality by preventing this behavior. See “Preserving recipient addresses for your data sources” on page 534.</td>
</tr>
</tbody>
</table>

About expanding distribution lists and preserving recipient addresses

Enable distribution list expansion lets you resolve addresses and apply filter policies to policy group members within distribution lists. Preserve recipient addresses stops the rewrite from alias to primary that occurs with address resolution and quarantine address resolution. These settings are available on the Administration > Settings > Directory Integration > Directory Integration Settings page.

If Preserve recipient addresses and Enable distribution list expansion are both checked, the recipient alias address resolves to the primary addresses of distribution-list members except when the alias belongs to a single-member distribution list, in which case the alias address is preserved.

Note: Enable distribution list expansion applies to members within distribution lists, but not to the distribution list itself. To apply policy information to a distribution list and its individual members, you must add the distribution list alias as a member of its own distribution list.

See “Enabling distribution list expansion for your data sources” on page 533.
See “Preserving recipient addresses for your data sources” on page 534.
Table 20-2 describes resolution output based on the **Preserve recipient addresses** and **Expand distribution list** configuration combinations when address resolution is enabled.

**Table 20-2** Address resolution based on recipient address preservation and distribution list expansion input

<table>
<thead>
<tr>
<th>Input type</th>
<th>Preserve recipient addresses (disabled by default)</th>
<th>Expand distribution list (enabled by default)</th>
<th>The address resolves to</th>
</tr>
</thead>
<tbody>
<tr>
<td>user's alias address</td>
<td>disabled</td>
<td>enabled</td>
<td>user's primary address</td>
</tr>
<tr>
<td>distribution list alias address</td>
<td>disabled</td>
<td>enabled</td>
<td>full list of primary user addresses within the distribution list</td>
</tr>
<tr>
<td>user's alias address</td>
<td>disabled</td>
<td>disabled</td>
<td>user's primary address</td>
</tr>
<tr>
<td>distribution list alias address</td>
<td>disabled</td>
<td>disabled</td>
<td>distribution list primary address</td>
</tr>
<tr>
<td>user's alias address</td>
<td>enabled</td>
<td>enabled</td>
<td>user's alias address</td>
</tr>
<tr>
<td>distribution list alias address</td>
<td>enabled</td>
<td>enabled</td>
<td>distribution list alias</td>
</tr>
<tr>
<td>user's alias address</td>
<td>enabled</td>
<td>disabled</td>
<td>user's alias address</td>
</tr>
<tr>
<td>distribution list alias address</td>
<td>enabled</td>
<td>disabled</td>
<td>distribution list alias</td>
</tr>
<tr>
<td>distribution list primary address</td>
<td>enabled</td>
<td>enabled</td>
<td>distribution list primary address</td>
</tr>
</tbody>
</table>

**Enabling distribution list expansion for your data sources**

Distribution list expansion lets the system use your LDAP directories to resolve addresses within distribution lists and apply filter policies to policy groups more consistently.

This field is enabled by default. If you disable this feature, you cannot apply policies to individuals within distribution lists when distribution lists are used as members of policy groups.

If **Preserve recipient addresses** and **Enable distribution list expansion** are both checked, the features may affect each other and produce unintended consequences.

See “About expanding distribution lists and preserving recipient addresses” on page 532.

See “Editing the LDAP server configuration for a data source” on page 539.
To enable or disable distribution list expansion

1. Click Administration > Settings > Directory Integration.

2. On the Directory Integration Settings - Directory Data Sources page, check Enable distribution list expansion to enable distribution list expansion, or uncheck the box to disable distribution list expansion.

   You are prompted to Cancel or Change your distribution list expansion setting.

3. Click Change.

   Distribution list expansion is enabled or disabled across all data sources.

   See “About modifying existing data sources” on page 535.

Preserving recipient addresses for your data sources

Recipient address preservation retains addresses by stopping the system from rewriting addresses from alias to primary, as normally occurs when address resolution is enabled. Enabling this field affects your address resolution functionality by preventing this behavior.

If Preserve recipient addresses and Enable distribution list expansion are both checked, the features may affect each other and produce unintended consequences.

See “About expanding distribution lists and preserving recipient addresses” on page 532.

See “Enabling distribution list expansion for your data sources” on page 533.

To preserve recipient addresses for a data source

1. Click Administration > Settings > Directory Integration.

2. In the Directory Integration Settings - Directory Data Sources page, check Preserve recipient addresses. You are prompted to Cancel or Change your recipient address preservation setting.

3. Click Change.

   See “About modifying existing data sources” on page 535.

Modifying an existing data source

Table 20-3 describes the ways that you can modify an existing data source. You can perform these tasks as needed in any order.
Table 20-3  Modify an existing data source

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about the implications of changes to an existing data source.</td>
<td>Before you modify a saved data source, you should carefully assess any unintended effects that your changes may have on your mail configuration. See “About modifying existing data sources” on page 535.</td>
</tr>
<tr>
<td>Disable a saved data source to make a data source unavailable to the system without losing your configuration.</td>
<td>Disabling the data source saves configuration time if you need to enable the data source again at a later date. The disable feature is also useful if you need to temporarily take the source offline for troubleshooting purposes. Although settings are saved, the cache for a disabled data source is cleared and is rebuilt if enabled in the future. See “Disabling or enabling a data source” on page 538.</td>
</tr>
<tr>
<td>Delete an existing data source if you need to make the data source or directory information unavailable to Symantec Messaging Gateway.</td>
<td>Depending on your existing configuration, modifying a saved data source can affect or disable existing functionality. You also may be prevented from deleting some data sources based on such configuration. Be aware of any unintended consequences your actions may have on your mail configuration before you attempt to delete your data source. See “Deleting a data source” on page 538.</td>
</tr>
</tbody>
</table>
| Edit an existing data source. | Once you create a data source, you can modify certain aspects of the source configuration, functions, and queries. See “Editing a data source” on page 539. Part of editing your data source can include any of the following tasks:  
  - See “Editing the LDAP server configuration for a data source” on page 539.  
  - See “Enabling or editing the authentication function” on page 541.  
  - See “Enabling or editing the address resolution function” on page 548.  
  - See “Enabling or editing the routing function” on page 553.  
  - See “Enabling or editing the recipient validation function” on page 556.  
  - See “Editing advanced settings for a data source” on page 558. |

About modifying existing data sources

Once you create a data source, you can modify certain aspects of the source configuration, functions, and queries. Before you modify a saved data source, you should carefully assess any unintended effects that your changes may have on your mail configuration.

Editing a data source can affect your system configuration as follows:
When a data source is disabled or deleted, the cache for that data source is cleared. The cache is then discarded and repopulated if the data source is enabled or added again in the future.

If you change a query or any setting that alters query results while mail is being processed, the directory data service discards the existing cache, and a new one is built as the messages are received.

If you reconfigure your LDAP settings to use a different directory type, you query data is not updated and therefore may become outdated. You must reconfigure all queries. You can alternately use the **Restore Defaults** option for each enabled function to populate the correct defaults for each query based on the new directory type.

Modifying or attempting to modify a data source so that functions are no longer available can affect your system as follows:

### Table 20-4

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Authentication** | ■ Disabling an authentication data source automatically disables the authentication query.  
If this data source is configured for end-user quarantine, users are no longer able to log into the Control Center and access the end-user quarantine. The **End User Quarantine** field in the **Quarantine Settings** page is unchecked and cannot be edited unless a data source is made available. See “Configuring end user quarantine” on page 284.  
■ When an authentication source is deleted or disabled, quarantine address resolution no longer occurs for that source. Emails are no longer quarantined under a single account that is tied to a single address. See “Setting up invalid recipient handling” on page 99.  
■ When an SMTP authentication source is disabled or deleted, SMTP authentication no longer occurs for that source. Users who attempt to send out mail through a queue that requires SMTP authentication are no longer able to do so. |
| **Recipient validation** | ■ Deleting or disabling a recipient validation source prevents the data directory from applying invalid recipient handling. You must have at least one data source configured for recipient validation to drop or reject invalid recipients. If your system is configured to drop or reject, you are not able to delete the last recipient validation data source.  
See “Setting up invalid recipient handling” on page 99.  
■ Deleting or disabling all recipient validation sources affects the behavior of your directory harvest attack configuration. If there is not at least one recipient validation data source, directory harvest attack only acts upon non-local recipients, which are counted as invalid recipients for purposes of statistics. Directory harvest attack does not evaluate local messages since there is no directory data available for validation, and the system attempts to deliver all local messages normally. |
### Table 20-4 (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Address resolution    | ■ Deleting or disabling an address resolution source prevents the resolution of alias addresses to the primary address, as well as the expansion of distribution lists for entries within that source.  
                        | ■ Groups associated with a deleted or disabled data source are no longer available for selection in the Add Policy Groups page.  
                        | See “Creating a policy group” on page 190.                                                                                                      |
| Routing               | A routing data source cannot be deleted or disabled if an enabled domain is associated with the source. To modify or remove that data source you must first remove the domain associations using the Domains page.  
                        | See “Adding or editing domains” on page 82.                                                                                                      |

You can modify data sources as follows:

- You can change the LDAP information for a data source.  
  See “Editing the LDAP server configuration for a data source” on page 539.

- You can delete a data source.  
  See “Deleting a data source” on page 538.

- You can disable or enable a data source.  
  See “Disabling or enabling a data source” on page 538.

- You can modify your advanced settings data, such as enabling or disabling cache functionality, setting TTL or TTL spread, and configuring client settings.  
  See “Editing advanced settings for a data source” on page 558.

- You can disable, enable, or modify the Control Center authentication, quarantine address resolution function or SMTP authentication and related queries for a data source.  
  See “Enabling or editing the authentication function” on page 541.

- You can disable, enable, or modify the address resolution function and query for a data source.  
  See “Enabling or editing the address resolution function” on page 548.

- You can disable, enable, or modify the routing function and queries for a data source.  
  See “Enabling or editing the routing function” on page 553.

- You can disable, enable, or modify the recipient validation function and queries (including the group listing query) for a data source.  
  See “Enabling or editing the recipient validation function” on page 556.

- You can enable or disable distribution list expansion for a data source.  
  See “Enabling distribution list expansion for your data sources” on page 533.
You can enable or disable recipient address preservation for a data source. See “Preserving recipient addresses for your data sources” on page 534.

Disabling or enabling a data source

You can disable a saved data source to make a data source unavailable to the system without losing your configuration. Disabling the data source saves configuration time if you need to enable the data source again at a later date. The disable feature is also useful if you need to temporarily take the source offline for troubleshooting purposes. Although settings are saved, the cache for a disabled data source is cleared and is rebuilt if enabled in the future.

Depending on your system configuration, disabling a data source can affect the functionality of other features. Affected functionality can include invalid recipient handling, directory harvest attack, and end-user preferences. In the case of certain feature dependencies, the system does not let you disable a saved source.

See “About modifying existing data sources” on page 535.

To disable or enable a data source

1. Click Administration > Settings > Directory Integration.
2. In the Directory Integration Settings - Directory Data Sources page, check the boxes for the data sources you want to enable or disable.
3. Click Disable to disable the selected data sources, or Enable to enable the selected data sources.

Deleting a data source

You can delete an existing data source if you need to make the data source or directory information unavailable to Symantec Messaging Gateway.

Depending on your existing configuration, modifying a saved data source can affect or disable existing functionality. You also may be prevented from deleting some data sources based on such configuration. Be aware of any unintended consequences your actions may have on your mail configuration before you attempt to delete your data source.

See “About modifying existing data sources” on page 535.

To delete a data source

1. Click Administration > Settings > Directory Integration.
2. In the Directory Integration Settings - Directory Data Sources page and check the boxes for the data sources that you want to delete.
3. Click Delete.
Editing a data source

Depending on your system configuration, editing a data source can affect the functionality of other features.

In the case of certain feature dependencies, the system does not let you disable a saved source or some of the source's configured functions.

**Note:** If you disable a function for a data source, the settings and query configuration information for that function are not saved. Query settings must be reconfigured if the function is enabled at a later date.

See “About modifying existing data sources” on page 535.

**To edit a data source**

1. Click **Administration > Settings > Directory Integration**.
2. In the **Directory Integration Settings - Directory Data Sources** page, check that the data source you want to modify.
3. Click **Edit**.
4. Click one of the following tabs to edit your data source settings and configuration:
   - **LDAP server**
     See “Editing the LDAP server configuration for a data source” on page 539.
   - **Authentication**
     See “Enabling or editing the authentication function” on page 541.
   - **Recipient validation**
     See “Enabling or editing the recipient validation function” on page 556.
   - **Routing**
     See “Enabling or editing the routing function” on page 553.
   - **Address resolution**
     See “Enabling or editing the address resolution function” on page 548.
   - **Advanced**
     See “Editing advanced settings for a data source” on page 558.

**Editing the LDAP server configuration for a data source**

If the LDAP server configuration changes for an existing data source, you must update that information in Symantec Messaging Gateway.

Before you modify a deployed data source, be sure to first assess the impact your changes may have on any related configuration or processes.
Any modification that would affect query results cause the cache to be cleared and subsequently rebuilt, which can slow down mail delivery. Use the test functionality to help diagnose issues before the data source begins production service.

See “About modifying existing data sources” on page 535.

To edit LDAP server configuration for a data source

1. Click **Administration > Settings > Directory integration**.

2. In the **Directory Integration Settings - Directory Data Sources** page, check the box for the data source you want to edit.

3. Click **Edit** and then click the **LDAP Server** tab.

4. You can edit any of the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data source name</strong></td>
<td>You can edit the unique name of the data source.</td>
</tr>
<tr>
<td><strong>Directory type</strong></td>
<td>You can change the directory type the LDAP source uses. If you change the directory type for a saved data source, your query default values are not updated accordingly. You must individually reconfigure your queries or use the <strong>Restore Defaults</strong> option for each function.</td>
</tr>
<tr>
<td></td>
<td>The available choices are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Active Directory</td>
</tr>
<tr>
<td></td>
<td>■ Active Directory Global Catalog</td>
</tr>
<tr>
<td></td>
<td>■ iPlanet/Sun ONE/Java Directory Server</td>
</tr>
<tr>
<td></td>
<td>■ Domino</td>
</tr>
<tr>
<td></td>
<td>■ Other (can be any LDAPv3 compliant directory type)</td>
</tr>
<tr>
<td></td>
<td>Though Symantec Messaging Gateway is compatible with any LDAPv3 directory, it is specifically designed to support configurations using the four specific directory types listed. If you select &quot;other&quot; for your directory type, consult your directory documentation for more information.</td>
</tr>
<tr>
<td></td>
<td>If you use the Active Directory Global catalog, you may experience authentication issues depending on your query configuration. These issues can be resolved by replicating the Global Catalog.</td>
</tr>
<tr>
<td><strong>Host name</strong></td>
<td>Modify the host name or IP address of the LDAP server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Modify the TCP/IP port that is used to access the LDAP server.</td>
</tr>
<tr>
<td><strong>Enable SSL</strong></td>
<td>Enable or disable SSL on all connections to the LDAP server host. Verify your port setting when you modify this field.</td>
</tr>
<tr>
<td><strong>Anonymous bind</strong></td>
<td>Check to let the directory data service connect to the LDAP server without providing specific user ID and password information.</td>
</tr>
</tbody>
</table>
Check if you want to configure specific login credentials for authentication to the LDAP server.

**Name (Bind DN)**
The distinguished name (DN) that is used for authenticating to the LDAP server.

*Note:* For an Active Directory or Global Catalog server, you can optionally use the full DN, the NetBIOS and logon name (NetBIOS\SAM Account Name), or the User Principal Name.

**Password**
The password to be used for authenticating to the LDAP server. A password is required if you checked **Use the following**.

5 When you are finished editing the desired fields, click **Test Login** to connect to the client and ensure that your LDAP connection settings are valid.

This test only verifies that the LDAP server can be reached and that the provided account has read access to the root of the directory data tree on a directory server. A successful test result does not guarantee that the credentials can succeed elsewhere in the directory. This is particularly true for anonymous access. You should verify access before deployment.

6 Click **Save**.

### Enabling or editing the authentication function

You can customize your queries by configuring custom attributes and filters to suit your system's configuration. Use the custom query to change scope and support unique directory schemas.

See “About data source queries” on page 514.

Depending on your system configuration, editing an authentication data source can affect the functionality of other features. You may not be able to disable an authentication source if other features are dependent upon it.

See “About modifying existing data sources” on page 535.

Changing the authentication type for a data source can have the same effects as disabling it.

For example, assume that you configure end-user quarantine for a data source that is enabled for Control Center authentication. If you later enable the data source for "SMTP authentication only," end-user quarantine is automatically disabled because that functionality is dependent upon Control Center authentication. If, however, you enable the data source for "Control Center and SMTP authentication," you enable SMTP functionality and preserve all configuration that is based on Control Center authentication.

When a data source is enabled for authentication, the system can:

- Authenticate end-user login to Spam Quarantine.
Let end users configure personal Good and Bad Sender lists based on email address (address resolution also required).

Validate email recipients for messages that are stored in Spam Quarantine.

Let end users configure personal language settings (address resolution also required).

Authenticate users who use SMTP authentication to send messages.

See “About using the authentication function with your data source” on page 510.

See “About modifying existing data sources” on page 535.

See “About using SMTP authentication” on page 103.

**To edit authentication for a data source**

1. Click **Administration > Settings > Directory integration**.

2. In the **Directory Integration Settings - Directory Data Sources** page, check the data source that you want to edit.

3. Click **Edit**.

4. Click the **Authentication** tab.

5. Check **Enable Authentication** to enable authentication, or uncheck it to disable the data source for authentication.

When you remove a function from a data source by disabling the function for that source, the settings and query configuration information for that source are not saved and must be reconfigured.
In the drop-down list, select the type of authentication you want to configure for your data source.

**Note:** Editing from one exclusive authentication type to another authentication type can disable certain dependent features in your messaging system. If you are unsure as to how a change might affect your system, Symantec recommends that you select "Control Center and SMTP authentication" to preserve existing functionality.

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Center authentication only</td>
<td>To authenticate end users for accessing quarantine or setting end-user preferences only (authentication is also required). You must configure Control Center authentication and quarantine address resolution details.</td>
</tr>
<tr>
<td>SMTP authentication only</td>
<td>To enable remote users to send email without a VPN connection by using the SMTP authentication protocol. You must configure SMTP authentication details.</td>
</tr>
<tr>
<td>Control Center and SMTP authentication</td>
<td>To enable features for both Control Center and SMTP authentication. You must configure Control Center authentication, quarantine address resolution, and SMTP authentication details. You can check Share Control Center and SMTP Authentication query details if you want to share your query details.</td>
</tr>
</tbody>
</table>

If you have selected Control Center and SMTP authentication you can check Share Control Center and SMTP Authentication query details if you want to use the same query details for Control Center and SMTP authentication.

Provide the following information for the Control Center authentication query if you selected Control Center authentication only or Control Center and SMTP authentication (but did not check Share Control Center and SMTP Authentication query details) as the authentication type:

**Test user name**

Type a user name that can be used to test and validate your authentication configuration. Symantec recommends that you verify your settings using a variety of input designed to produce both successful results and unsuccessful results. If the test produces unexpected results, use Customize Query to verify your settings and directory data.

**Test password**

Type the password for the test user name.
Test domain (optional)  Type a NetBIOS domain for the provided test credentials. You can optionally specify a NetBIOS domain for the authentication query test. This field is required if your Test user name is not unique across multiple domains within the scope of your data source. This field is only available if you use Active Directory or Active Directory Global Catalog.

Test Query  Click to validate the quarantine address resolution query using the test information provided. This test is conducted against the directory data service instance that is running on the Control Center host. It does not verify connectivity from attached scanners to your LDAP server. Test results reflect only the data source tested. Results do not provide information about the effects of other data sources or system settings such as aliasing and masquerading.

Customize Query  Click to display the custom query fields. You can examine the default settings for your query or create a custom query to change scope and support custom directory schemas. See “About data source queries” on page 514.

NetBIOS domain names (optional)  Provide a list of NetBIOS domain names that the system can use to resolve login ambiguities. This field is optional but recommended if all of the following are true:

- Your directory type is Active Directory or Active Directory Global Catalog
- Your directory uses more than one NetBIOS domain
- User name uniqueness is not guaranteed

Base DN  Provide a Base DN for the routing query. A default value is provided, select "Customize" to provide your own values in the Custom query start field.

Custom query start  If you select "Customize" for the Base DN field, provide a Custom query start. You can customize the base DN to refocus the search to a specific part of the directory tree. Custom query start lets you configure the query to fit your particular needs and return data more quickly.
Provide a **Query filter** for the authentication query, if desired.

The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.

**Primary email attribute**

This field is not relevant to SMTP authentication. It is required for Control Center authentication.

In the **Primary email attribute** field, type the attribute in your LDAP schema that is used to store the primary email address information for the authentication query.

If you specify a primary email attribute of "proxyAddresses," the directory data service automatically identifies the attribute value that is prepended with "SMTP" as the address. There is no need to specify this prefix in the Primary email attribute field.

Choose your **Authentication Method**.

Click **Simple bind** to attempt login using the user-provided password.

Or, you can use password fetching, which fetches the password from the data source and compares it to the user-provided password. Click **Password attribute** to choose password fetching. You can use the default password attribute or change it.

You can optionally specify a **Default hash type** for password fetching. If you choose **none**, your directory data must prepend the password attribute with a prefix indicating the scheme, such as `{PLAIN}`. If you choose **plaintext**, a scheme prefix is not needed.

To disable password fetching, you can disable the cache for the authentication source. Or you can use **Simple bind** as your authentication method.

Symantec Messaging Gateway supports SMTP authentication through LDAP using simple bind for all supported LDAP directory types. For SMTP authentication through LDAP using password fetching, all supported directory types except Active Directory, Active Directory Global Catalog, and Domino are supported.

Click to hide the custom query fields.

Click to remove your edits to the query configuration fields and replace them with the default values.
9  Provide the following information for the quarantine address resolution query if you selected Control Center authentication only or Control Center and SMTP authentication as the authentication type. You can check Share Control Center and SMTP Authentication Query details to use your Control Center information:

**Test email address**  In the Test email address field, type an address that can be used to test and validate your quarantine address resolution configuration. Symantec recommends that you test your data source using a combination addresses including a user address, distribution list address, alias address, and an invalid address.

**Test Query**  Click Test Query to validate the quarantine address resolution query using the provided test email address.

This test is conducted against the directory data service instance that is running on the Control Center host. It cannot be used to verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source tested. This test does not provide information about the effects of other data sources or system settings such aliasing and masquerading.

**Customize Query**  Click to display the custom query fields. You can view the default query or customize the query to change scope and support custom directory schemas.

See “About data source queries” on page 514.

**Query filter**  In the Query filter field under Quarantine Address Resolution Query, type a custom filter for the quarantine address resolution query, if desired. The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.

**Distribution list object classes**  In the Distribution list object classes field, type the object classes in your LDAP schema that should be used to identify distribution list entries.

**Hide Query**  Click to hide the custom query fields.

**Restore Defaults**  Click to remove your edits to the query configuration fields and replace them with the default values.
10 Provide the following information for the SMTP authentication query if you selected **SMTP authentication only** or **Control Center and SMTP authentication** as the authentication type:

**Test user name**
Type a user name that can be used to test and validate your authentication configuration.

Symantec recommends that you verify your settings using a variety of input designed to produce both successful results and unsuccessful results. If the test produces unexpected results, use **Customize Query** to verify your settings and directory data.

**Test password**
Type the password for the test user name.

**Test Query**
Click to validate the quarantine address resolution query using the test information provided.

This test is conducted against the directory data service instance that is running on the Control Center host. It does not verify connectivity from attached scanners to your LDAP server.

Test results reflect only the data source tested. It does not provide information about the effects of other data sources or system settings such aliasing and masquerading.

**Customize Query**
Click to display the custom query fields. Create a custom query to change scope and support custom directory schemas.

See “About data source queries” on page 514.

**Base DN**
Provide a **Base DN** for the routing query.

A default value is provided, select "Customize" to provide your own values in the **Custom query start** field.

**Custom query start**
If you select "Customize" for the **Base DN** field, provide a **Custom query start**.

You can customize the base DN to refocus the search to a specific part of the directory tree. **Custom query start** lets you configure the query to fit your particular needs and return data more quickly.

**Query filter**
Provide a **Query filter** for the authentication query, if desired.

The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.
Primary email attribute (optional)

This field is not relevant to SMTP authentication. It is required for Control Center authentication.

In the **Primary email attribute** field, type the attribute in your LDAP schema that is used to store the primary email address information for the authentication query.

Authentication Method

Choose your **Authentication Method**.

Click **Simple bind** to attempt login using the user-provided password.

Or, you can use password fetching, which fetches the password from the data source and compares it to the user-provided password. Click **Password attribute** to choose password fetching. You can use the default password attribute or change it.

You can optionally specify a **Default hash type** for password fetching. If you choose **none**, your directory data must prepend the password attribute with a prefix indicating the scheme, such as `{PLAIN}`. If you choose **plaintext**, a scheme prefix is not needed.

To disable password fetching, you can disable the cache for the authentication source. Or you can use **Simple bind** as your authentication method.

Symantec Messaging Gateway supports SMTP authentication through LDAP using simple bind for all supported LDAP directory types. For SMTP authentication through LDAP using password fetching, all supported directory types except Active Directory, Active Directory Global Catalog, and Domino are supported.

Hide Query

Click to hide the custom query fields.

Restore Defaults

Click to remove your edits to the query configuration fields and replace them with the default values.

11 Click Save.

Enabling or editing the address resolution function

You can customize your queries by configuring custom attributes and filters to suit your system's configuration. Use the custom query to change scope and support unique directory schemas.

See “About data source queries” on page 514.

Depending on your system configuration, editing or disabling the address resolution function for a saved data source can affect the functionality of other features.

See “About modifying existing data sources” on page 535.
To edit address resolution configuration for a data source

1. Click Administration > Settings > Directory integration.
2. In the Directory Integration Settings - Directory Data Sources page, check the boxes for the data source that you want to edit.
3. Click Edit.
4. Click the Address resolution tab.
You can edit any of the following fields:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Source Name</td>
<td>You can edit the unique name of the data source.</td>
</tr>
<tr>
<td>Enable Address Resolution</td>
<td>The address resolution function resolves alias and distribution list data to let you apply policies on a per-user basis by using LDAP based group memberships to define policies.</td>
</tr>
<tr>
<td></td>
<td>See &quot;About using the address resolution function with your data source&quot; on page 512.</td>
</tr>
<tr>
<td></td>
<td>If you remove a function from a data source by disabling the function for that source, settings and query configuration information for that source are not saved. This information must be reconfigured if the function is enabled in the future.</td>
</tr>
<tr>
<td></td>
<td>See “About modifying existing data sources” on page 535.</td>
</tr>
<tr>
<td>Test email address</td>
<td>Provide an email address that can be used to test and validate your address resolution configuration.</td>
</tr>
<tr>
<td>Test Query</td>
<td>Click to test and validate the defined address resolution query using the provided test email address.</td>
</tr>
<tr>
<td></td>
<td>This test reports all email addresses, distribution list memberships, and directory group memberships that are associated with the test email address. This test is conducted against the directory data service instance that is running on the Control Center host. It cannot be used to verify connectivity from attached scanners to your LDAP server.</td>
</tr>
<tr>
<td></td>
<td>If your query is successful, you can click the icon next to the Test Query option to display all query results. This test reports all email addresses and user preferences that are associated with the test email address. If the recipient is a distribution list, this information is provided for all users associated with that distribution list.</td>
</tr>
<tr>
<td></td>
<td>Test results reflect only the data source being tested. It does not provide information about the effects of other data sources or system settings such aliasing and masquerading.</td>
</tr>
<tr>
<td>Customize Query</td>
<td>Click to view or customize the default address resolution query. Create a custom query to change scope and support custom directory schemas.</td>
</tr>
<tr>
<td></td>
<td>See “About data source queries” on page 514.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Base DN</strong></td>
<td>Specify the name for the place in the directory from which to start searching for entries to authenticate.</td>
</tr>
<tr>
<td></td>
<td>A default value is provided, select &quot;Customize&quot; to provide your own values in the <strong>Custom query start</strong> field.</td>
</tr>
<tr>
<td><strong>Custom query start</strong></td>
<td>If you select &quot;Customize&quot; for the <strong>Base DN</strong> field, provide a <strong>Custom query start</strong>. You can customize the base DN to refocus the search to a specific part of the directory tree. <strong>Custom query start</strong> lets you configure the query to fit your particular needs and return data more quickly.</td>
</tr>
<tr>
<td><strong>Query filter</strong></td>
<td>The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.</td>
</tr>
<tr>
<td><strong>Primary email attribute</strong></td>
<td>Specify the attribute in your LDAP schema that is used to store the primary email address information.</td>
</tr>
<tr>
<td></td>
<td>If you specify a primary email attribute of &quot;proxyAddresses,&quot; the directory data service automatically identifies the attribute value that is prepended with &quot;SMTP&quot; as the address. You do not need to specify this prefix in the <strong>Primary email attribute</strong> field.</td>
</tr>
<tr>
<td><strong>Email alias attribute (optional)</strong></td>
<td>Specify the attribute in your LDAP schema that is used to store the email alias address information.</td>
</tr>
<tr>
<td><strong>Distribution list object classes</strong></td>
<td>List the object classes in your LDAP schema to be used to identify distribution list entries.</td>
</tr>
<tr>
<td><strong>Child membership attributes</strong></td>
<td>Provide the names of the attribute in your schema, separated by semicolons, that are used to define members of a group.</td>
</tr>
<tr>
<td></td>
<td>If you do not provide a child membership attribute, distribution lists and groups are not expanded. This can create a performance benefit. It also means, however, that policies can only be applied to the email address of the recipient since LDAP group membership are not evaluated. Indirect policy groups through email aliases are still honored.</td>
</tr>
</tbody>
</table>

**Hide Query** Click to hide the custom query fields.

**Restore Defaults** Click to remove your edits to the query configuration fields and replace them with the default values.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Query</strong></td>
<td>Click to test and validate the group listing query using the provided test information. This test is conducted against the directory data service instance that is running on the Control Center host. It does not verify connectivity from attached scanners to your LDAP server. Test results reflect only the data source tested.</td>
</tr>
<tr>
<td><strong>Customize Query</strong></td>
<td>Click to create a custom group listing query. Create a custom query to change scope and support custom directory schemas. See “About data source queries” on page 514.</td>
</tr>
</tbody>
</table>
| **Query filter** (optional) | The query filter defines the rules the directory data service uses to search for groups in the directory. It is specified in standard LDAP query syntax. For example, for a SunONE data source, you might use the following query filter to identify all groups within the directory: 

\[
(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames))
\]

If this field is left blank, then groups are not listed on the Add Policy Groups page. See “About policy groups” on page 188.                                                                 |
| **Group name attribute** (optional) | Specify the attribute in your schema that is used as the display name for the groups that are returned. See “About policy groups” on page 188.                                                               |
| **Hide Query**              | Click to hide the custom query fields.                                                                                                                                                                       |
| **Restore Defaults**        | Click to remove your edits to the query configuration fields and replace them with the default values.                                                                                                            |
| **Distribution List**       | Applies a secondary filter for distribution lists. This query filter is applied to the distribution lists that are obtained from the directory server as a result of distribution list expansion. The default value of \(\text{objectclass}^*=\) results in any distribution list that is a child member of a recipient distribution list that is included in the result set. This list occurs regardless of whether that distribution list would have been excluded by the primary query filter that you applied on the initial search. **Note:** If you modify this value from the default with attributes that are not indexed by the directory server, it may result in performance degradation. |
Enabling or editing the routing function

You can customize your queries by configuring custom attributes and filters to suit your system's configuration. Use the custom query to change scope and support unique directory schemas.

See “About data source queries” on page 514.

Depending on your system configuration, editing the routing function for a saved data source can affect the functionality of other features.

See “About modifying existing data sources” on page 535.

To edit the routing function for a data source

1 Click Administration > Settings > Directory Integration.
2 In the Directory Integration Settings - Directory Data Sources page, check the boxes for the data source you want to edit.
3 Click Edit.
4 Click the Routing tab.
5 You can edit any of the following fields:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data source name</td>
<td>You can edit the unique name of the data source.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Enable Routing</strong></td>
<td>The routing function uses the information provided by your data source to route messages to addresses and domains. See “About using the routing function with your data source” on page 511. You cannot delete a routing source that has been associated with a domain. If you want to disable such a routing source, you must remove the association on the <strong>Domains</strong> page. When you remove a function from a data source by disabling the function for that source, the settings and query configuration information for that source are not saved. This information will need to be reconfigured if the function is enabled in the future. See “About modifying existing data sources” on page 535.</td>
</tr>
<tr>
<td><strong>Test email address</strong></td>
<td>Provide an email address that can be used to test and validate your routing configuration.</td>
</tr>
<tr>
<td><strong>Test Query</strong></td>
<td>Click to test and validate the defined routing query using the provided test email address. This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot be used to verify connectivity from attached scanners to your LDAP server. Test results reflect only the data source tested. Test results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.</td>
</tr>
<tr>
<td><strong>Customize Query</strong></td>
<td>Click to expose the custom query fields. Create a custom query to change scope and support custom directory schemas. See “About data source queries” on page 514.</td>
</tr>
<tr>
<td><strong>Base DN</strong></td>
<td>Specify the name for the place in the directory from which to start searching for entries to authenticate. A default value is provided, select &quot;Customize&quot; to provide your own values in the <strong>Custom query start</strong> field.</td>
</tr>
<tr>
<td><strong>Custom query start</strong></td>
<td>If you select &quot;Customize&quot; for the <strong>Base DN</strong> field, provide a <strong>Custom query start</strong>. You can customize the base DN to refocus the search to a specific part of the directory tree. <strong>Custom query start</strong> lets you configure the query to fit your particular needs and return data more quickly.</td>
</tr>
<tr>
<td><strong>Query filter</strong></td>
<td>The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Alternate address attribute | If you want to enable per-user, directory-based alternate address routing, provide an **Alternate address attribute**. When an alternate email address attribute is supplied, mail bound for the original user is rerouted to the new email address.  
**Note:** To save your routing source, you provide an **Alternate address attribute**, an **Alternate mailhost attribute**, or both. If you configure both an **Alternate address attribute** and an **Alternate mailhost attribute**, the directory data service resolves all alternate email addresses before it resolves the alternate mailhost values.  
See “About using the routing function with your data source” on page 511.                                                                  |
| Alternate mailhost attribute | If you want to enable directory-based alternate mail host routing, provide an **Alternate mailhost attribute** that corresponds to the attribute in the directory schema that you have selected to store this information.  
The mail host should be specified as either an IP address or a fully qualified host name. A port can be specified by using a colon followed by the port, for example ":25". By default, the SMTP protocol uses port 25 for email transmission.  
You can use the following valid attributes:  
■ 10.32.100.64  
■ 10.32.100.64:25  
■ myothermailserver.mycompany.com  
■ myothermailserver.mycompany.com:25  
If an LDAP entry has multiple alternate mailhost attribute values, the MTA randomly selects one of the values to use each time a message is delivered to that recipient.  
**Note:** To save your routing source, you provide an **Alternate address attribute**, an **Alternate mailhost attribute**, or both. If you configure both an **Alternate address attribute** and an **Alternate mailhost attribute**, the directory data service resolves all alternate email addresses before it resolves the alternate mailhost values.  
See “About using the routing function with your data source” on page 511.                                                                  |
| Perform MX Lookup on alternate mailhost       | Allows MX lookup for the specified alternate mailhost.                                                                                                                                                           |
| Hide Query                  | Click to hide the custom query fields.                                                                                                                                                                         |
### Enabling or editing the recipient validation function

You can customize your queries by configuring custom attributes and filters to suit your system’s configuration. Use the custom query to change scope and support unique directory schemas.

See “About data source queries” on page 514.

Depending on your system configuration, editing the recipient validation function for a saved data source can affect the functionality of other features.

See “About modifying existing data sources” on page 535.

#### To edit the recipient validation function for a data source

1. In the Control Center, click **Administration > Settings > Directory Integration**.
2. In the **Directory Integration Settings - Directory Data Sources** page, check the box for the data source you want to edit.
3. Click **Edit**.
4. Click the **Recipient Validation** tab.
5. To enable recipient validation on your data source, check **Enable Recipient Validation**.
You can edit any of the following fields:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data source name</strong></td>
<td>You can edit the unique name of the data source.</td>
</tr>
<tr>
<td><strong>Enable Recipient Validation</strong></td>
<td>Check <strong>Enable Recipient Validation</strong>. Recipient validation works with other features within Symantec Messaging Gateway to help you identify and manage invalid recipients and messages sent to those recipients. See “About using the recipient validation function with your data source” on page 513. You cannot disable or delete the last recipient validation source if you have configured invalid recipient handling to drop messages or reject invalid recipients. You must set invalid recipient handling to accept all messages to delete or disable the last recipient validation source. When you remove a function from a data source by disabling the function for that source, the settings and query configuration information for that source are not saved. This information must be reconfigured if the function is enabled in the future. See “About modifying existing data sources” on page 535.</td>
</tr>
<tr>
<td><strong>Test email address</strong></td>
<td>Enter an email address that can be used to test and validate your recipient validation configuration.</td>
</tr>
<tr>
<td><strong>Test Query</strong></td>
<td>Click to test and validate the defined recipient validation query using the provided test email address.</td>
</tr>
<tr>
<td></td>
<td>This test is conducted against the directory data service instance that is running on the Control Center host. The test cannot be used to verify connectivity from attached scanners to your LDAP server. Test results reflect only the data source tested. Test results do not provide information about the effects of other data sources or system settings such aliasing and masquerading.</td>
</tr>
<tr>
<td><strong>Customize Query</strong></td>
<td>Click to expose the custom query fields. You can review the default query information or create a custom recipient validation query to change scope and support custom directory schemas. See “About data source queries” on page 514.</td>
</tr>
</tbody>
</table>
Item | Description
--- | ---
**Base DN** | Specify the name for the place in the directory from which to start searching for entries to authenticate. A default value is provided, select "Customize" to provide your own values in the **Custom query start** field.
**Custom query start** | If you select "Customize" for the **Base DN** field, provide a **Custom query start**.
You can customize the base DN to refocus the search to a specific part of the directory tree. **Custom query start** lets you configure the query to fit your particular needs and return data more quickly.
**Query filter** | The query filter instructs the directory data service to return data using attributes and tokens that describe a specific LDAP query syntax.
**Hide Query** | Click to hide the custom query fields.
**Restore Defaults** | Click to remove your edits to the query configuration fields and replace them with the default values.

7 Click **Save**.

**Editing advanced settings for a data source**

Use caution when editing your settings on a deployed data source, as changes may affect your current configuration and processes. For example, modifying cache settings may clear the cache, while modifying referral chasing may stop referrals from working.

See "About the directory data cache" on page 562.

See “About modifying existing data sources” on page 535.

To edit advanced settings for a data source

1 Click **Administration > Settings > Directory Integration**.

2 In the **Directory Integration Settings - Directory Data Sources** page, check the boxes for the data source that you want to edit.

3 Click **Edit**.

4 Click the **Advanced Settings** tab.
5 You can edit any of the following fields:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum connections</td>
<td>Specify the maximum number of client connections (bind operations) that can be created at one time.</td>
</tr>
<tr>
<td></td>
<td>If this field is set to zero, connection pooling is turned off and a new connection is created for each request.</td>
</tr>
<tr>
<td>Minimum connections</td>
<td>Specify the number of connections that are added to the connection pool when the source services the first request.</td>
</tr>
<tr>
<td></td>
<td>A value of zero indicates that connections are created only to service actual pending requests. Connections are released if they are idle for longer than the specified idle timeout.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Specify the amount of time that should elapse before an attempt to connect to the LDAP server host is timed out and automatically ended.</td>
</tr>
<tr>
<td></td>
<td>A value of zero indicates that the connection can never time out on the client side (the LDAP server can still close the connection).</td>
</tr>
<tr>
<td>Idle timeout</td>
<td>Specify how long a client connection can remain idle before the connection is automatically closed.</td>
</tr>
<tr>
<td></td>
<td>A value of zero indicates that the connection can remain idle indefinitely without being closed (though the LDAP server can also close the connection).</td>
</tr>
<tr>
<td>Search timeout</td>
<td>Specify how long (in seconds) a request/search operation should run before the directory data service ends the operation and displays the partial results. The directory server can impose a search timeout lower than this value.</td>
</tr>
<tr>
<td></td>
<td>Setting this value too low can impede performance. A page size higher than the limit set by the LDAP server can cause the operation to fail when the page size exceeds that limit. The default server-side limit for this value varies according to directory type. To change this limit on your directory server, see your directory server documentation.</td>
</tr>
<tr>
<td></td>
<td>To disable paged searching entirely, set this value to 0.</td>
</tr>
<tr>
<td>Page size</td>
<td>Determine the maximum number of initial entries to return when a query is successful.</td>
</tr>
<tr>
<td></td>
<td>Setting this value too low can impede performance. A page size higher than the limit set by the LDAP server can cause the operation to fail when the page size exceeds that limit. The default server-side limit for this value varies according to directory type. To change this limit on your directory server, see your directory server documentation.</td>
</tr>
<tr>
<td></td>
<td>To disable paged searching entirely, set this value to 0.</td>
</tr>
</tbody>
</table>

**Note:** Make sure that the Name (bind DN) configured for the Administration Credentials used by the LDAP source has sufficient access rights to bypass search limits.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chase referrals</td>
<td>A server may return a query response that suggests that the directory data service query another LDAP server. When this field is enabled, the directory data service follows such referrals when it executes queries. The directory data service uses the same bind credentials to connect to the referred server. If the referred-to LDAP server does not recognize the same bind credentials, a query can return an error.</td>
</tr>
<tr>
<td>Enable cache</td>
<td>The cache stores address entry data from previous requests. This allows the directory data service to process requests faster by using this cached data instead of consulting the LDAP server. The cache is enabled by default.</td>
</tr>
<tr>
<td>Cache size</td>
<td>Specify the maximum number of entries that can be stored in the cache. When the cache size limit is exceeded, the least recently used entry is deleted to make room for a new entry. You should set the cache size based on your system's needs and memory availability. Symantec recommends that you set this value equal to or greater than the number of users and groups (including distribution lists, contacts, and public folders) in your environment. If you set the cache to zero entries, each new invalid recipient is trimmed as it is added to the cache. This results in a total size of 0 at any given time. See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td>Cache index size multiplier</td>
<td>Specify the size of the email address index in relation to the cache. This setting allows the index to store multiple aliases for each entry in the cache. For example, a multiplier of two would be twice the size of the cache and allow for an average of two aliases per cache entry.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Minimum cache TTL</td>
<td>Set the minimum Time to Live (TTL) for entries in the cache. When a cache TTL is reached, the entries in that cache expire and are refreshed upon query. A minimum value and maximum value for cache expiration creates a period of time over which these entries can be expired and refreshed. This helps pace your system's workload. For address resolution sources, this setting also determines how often the membership information is rebuilt for LDAP groups used in policies. See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td>Maximum cache TTL</td>
<td>Set the maximum Time to Live (TTL) for entries in the cache. When a cache TTL is reached, the entries in that cache expire and are refreshed upon query. A minimum value and maximum value for cache expiration creates a period of time over which these entries can be expired and refreshed. This helps pace your system's workload. See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td>Invalid recipient cache size</td>
<td>Provide the maximum number of entries that can be stored in the invalid recipient cache. When the directory data service cannot find an entry in the directory, the entry is considered invalid and is added to the invalid recipient cache. When the entry is queried in the future, load time is reduced because the directory data service checks the cache before it queries the directories. You should set the cache size based on your system's needs and memory availability. If you set the cache to 0, each new invalid recipient is trimmed as it is added to the cache, resulting in a total of 0 at any given time.</td>
</tr>
<tr>
<td>Invalid recipient cache TTL</td>
<td>Period of time an email address entry should be kept in the invalid recipient cache.</td>
</tr>
<tr>
<td>Clear Cache</td>
<td>Click to clear the cache of all entries.</td>
</tr>
<tr>
<td>Restore Defaults</td>
<td>Click to restore the default values to all Advanced Settings fields.</td>
</tr>
</tbody>
</table>

Click Save.
Setting the directory data cache

You can configure an appropriate directory data cache size based on your system's needs and memory availability. You can also preload your directory data cache and enable cache persistence.

Table 20-5 describes the ways that you can set your directory data cache. You can perform these tasks as needed in any order.

Table 20-5  Set the directory data cache

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about the directory data cache.</td>
<td>Symantec Messaging Gateway provides caching functionality that stores directory data from previous requests. This lets the directory data service process requests faster by using this cached data instead of the more time-consuming LDAP directory query. See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td>Enable cache persistence.</td>
<td>Cache persistence saves the existing cache to a file any time the directory data service is stopped as a result of the Symantec Messaging Gateway being shut down or rebooted. This cache can then be read at reboot to prevent the loss of cache data. The cache is enabled by default. See “Enabling cache persistence” on page 563.</td>
</tr>
<tr>
<td>Learn more about the benefits of preloading your directory data cache.</td>
<td>If you have a large number of LDAP entries or a slow LDAP connection, you can preload your directory caches to prevent mail from backing up in the system during the initial directory cache building process. Under most circumstances, cache preload is not necessary because the caches can be built gradually during the normal course of operation with satisfactory system performance. See “About preloading your directory data cache” on page 564.</td>
</tr>
<tr>
<td>Preload your data cache.</td>
<td>Caches are built gradually during the normal course of operation with satisfactory system performance. If your system configuration is complex or your data sources are large, you can preload your directory caches to prevent mail from backing up in the system during the initial directory cache building process. See “Preloading your data cache” on page 564.</td>
</tr>
</tbody>
</table>

About the directory data cache

Symantec Messaging Gateway provides caching functionality that stores directory data from previous requests. This lets the directory data service process requests faster by using this cached data instead of the more time-consuming LDAP directory query.

The cache is enabled by default and entries are added to the cache as they are received and validated. When the directory data service receives a request, it searches all caches until the
recipient is found or there are no more caches to search. If the recipient is not found in a cache, the directory data service then searches the data source directories. If the recipient is found in a data source, it adds the recipient to the associated cache.

If the recipient is not found in a data source then the directory data service adds a cache entry to the invalid recipient cache for that data source.

Configure an appropriate cache size based on your system's needs and memory availability. Symantec recommends that you set this value equal to or greater than the number of users and groups in your environment. This list should include distribution lists, contacts, and public folders.

You can control aspects of each of your caches as follows:

■ Set the cache size and entry life span using the Advanced Settings page.
  See “Editing advanced settings for a data source” on page 558.
  Use the Minimum TTL (Time to Live) and Maximum TTL settings on the Advanced Settings page to find the right balance of refresh frequency versus data freshness.

■ Set alerts to notify you when your cache size has been exceeded.
  See “Configuring alerts” on page 688.

■ If your directory is very large or if you have a slow LDAP connection, you can preload your cache to avoid a backup in your mail queues caused by the cache building process.
  See “About preloading your directory data cache” on page 564.

■ Disable your cache. Note that if the cache is disabled, then the LDAP host is queried for each request. Disabling the cache can increase processing time.
  See “Editing advanced settings for a data source” on page 558.

Enabling cache persistence

Cache persistence saves the existing cache to a file any time the directory data service is stopped as a result of the Symantec Messaging Gateway being shut down or rebooted. This cache can then be read at reboot to prevent the loss of cache data. The cache is enabled by default.

See “About the directory data cache” on page 562.
To enable or disable cache persistence for a data source

1. Click **Administration > Settings > Directory Integration**.

2. On the **Directory Integration Settings - Directory Data Sources** page, check **Enable cache persistence** to enable cache persistence, or uncheck the box to disable cache persistence.

   You are prompted to **Cancel** or **Change** your distribution list expansion setting.

3. Click **Change**.

   Cache persistence is enabled or disabled across all data sources.

   See “About modifying existing data sources” on page 535.

### About preloading your directory data cache

If you have a large number of LDAP entries or a slow LDAP connection, you can preload your directory caches to prevent mail from backing up in the system during the initial directory cache building process. Under most circumstances, cache preload is not necessary because the caches can be built gradually during the normal course of operation with satisfactory system performance.

Cache preload is performed on a per-function basis and is supported for the following functions:

- Quarantine address resolution
- Recipient validation
- Routing
- Address resolution

For all functions except routing, a single input file populates all data sources that are enabled for that function. For routing, a separate input file is required to populate each data source.

If you disable a data source, the cache for all enabled functions for that data source is cleared. If you create a new data source or enable a disabled data source you must preload the caches again.

See “Preloading your data cache” on page 564.

See “About the directory data cache” on page 562.

### Preloading your data cache

Caches are built gradually during the normal course of operation with satisfactory system performance. If your system configuration is complex or your data sources are large, you can preload your directory caches to prevent mail from backing up in the system during the initial directory cache building process.
You must upload all your input files before you begin the preloading process. Each import file must be comprised of newline-separated email addresses and use ASCII or UTF8 encoding.

To preload a data source cache

1. Select Administration > Settings > Directory Integration.
2. Click Preload Cache.
3. On the Preload Configuration and Status page, browse to the Input file you want to use to preload your cache.
   This file must be comprised of newline-separated email addresses using either ASCII or UTF format.
4. In the Function field, select the function for which the uploaded file is used.
   Cache preload is performed in a per-function basis and is supported for the following enabled and configured functions: quarantine address resolution, recipient validation, routing, and address resolution. For all functions except routing, a single input file is shared across all data sources that are enabled for that function. For routing, you must associate your data source input file or files with each routing function.
5. Click Upload.
6. Continue to upload your files until you have uploaded all of the files you want to preload. You must upload the data source file for each function. If the list of email addresses is shared across functions, you must upload the same input file for each function.
7. When you have uploaded all the files, click Start Preload.
   You can return to this page at anytime to check your status until the Control Center restarts. The Preload % Complete column shows updates for each function as the page is refreshed automatically. You can also manually refresh the status by clicking Refresh.

The preload status appears as follows:

- **In progress**
  - The preloading process has begun but is not yet completed.

- **Successfully completed**
  - All files have been successfully loaded.

- **Cancel initiated**
  - Cancel was initiated but not completed.

- **Canceled**
  - The file loading process has been stopped.

- **Failed**
  - The file load process was unsuccessful.
You can return at anytime to check your status until the Control Center restarts. You can also consult the Control Center logs for additional information.

See “About logs” on page 614.

### Configuring data source advanced settings

In addition to setting up your LDAP server in the Configure LDAP Server page, you can further adjust your cache size and network settings in the Advanced Settings fields.

See “About the directory data cache” on page 562.

To configure advanced settings for a data source

1. Add your data source on the Directory Integration Settings - Directory Data Sources page then click Next.

   See “Adding a data source” on page 496.

2. On the LDAP Server Configuration page, configure your server integration settings then click Show Advanced Settings.
You can configure any of the following settings for your new data source. All fields are optional and only need to be configured if your system has special requirements.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum connections</td>
<td>Specify the maximum number of client connections (bind operations) that can be created at one time. If this field is set to zero, connection pooling is turned off and a new connection is created for each request.</td>
</tr>
<tr>
<td>Minimum connections</td>
<td>Specify the number of connections that are added to the connection pool when the source services the first request. A value of zero indicates that connections are created only to service actual pending requests. Created connections are released if they are idle for longer than the specified idle timeout.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Specify the amount of time that should elapse before an attempt to connect to the LDAP server host is timed out and automatically ended. A value of zero indicates that the connection should never be timed out (though the LDAP server can also close the connection).</td>
</tr>
<tr>
<td>Idle timeout</td>
<td>Specify how long a client connection can remain idle before the connection is automatically closed. A value of zero indicates that the connection can remain idle indefinitely without being closed (though the LDAP server can also close the connection).</td>
</tr>
<tr>
<td>Search timeout</td>
<td>Specify how long (in seconds) a request /search operation should run before the directory data service ends the operation and displays the partial results. Please note that the LDAP server can impose a search timeout lower than this value.</td>
</tr>
<tr>
<td>Page size</td>
<td>Determine the maximum number of initial entries to return when a query is successful. Setting this value too low can impede performance. A page size higher than the limit set by the LDAP server can cause the operation to fail when the page size exceeds that limit. The default server-side limit for this value varies according to directory type. To change this limit on your directory server, see your directory server documentation. To disable paged searching entirely, set this value to 0.</td>
</tr>
</tbody>
</table>

**Note:** Make sure that the Administration Credentials you provide have sufficient access rights to bypass search limits.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chase referrals</td>
<td>When a request is processed, a server may return a query response that suggests that the directory data service query another LDAP server. When this field is enabled, the directory data service follows such referrals when it executes queries.</td>
</tr>
<tr>
<td></td>
<td>The directory data service uses the same bind credentials to connect to the referred to server. If the referred-to LDAP server does not recognize the same bind credentials, a query can return an error.</td>
</tr>
<tr>
<td>Enable cache</td>
<td>The cache stores address entry data from previous requests. The cache lets the directory data service process requests faster by using this cached data instead of consulting the LDAP server directly for each lookup.</td>
</tr>
<tr>
<td></td>
<td>See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td></td>
<td>The cache is enabled by default.</td>
</tr>
<tr>
<td>Cache size</td>
<td>Specify the maximum number of entries that can be stored in the cache. When the cache size limit is exceeded, the least recently used entry is deleted to make room for a new entry.</td>
</tr>
<tr>
<td></td>
<td>You should set the cache size based on your system’s needs and memory availability. Symantec recommends that you set this value equal to or greater than the number of users and groups (including distribution lists, contacts, and public folders) in your environment.</td>
</tr>
<tr>
<td></td>
<td>If you set the cache to zero entries, the cache is effectively disabled.</td>
</tr>
<tr>
<td>Cache index size multiplier</td>
<td>Specify the size of the email address index in relation to the cache. This setting allows the index to store multiple aliases for each entry in the cache. For example, a multiplier of 2 would be twice the size of the cache and allow for an average of two aliases per cache entry.</td>
</tr>
<tr>
<td></td>
<td>Symantec recommends that you set this value equal to or greater than the average number of primary and alias addresses that are associated with your users.</td>
</tr>
<tr>
<td>Minimum cache TTL</td>
<td>Set the minimum Time to Live (TTL) for entries in the cache.</td>
</tr>
<tr>
<td></td>
<td>When a cache TTL is reached, the entries in that cache expire and are refreshed upon query. A minimum value and maximum value for cache expiration creates a period of time over which these entries can be expired and refreshed. This helps pace your system’s workload by ensuring that all entries do not expire at the same time.</td>
</tr>
<tr>
<td></td>
<td>For address resolution sources, this setting also determines how often the membership information is rebuilt for LDAP groups used in policies.</td>
</tr>
<tr>
<td></td>
<td>See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Maximum cache TTL</strong></td>
<td>Set the maximum Time to Live (TTL) for entries in the cache.</td>
</tr>
<tr>
<td></td>
<td>When a cache TTL is reached, the entries in that cache expire and are refreshed upon query. A minimum value and maximum value for cache expiration creates a period of time over which these entries can be expired and refreshed. This helps pace your system's workload by ensuring that all entries do not expire at the same time.</td>
</tr>
<tr>
<td></td>
<td>See “About the directory data cache” on page 562.</td>
</tr>
<tr>
<td><strong>Invalid recipient cache size</strong></td>
<td>Provide the maximum number of entries that can be stored in the invalid recipient cache.</td>
</tr>
<tr>
<td></td>
<td>When the directory data service cannot find an entry in the directory, the entry is considered invalid and is added to the invalid recipient cache. When the entry is queried in the future, load time is reduced because the directory data service checks the cache before it queries the directories.</td>
</tr>
<tr>
<td></td>
<td>You should set the cache size based on your system's needs and memory availability. If you set the cache to 0 the cache is effectively disabled.</td>
</tr>
<tr>
<td><strong>Invalid recipient cache TTL</strong></td>
<td>Provide the period of time an email address entry should be kept in the invalid recipient cache.</td>
</tr>
</tbody>
</table>

4. To undo your changes, click **Restore Defaults**. The original default values are restored to all Advanced Settings fields.

5. To hide these fields on the LDAP Server Configuration page, click **Hide Advanced Settings**.

6. When you are finished, click **Next** to configure the functions for the data source. See “Enabling functions on a new data source” on page 498.

**Best practices for security**

When integrating the directory data service, it is very important to take appropriate precautions to safeguard your directory systems and data.

Symantec recommends that you implement some or all of the following to increase security for your deployment:

- Enable secure socket layer functionality by checking the SSL checkbox when setting up your LDAP server configuration.
SSL can be used alone or can be used to augment password hashing to provide an additional layer of protection. Symantec recommends that you use SSL for your data sources whenever possible, and very strongly recommends it for authentication sources. You enable SSL when you set up or edit your data source’s server configuration. See “Adding a data source” on page 496.

Additionally, you must make sure that your directory servers are configured for SSL. See your directory administrator or directory documentation for more information.

■ Use password hash algorithms to protect the passwords that are stored in your directory server.

Although hash algorithms provide some additional protection, used alone they do not provide adequate security for user password data and should not be used as a substitute for SSL. SSL is essential for authentication sources to protect user name and password data in transit.

■ Use an account that is restricted to read-only access for your directory data source administrator credentials.

If possible, avoid anonymous bind for such accounts. See “Adding a data source” on page 496.

See “Editing the LDAP server configuration for a data source” on page 539.

■ Limit access to your server by using minimal access rights.

Restrict access to namespaces, object classes, or entry attributes of interest. For example, in addition to configuring the Bind DN for a data source to have read-only access, the access control for the directory should only grant read access to the objectClass and the attributes used for email addresses, mailhosts, and group membership. You can find these attribute names by looking at the custom query information for your existing source. See “Enabling or editing the authentication function” on page 541.

For directory-specific recommendations, consult your directory documentation.

■ If your appliance has two NICs, you can place one on an internal subnet and configure the system only that one for your LDAP traffic.

This isolates your LDAP servers and directory data from potential exposure to the Internet. See “Modifying Scanner configurations” on page 67.

Best practices for scalability

If using the directory data service in a large or distributed environment, consider the following best practices to improve system performance and scalability:

■ Use directory data service caching functionality to improve throughput and reduce the load on your directory servers.

You should set the cache size based on your system’s needs and memory availability. Symantec recommends that you set this value equal to or greater than the number of users.
and groups in your environment. This number should include distribution lists, contacts, 
public folders, and any other LDAP entry that lists a deliverable email address or a 
username.
See “Configuring data source advanced settings” on page 566.
See “Editing advanced settings for a data source” on page 558.

- Use alert settings to manage your processes and cache.
  The **Monitor swap space utilization** alert triggers when swapping exceeds the specified 
  utilization. Use the swap alert to make sure that your systems have adequate RAM for all 
  Symantec Messaging Gateway processes, including the directory data service cache.
  The default value to trigger this alert is 60% and can be modified to suit your needs. For 
  high performance deployments that are adequately provisioned with memory, there should 
  be little or no swap space utilization. Symantec recommends setting the swap space alert 
  threshold to only a few percent for such deployments.
  The **Undersized data source cache** alert lets you know immediately when you need to 
  increase the cache size to support your data.
  See “Configuring alerts” on page 688.

- Use the Symantec Messaging Gateway directory cache preloader to complete the cache 
  building process before directing your production mailflow to the system.
  For most deployments, caches can be built gradually through normal system activity with 
  adequate system performance and preloading the cache is not necessary. For some 
  deployments with very large directories or slow LDAP connections, however, the preloader 
  can be used to avoid temporary performance problems that may occur while a very large 
  cache is built.
  Perform this task offline (for example, during a maintenance window) as the preloaded 
  caches are not available to your Scanners until the process is complete.
  See “About preloading your directory data cache” on page 564.

- Use the **Minimum TTL** (Time to Live) and **Maximum TTL** settings on the Advanced 
  Settings page to find the right balance of cache refresh frequency versus data freshness.
  Adequate spread smooths out the load on your LDAP servers by randomizing the expiration 
  of cache entries. Refreshes that occur too frequently can increase processing time, but 
  failing to refresh often enough results in stale data. Work with your directory administrator 
  to determine the right refresh rate for your system.
  See “About the directory data cache” on page 562.
  See “Configuring data source advanced settings” on page 566.
  See “Editing advanced settings for a data source” on page 558.

- Improve Symantec Messaging Gateway system performance by turning off distribution list 
  expansion.
  Disabling **Distribution list expansion** can significantly increase mail delivery throughput. 
  If **Distribution list expansion** is disabled, however, distribution lists are not resolved into 
  their individual members for policy evaluation.
This means that mail sent to a distribution list is subject only to the policies associated with the distribution list itself (either through an email address or a distinguished name). The policies associated with its individual members are not applied, even if they have higher precedence.

See "Enabling distribution list expansion for your data sources" on page 533.

Limit the number and size of LDAP groups and distribution lists associated with your policy groups.

If you clear a data source cache or make a configuration change to your policy groups or a directory data source, the Symantec Messaging Gateway must reload group information from your directory. This can result in the growth of your inbound or outbound message queues.

For most deployments this process takes only a few seconds and results in an insignificant queue backup if any at all. However, in cases where LDAP access is slow, or the policy groups references many thousands of LDAP users, a noticeable backup can occur. For best performance, Symantec recommends that you use the default group to implement the most common behavior and then assign specific policies to smaller groups as necessary.

See "Creating a policy group" on page 190.

To improve performance for queries, restrict the Base DN for your LDAP queries to cover only the data that is needed for your data source.

The larger the scope of the query, the longer the searches take. Poor query performance for quarantine address resolution can lead to a backup in your delivery queues. Poor query performance for address resolution can cause inbound or outbound queues to back up.

See "About data source queries" on page 514.

If your data source uses the Active Directory Global Catalog, be sure to configure the directory data service to use the global catalog port (default 3268) instead of the domain controller port (default 389).

See "Adding a data source" on page 496.

Create read-only copies of firewalled LDAP servers and place them outside of the firewall to improve connection time.

In an environment where Scanners hosts are located outside the firewall and LDAP servers reside inside the firewall, you can speed up connection and query times by setting up replicas of those LDAP servers outside the firewall and near the Scanners in the network. Figure 20-1 provides an example of a firewalled server configuration and how you might use an LDAP server replica to improve processing time.

Your directory administrator can determine the best path for this action based on your system configuration.
Improving messaging and system load when using the directory data service

Depending on your configuration, you may need to take additional steps to ensure optimal messaging or load balancing. Consider the following configuration options if you are trying to resolve load or messaging issues.

- **Create duplicates of LDAP servers that are behind firewalls for easier client access.**
  If your configuration uses an LDAP client that resides behind a firewall, you can resolve connection issues by setting up a replica of their LDAP server, close to where the scanners are located in the network. Your directory administrator should determine the best path for this action based on your configuration.

- **Turn off distribution list expansion to speed up query time.**
  You can improve performance by disabling distribution list expansion. If you use this option, distribution lists cannot be evaluated for individual members and can only be managed as a single entity.

- **Use child membership attributes to speed up query time.**
  Providing parent attributes in queries allows the client to immediately determine what groups the child belongs to and avoids a query to the directory.
  Active Directory provides the ability to use these attributes by default. More customizable directories, such as SunOne or OpenLDAP can be expanded to carry the parent and child membership attributes. Consult your directory provider’s documentation for more information.

- **Use caching and the cache preloader to save query time.**
  To optimize performance, create a cache that incorporates all of your entries, including your distribution list members, all primary users, and all aliases, then estimate up if possible.
Troubleshooting your LDAP connection

User authentication and message processing can be affected when your directory data service cannot properly communicate with an LDAP server. For example, the network link to the LDAP server may be down or a data integrity problem may prevent authentication or address resolution. The effect on message processing varies, based on which directory data service function is affected.

You may need to contact your system administrator for assistance, or you can attempt the following strategies through your directory data service configuration.

- Use a network load balancer between the Symantec Messaging Gateway hosts and the LDAP directory to distribute requests between replicas of the directory data. This can improve performance and provide for failover if one of the servers becomes unavailable.
- If you do not use a network load balancer, the directory data service rotates the connections in a round-robin fashion among the IP addresses that you assigned to your LDAP server.
- Ensure that your data source cache size and time-to-live (TTL) values are appropriate for your deployment. If the directory data service cannot contact an LDAP server, that cached result could be useful, even if the TTL of the cached entry has expired.

See “Editing advanced settings for a data source” on page 558.

**Note:** If Symantec Messaging Gateway encounters 10 data source access errors over a period of 60 seconds, then the directory data source is marked as unavailable for 300 seconds. All requests are served from the cache during that time. This action reduces the impact on message delivery when requests to a faltering LDAP server host produce long network timeouts.
Reports

This chapter includes the following topics:

- Reports overview
- Select data to track for reports
- Retain, delete, and purge report data
- Specify report export settings
- Create, save, email, and print a report
- Copy, edit, schedule, and delete favorite reports
- Schedule reports to generate automatically
- Report types
- Troubleshooting report generation
- Generated reports layout and data

Reports overview

SMG comes with 10 predefined reports that are known as report types. When you create a new report, you choose a report type to get started. You can configure SMG to store additional data to add to your reports. The data that is included in each report type is described in See “Report types” on page 582..

You configure reports in two places in the Control Center.

- Under the Administration tab, Settings -> Reports you can:
  - Select additional sets of data to track. See “Select data to track for reports” on page 576.
Select data to track for reports

This section describes how to configure SMG to track and store data to add to basic reports. You must configure SMG 24 hours in advance to track and store the added data. Extended statistics such as Top Senders, Top Sender Domains, and Invalid Recipient data are only collected when you select the appropriate options.

To select data to track for reports

1. In the Control Center, click the Administration>Settings > Reports.
2. Under Email Reports Data, check the box beside the report data that you want to track. You can select more than one.
   - To track extended statistics, select all of the Sender-related boxes.
   - To view the Top Probe Accounts report, select Recipients, and then enable Invalid Recipients.
3. Sender statistics usually use a large amount of disk space. Choose an appropriate length of time to store report data.
   See “Retain, delete, and purge report data ” on page 577.
4. Click Save.
Once you select the data to track, you can view the reports for that data after 24 hours.

See “Create, save, email, and print a report” on page 578.

Retain, delete, and purge report data

By default, report and dashboard data are retained for 7 days. When SMG has 7 days of data, the oldest hour of data is deleted as each new hour of data is stored. You may want to modify how long SMG retains report data.

Expunging data is resource-intensive, so you may want to configure the Expunger to run at off hours. Report data that is purged cannot be retrieved.

You can check the status of your scheduled task from the Status > Scheduled Tasks page.

You must have full administration rights or rights to view or modify report settings.

To specify how long report data is retained
1. In the Control Center, click Administration > Settings > Reports.
2. Under Report and Dashboard Expunger Settings, click the Delete data older than drop-down list to select how long SMG keeps your report data.
3. Click Save.

To delete all report data at one time
1. In the Control Center, click Administration > Settings > Reports.
2. Beside Delete all reporting and dashboard data now, click Delete Data Now to remove all report data that is stored to date.
3. In the confirmation dialog box, click OK.

To specify when and how often report data is purged
1. In the Control Center, click Administration > Settings > Reports.
2. Under Report and Dashboard Expunger Settings, in the Run Expunger drop-down list, select the Expunger frequency.
3. Click the Start Expunger at drop-down lists, and specify the Expunger start time. The hour drop-down list uses a 24 hour clock. The default setting is 3:00 A.M.
4. Click Save.
Specify report export settings

You can set a default sender email address, and customize the default subject line for reports you send by email from SMG. The default sender email address that you specify must be a valid email address for your domain.

When you install SMG, the default email address is ReportAdmin@yourcompany.com. Users cannot reply to the default sender email address.

The default subject line for reports consists of the title of the report and the report range date. You can specify a custom subject line using a combination of static text and variables.

The default report subject lines are as follows:

Report by hour or day

%TITLE% ({MMMM d, yyyy hh:mm a} to {MMMM d, yyyy hh:mm a zz})

For example:


Report by week or month

%TITLE% ({MMMM d, yyyy} to {MMMM d, yyyy zz})

For example:

MonthlyReport (December 1, 2008 to January 1, 2009 PST)

You must have full administration rights or rights to view or modify report settings.

To specify the report email notification sender and subject line

1 In the Control Center, click Administration > Settings > Reports.

2 In the Email send from box, type the email address that you want to appear on the report notification email as the sender.

3 If you want to apply a custom subject line for the report email, check Apply custom subject and filename format.

   If unchecked, default text is used for the subject line.

4 Modify the subject, as needed.

5 Click Save.

Create, save, email, and print a report

This section describes how to create and configure a report, customize filters, and how to save your report to the Favorite Reports page.
You can add specific data sets such as Top Senders, Top Sender Domains, and Invalid Recipients, to the default data in a report. You must configure SMG 24 hours in advance to track and store the added statistics. See “Select data to track for reports” on page 576.

You must have full administration rights to create, view, or modify reports.

To create and generate a report

1. In the Control Center, go to Reports > View > Create a Report.
2. In the Report type drop-down list, select a report category.
3. In the drop-down list next to the Report type field, select a specific report.
   This step does not apply to the Executive Summary report.
   If you participate in the Symantec Probe Network, and want to see a Top Probe Accounts report, select Invalid Recipients > Top Probe Accounts.
   For the Spam and Unwanted Mail Report type, you can also select a Spam disposition if you select any of the following values: Top Sender Domains, Top Senders, Top Sender Helo Domains, Top Sender IP Connections, Top Recipient Domains, Top Recipients, Specific Senders or Specific recipients.
4. If the report type you choose filters on specific elements, a new field with the name of that specific element appears. Enter the criteria for that element.
   For reports that are filtered by Sender name, you can use the null sender address <> to filter for messages that do not contain Sender names.
5. Some reports let you select from the following drop-down lists:
   - Direction
   - Time range Note: You must enable JavaScript in your browser to use the pop-up calendar.
   - Group By
   - For reports that rank results, in the Entries box, type the maximum number for each time range that is specified in the Group by drop-down.
   - Display as Graph, Table or both
   - Columns to display in the report
   - Character Set
6. To save the report to your Favorite Report page, enter a report name and then click Save to Favorites.
7. To generate the report, click Run.
When you generate a report, it appears in a new browser window. From there, you can save the report in HTML, CSV or PDF format, and email it to multiple recipients. Separate multiple email addresses with a comma, semi-colon, or space.

To print a report, right click in the Report browser window and select Print.

Copy, edit, schedule, and delete favorite reports

This section describes how to edit, copy, delete, and generate your Favorite Reports.

You must have full administration rights or rights to view or modify reports to delete a favorite report.

To copy favorite reports

1. In the Control Center, click Reports > View > Favorite Reports.
2. In the Report Name column, check the box beside the report that you want to copy.
3. Click Copy.
4. Click on the underlined name of the new, copied report.
5. Change the values in the report as necessary.
6. Click Save.

When you copy a report, the name of the new report is: Copy of <original report name>. Specify a unique name for the new report to help you remember the scope of the report.

To edit the filter options in a favorite report

1. In the Control Center, click Reports > View > Favorite Reports.
2. Click on the underlined name of a report in the list.
3. Change the values in the report as necessary.
4. Click Save.

To edit the schedule for a favorite report to run

1. In the Control Center, click Reports > View > Favorite Reports.
2. Check the box beside the report that you want to edit, and then click View Schedule.
3. Make any changes to the settings.
4. Click Save.
To delete favorite reports

1. In the Control Center, click **Reports > View > Favorite Reports**.
2. Check the box beside the report that you want to delete.
3. Click **Delete**.

   When you delete a report, the report configuration cannot be retrieved.

Schedule reports to generate automatically

You can schedule a favorite report to run automatically at specified intervals. Scheduled reports cannot be automatically saved to the host computer. They must be emailed to at least one recipient.

You can check the status of your scheduled task from the **Status > Scheduled Tasks** page.

You must have full administration rights or rights to view or modify reports, and to create automatically generated reports.

To schedule a report to generate automatically

1. In the Control Center, click **Reports > View > Favorite Reports**.
2. Check the box beside the report that you want to schedule and click **View Schedule**.

   To cancel a scheduled report, check the box beside the report that you no longer want scheduled, and then click **Clear Schedule**.
3. Under the **Schedule** tab set the time of day to generate the report.
4. Under the **Export** tab, specify the format for the report.
5. Under the **Export** tab, enter sender and recipient email addresses. Separate multiple recipient email addresses with a space, comma, or semi-colon.
6. In the **Character Set** drop-down list, select a character set appropriate for the recipient of the email message.
7. Click **Save**.
To run reports on demand

1. Create a report.
   See “Create, save, email, and print a report” on page 578.

2. Click **Run**.
   The report appears in a separate browser window.

   **Note:** If a "Pop-up blocked" message appears in the Control Center, click the message and permit pop-ups from SMG Control Center.

To run scheduled reports on demand

1. In the Control Center, click **Reports > View > Favorite Reports**.

2. In the **Report Name** column, check the box besides the report that you want to run.

3. Click **Run**.
   The report appears in a separate browser window.

   **Note:** If a "Pop-up blocked" message appears in the Control Center, click the message and permit pop-ups from SMG Control Center.

---

### Report types

SMG comes with 10 predefined reports that are known as report types. When you create a new report, you choose a report type to get started. The tables in this section describe what information is in each report type. The last column in each table lists the type of data you want the system to track. You must specify one or more options before you can generate that report.

See “Select data to track for reports” on page 576.

See “Generated reports layout and data” on page 597.

<table>
<thead>
<tr>
<th>Table 21-1</th>
<th>Summary reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Executive</td>
<td>Overview of your security profile, which includes total messages and threats processed, and malware and content filtering summaries.</td>
</tr>
</tbody>
</table>
Table 21-1  Summary reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content filtering</td>
<td>Overview of the content filtering violations and trends affecting your organization. Includes the number of policies triggered, and percentage of policies triggered versus total processed messages.</td>
<td>None</td>
</tr>
<tr>
<td>Email Messages</td>
<td>Overview of email message threat counts and types of threats.</td>
<td>None</td>
</tr>
<tr>
<td>Invalid Recipients</td>
<td>Overview of invalid recipient data.</td>
<td>None</td>
</tr>
<tr>
<td>IP Connections</td>
<td>Overview of the IP connections of email entering your system.</td>
<td>None</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Overview of spam and unwanted email.</td>
<td>None</td>
</tr>
<tr>
<td>Submissions</td>
<td>Overview of spam submissions.</td>
<td>None</td>
</tr>
<tr>
<td>Malware</td>
<td>Overview of the current malware threats to your organization. Includes a message summary, malware summary, suspect malware outcomes, and separate tables showing stats for known and potential malware threats.</td>
<td>None</td>
</tr>
<tr>
<td>Threat defense</td>
<td>Overview of the current advanced threats that affect your organization.</td>
<td>None</td>
</tr>
<tr>
<td>Disarm</td>
<td>Overview of the potentially malicious content containers and types of threats detected and removed from email attachments.</td>
<td>None</td>
</tr>
<tr>
<td>Unscannable</td>
<td>Overview of unscannable email.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 21-2 describes the available content filtering reports.

Table 21-2  Content filtering reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>A summary of total detected content filtering violations.</td>
<td>None</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most content filtering matches have been detected. For each domain, the total messages that are processed, and number and percentage of content filtering policies triggered are listed.</td>
<td>Sender domains</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Required data storage options</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most content filtering matches have been detected. For each email address, the total messages that are processed and number and percentage of content filtering policies triggered are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most content filtering matches have been detected. For each HELO domain, the total messages that are processed, and number and percentage of content filtering policies triggered are listed. Specify the maximum number of HELO domains to list for the specified time range.</td>
<td>Sender HELO domains</td>
</tr>
<tr>
<td>Top Sender IP Connections</td>
<td>IP addresses from which the most content filtering matches have been detected. For each IP address, the total messages that are processed and number and percentage of content filtering policies triggered are listed. Specify the maximum number of IP addresses to list for the specified time range.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Recipient Domains</td>
<td>Recipient domains for which the most content filtering matches have been detected. For each recipient domain, the total messages that are processed, and number and percentage of content filtering policies triggered are listed. Specify the maximum number of recipient domains to list for the specified time range.</td>
<td>Recipient domains</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most content filtering matches have been detected. For each email address, the total messages that are processed and number and percentage of content filtering policies triggered are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Specific Senders</td>
<td>Number of content filtering policies triggered from a sender email address that you specify. For each grouping, the total messages that are processed and number and percentage of content filtering policies triggered are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of content filtering policies triggered for a recipient email address that you specify. For each grouping, the total messages that are processed and number and percentage of content filtering policies triggered are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Required data storage options</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Top Policies</td>
<td>Names of the most common content filtering match, number of policies triggered, and percentage of policies triggered versus total processed messages. Optionally, you can limit the report to a particular content incident folder.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 21-3 describes the available email messages reports.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>The following list is a summary of the total messages and messages that matched filters for:</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>■ Spam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Suspected spam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Unwanted email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Attacks (directory harvest, virus, and spam attacks)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Bad Sender groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Viruses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Suspicious attachments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Worms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Malware (spyware and adware)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Encrypted attachments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Content filtering.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Potentially malicious content (Disarm)</td>
<td></td>
</tr>
</tbody>
</table>

Custom       | Lets you select the columns that you want to appear in the report.                                                                           | None                          |

Average Message Size | The average size of messages in KB.                                                                                                           | None                          |

Total Message Size | Total size in KB of all messages in the report, and total size of each grouping.                                                           | None                          |

Number of Messages | Number of all messages in the report, and number for each grouping.                                                                         | None                          |

Number of Recipients | Number of recipients in the report, and number of recipients in each grouping. Every recipient in a message (To:, Cc:, and Bcc) counts as one. | None                          |
Table 21-3  Email messages reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most messages have been processed. For each domain, the total processed and number of malware, spam, and unwanted emails are listed. Specify the maximum number of domains to list for the specified time range.</td>
<td>Sender domains</td>
</tr>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most messages have been processed. For each email address, the total processed and number of malware, spam, and unwanted emails are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most messages have been processed. For each HELO domain, the total processed and number of malware, spam, and unwanted emails are listed. Specify the maximum number of HELO domains to list for the specified time range.</td>
<td>Sender HELO domains</td>
</tr>
<tr>
<td>Top Sender IP Connections</td>
<td>IP addresses from which the most messages have been processed. For each IP address, the total processed and number of malware, spam, and unwanted emails are listed. Specify the maximum number of IP addresses to list for the specified time range.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Recipient Domains</td>
<td>Recipient domains for which the most messages have been processed. For each recipient domain, the total processed, and number of malware, spam, and unwanted emails are listed. Specify the maximum number of recipient domains to list for the specified time range.</td>
<td>Recipient domains</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most messages have been processed. For each email address, the total processed and number of malware, spam, and unwanted emails are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Specific Senders</td>
<td>Number of messages that were processed for a sender email address that you specify. For each grouping, the total processed and number of malware, spam, and unwanted emails are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of messages that were processed for a recipient email address that you specify. For each grouping, the total processed and number of malware, spam, and unwanted emails are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
</tbody>
</table>

Table 21-4 describes the available types of invalid recipient reports.
### Table 21-4  Invalid recipients reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Summary of all invalid recipient email that enters your network.</td>
<td>None</td>
</tr>
<tr>
<td>Top Invalid Recipients</td>
<td>Invalid recipient email addresses with the most incoming messages.</td>
<td>Recipients, Recipient domains, Invalid Recipients</td>
</tr>
<tr>
<td>Top Probe Accounts</td>
<td>Probe accounts with the most incoming messages.</td>
<td>Recipients, Recipient domains, Invalid Recipients</td>
</tr>
<tr>
<td>Specific Invalid Recipients</td>
<td>Specified invalid email address with the most incoming messages.</td>
<td>Recipients, Recipient domains, Invalid Recipients</td>
</tr>
</tbody>
</table>

### Table 21-5  IP Connections reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation Summary</td>
<td>Summary of all good reputation and bad reputation verdicts on messages that enter your network. Includes Fastpass and Connection Classification.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Connection Summary</td>
<td>Number of connections that are attempted, accepted, rejected, and deferred at connection time.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Connection Classification Summary</td>
<td>Summary of connections based on their connection class.  See “About managing connection load at the gateway” on page 143.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Accepted Connections</td>
<td>IP addresses from which the most successful SMTP connections were detected.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Deferred Connections</td>
<td>IP addresses from which the most failed SMTP connections were detected.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Rejected Connections</td>
<td>IP addresses from which the most rejected SMTP connections were detected.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Virus Attacks</td>
<td>IP addresses from which the most malware attacks have been detected. For each IP address, the total messages that were processed and number and percentage of malware attacks are listed.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Directory Harvest Attacks</td>
<td>IP addresses from which the most directory harvest attacks have been detected. For each IP address, the total messages that were processed and number and percentage of directory harvest attacks are listed.</td>
<td>Sender IP connections</td>
</tr>
</tbody>
</table>
Table 21-6 describes the available spam reports.

### Table 21-6  Spam and unwanted email reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Summary of total detected spam and unwanted email messages (spam, Bad Senders, suspected spam, and unwanted emails). This summary includes messages that are detected by customer-specific spam rulesets.</td>
<td>None</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most spam and unwanted emails have been detected. For each domain, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and bad sender messages are listed.</td>
<td>Sender domains</td>
</tr>
<tr>
<td></td>
<td>Specify the maximum number of senders to list for the specified time range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify a specific verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu will be included in the report.</td>
<td></td>
</tr>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most spam and unwanted emails have been detected. For each email address, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and Bad Sender messages are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td></td>
<td>Specify the maximum number of email addresses to list for the specified time range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify a verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu are included in the report.</td>
<td></td>
</tr>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most spam and unwanted emails have been detected. For each HELO domain, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and Bad Sender messages are listed.</td>
<td>Sender HELO domains</td>
</tr>
<tr>
<td></td>
<td>Specify the maximum number of HELO domains to list for the specified time range.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify a verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu are included in the report.</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Required data storage options</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Top Sender IP Connections</td>
<td>IP addresses from which the most spam and unwanted emails have been detected. For each IP address, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and Bad Sender messages are listed. Specify the maximum number of IP addresses to list for the specified time range. Specify a verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu are included in the report.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Recipient Domains</td>
<td>Recipient domains for which the most spam and unwanted emails have been detected. For each recipient domain, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and Bad Sender messages are listed. Specify the maximum number of recipient domains to list for the specified time range. Specify a verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu are included in the report.</td>
<td>Recipient Domains</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most spam and unwanted emails have been detected. For each email address, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and Bad Sender messages are listed. Specify the maximum number of email addresses to list for the specified time range. Specify a verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu are included in the report.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Specific Senders</td>
<td>Number of spam and unwanted emails that were detected from a sender email address that you specify. For each grouping, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and bad sender messages are listed. Specify a specific verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu will be included in the report.</td>
<td>Senders, Sender domains</td>
</tr>
</tbody>
</table>
Table 21-6  Spam and unwanted email reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific Recipients</td>
<td>Number of spam and unwanted emails that were detected for a recipient email address that you specify. For each grouping, the spam-to-total-processed percentage, total processed, and the number of messages for spam, suspected spam, unwanted emails, and bad sender messages are listed. Specify a specific verdict to filter on from the Verdict menu. By default, all listed verdicts from the Verdict menu will be included in the report.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Sender Authentication Overview</td>
<td>Total number of messages that were processed, and number and percentage of the sender authentication sessions that were attempted, not attempted, successful, or failed.</td>
<td>None</td>
</tr>
<tr>
<td>Top Attempted Senders</td>
<td>Email addresses from which the most sender authentication attempts have been detected. For each email address, the total messages that were processed and number and percentage of sender authentication attempts are listed.</td>
<td>Senders</td>
</tr>
<tr>
<td>Top Not Attempted Senders</td>
<td>Email addresses from which the fewest sender authentication attempts have been detected. For each email address, the total messages that were processed and number and percentage of not attempted sender authentication sessions are listed.</td>
<td>Senders</td>
</tr>
<tr>
<td>Top Succeeded Senders</td>
<td>Email addresses from which the most successful sender authentication attempts have been detected. For each email address, the total messages that were processed and number and percentage of successful sender authentication attempts are listed.</td>
<td>Senders</td>
</tr>
<tr>
<td>Top Failed Senders</td>
<td>Email addresses from which the most failed sender authentication attempts have been detected. For each email address, the total messages that were processed and number and percentage of failed sender authentication attempts are listed.</td>
<td>Senders</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Total number of quarantined messages and quarantine releases.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 21-7 describes the available spam submission reports.

Table 21-7  Submissions reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Summary of customer-specific spam submissions (this summary does not include general spam submissions).</td>
<td>None</td>
</tr>
</tbody>
</table>
### Table 21-7  Submissions reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Submitters</td>
<td>Email addresses of the users who most frequently submit spam messages for customer-specific rulesets.</td>
<td>None</td>
</tr>
<tr>
<td>Top Admin Submitters</td>
<td>Email addresses of the administrators who most frequently submit spam messages for customer-specific rulesets.</td>
<td>None</td>
</tr>
<tr>
<td>Top Blocked Submitters</td>
<td>Email addresses of the submitters that you blocked who most frequently submit spam messages for customer-specific rulesets. See “Specifying who can submit messages for customer-specific rules” on page 273.</td>
<td>None</td>
</tr>
<tr>
<td>Top End-user Submitters</td>
<td>Email addresses of the end users that most frequently submit spam messages for customer-specific rulesets.</td>
<td>None</td>
</tr>
</tbody>
</table>

**Note:** Unscannable messages are no longer included in the Malware reports. Instead, a separate group of Unscannable reports are now available. Unscannable messages are no longer added to the counts in any of the Malware reports.

### Table 21-8  Malware reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Summary of the total number of malware instances detected. The <strong>Threats Detected</strong> column does not represent the threats that are detected as a percentage of the total messages that appear in the <strong>Messages Processed</strong> column. The <strong>Threats Detected</strong> column is the total of all the columns to its right (Viruses, Worms, Malware, Suspect Virus, and Encrypted Attachments). As such, the <strong>Threats Detected</strong> column is either 100% if any threats are detected, or 0% if no threats are detected.</td>
<td>None</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most malware messages have been detected. For each domain, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed. Specify the maximum number of senders to list for the specified time range.</td>
<td>Sender domains</td>
</tr>
<tr>
<td>Report</td>
<td>Description</td>
<td>Required data storage options</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most malware messages have been detected. For each email address, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most malware messages have been detected. For each HELO domain, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed. Specify the maximum number of HELO domains to list for the specified time range.</td>
<td>Sender HELO domains</td>
</tr>
<tr>
<td>Top Sender IP Connections</td>
<td>IP addresses from which the most malware messages have been detected. For each IP address, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed. Specify the maximum number of IP addresses to list for the specified time range.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Recipient Domains</td>
<td>Recipient domains for which the most malware messages have been detected. For each recipient domain, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed. Specify the maximum number of recipient domains to list for the specified time range.</td>
<td>Recipient Domains</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most malware messages have been detected. For each email address, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Top Virus and Worms</td>
<td>Names of the most common malware detected. For each grouping, the malware-to-total-processed percentage, malware to total malware and worm percentage, and last occurrence of the malware and worms are listed.</td>
<td>None</td>
</tr>
<tr>
<td>Specific Senders</td>
<td>Number of malware messages that were detected from a sender email address that you specify. For each grouping, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of malware messages that were detected for a recipient email address that you specify. For each grouping, the malware-to-total-processed percentage, total processed, and the number of instances of all types of malware are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
</tbody>
</table>
Table 21-9 describes the available Disarm reports.

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Summary of the total number of messages with potentially malicious attachments detected. The <strong>Multiple Threats</strong> column count includes only messages that contain two or more different types of threats (for example, PMC and spam). A message that contains several different types of PMC is counted as a single threat.</td>
<td>None</td>
</tr>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most messages containing attachments with PMC have been detected. For each domain, the PMC-to-total-processed percentage, total processed, and the number of PMC instances are listed. Specify the maximum number of senders to list for the specified time range.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most messages containing attachments with PMC have been detected. For each domain, the PMC-to-total-processed percentage, total processed, and the number of PMC instances are listed. Specify the maximum number of senders to list for the specified time range.</td>
<td>Sender domains</td>
</tr>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most messages with PMC have been detected. For each HELO domain, the PMC-to-total-processed percentage, total processed, and the number of PMC instances are listed. Specify the maximum number of senders to list for the specified time range. Specify the maximum number of HELO domains to list for the specified time range.</td>
<td>Sender HELO domains</td>
</tr>
<tr>
<td>Top Sender IP Connections</td>
<td>IP addresses from which the most messages with PMC have been detected. For each IP address, the PMC-to-total-processed percentage, total processed, and the number of PMC instances are listed. Specify the maximum number of IP addresses to list for the specified time range.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most messages with PMC have been detected. For each email address, the PMC-to-total-processed percentage, total processed, and the number of PMC instances are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Top Recipient Domains</td>
<td>Recipient domains for which the most messages with PMC have been detected. For each recipient domain, the PMC-to-total-processed percentage, total processed, and the number of messages with PMC are listed. Specify the maximum number of recipient domains to list for the specified time range.</td>
<td>Recipient Domains</td>
</tr>
</tbody>
</table>
### Table 21-9  Disarm reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific Senders</td>
<td>Number of messages with PMC that were detected from a sender email address that you specify. For each grouping, the PMC-to-total-processed percentage, total processed, and the number of messages with PMC are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of messages with PMC that were detected for a recipient email address that you specify. For each grouping, the PMC-to-total-processed percentage, total processed, and the number of messages with PMC are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
</tbody>
</table>

Table 21-10 describes the available unscannable reports.

### Table 21-10  Unscannable reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Summary of the total number of unscannable messages and attachments detected. The <strong>Threats Detected</strong> column does not represent the threats that are detected as a percentage of the total messages that appear in the <strong>Messages Processed</strong> column. The <strong>Threats Detected</strong> column is the total of all the columns to its right (different reasons why messages are unscannable). Thus, the <strong>Threats Detected</strong> column is either 100% (if any threats are detected) or 0% (if no threats are detected).</td>
<td>None</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most unscannable messages and attachments have been detected. For each domain, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed. Specify the maximum number of senders to list for the specified time range.</td>
<td>Sender domains</td>
</tr>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most unscannable messages and attachments have been detected. For each email address, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Senders, Sender domains</td>
</tr>
</tbody>
</table>
Table 21-10  Unscannable reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most unscannable messages and attachments have been detected. For each HELO domain, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed. Specify the maximum number of HELO domains to list for the specified time range.</td>
<td>Sender HELO domains</td>
</tr>
<tr>
<td>Top Sender IP Connections</td>
<td>IP addresses from which the most unscannable messages and attachments have been detected. For each IP address, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed. Specify the maximum number of IP addresses to list for the specified time range.</td>
<td>Sender IP connections</td>
</tr>
<tr>
<td>Top Recipient Domains</td>
<td>Recipient domains for which the most unscannable messages and attachments have been detected. For each recipient domain, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed. Specify the maximum number of recipient domains to list for the specified time range.</td>
<td>Recipient Domains</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most unscannable messages and attachments have been detected. For each email address, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed. Specify the maximum number of email addresses to list for the specified time range.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Specific Senders</td>
<td>Number of unscannable messages and attachments that were detected from a sender email address that you specify. For each grouping, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of unscannable messages and attachments that were detected for a recipient email address that you specify. For each grouping, the unscannable-to-total-processed percentage, total processed, and the number of unscannable messages are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
</tbody>
</table>

Troubleshooting report generation

Table 21-11 lists issues you might encounter when you generate reports.
Table 21-11  Report generation issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Information</th>
</tr>
</thead>
</table>
| No data available for the report type specified | Instead of displaying the expected reports, SMG might display the following message:  

No data is available for the report type and time range specified. |

If you receive this message, verify the following:  

■ Data exists for the filter you specified.  
   For example, perhaps you specified a recipient address that received no mail during the specified period for a Specific Recipients report.  
■ SMG is configured to keep data for that report type.  

Some reports require that you enable report data before those reports can be run.  

See “Select data to track for reports” on page 576.  

Occasionally you can produce reports even if data collection is not currently enabled. This situation can happen if you enabled data collection in the past and then turned off data collection. The data that are collected are available for report generation until they are old enough to be automatically purged. After that period, report generation fails. The "Delete data older than" setting on the Report Settings page controls this retention period. |

| Discrepancies in Suspect Virus Outcomes | The graph part of the Malware Summary report contains a section near the bottom called Suspect Virus Outcomes. The table part of the same report contains a Suspect Virus column. The total suspect virus outcomes may not match the suspect virus column.  

The reasons for this difference include the following:  

■ The suspect virus outcomes are counted as messages only if the message matches a policy that contains the action "Strip and Delay in Suspect Virus Quarantine" or "Hold message in Suspect Virus Quarantine."  
■ Even if a matching policy might trigger one of those actions for a message, another policy may match the message, and take precedence. For example, the message is deleted if a message contains a virus and a suspect virus, and the matching malware policy is "Delete message", and the matching suspect virus policy is "Hold message in Suspect Virus Quarantine,.". The message is deleted because deletion takes precedence over "Hold message in Suspect Virus Quarantine." |
Table 21-11 Report generation issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data in Content Filtering Summary report can look inconsistent</td>
<td>By default, the bottom of the Content Filtering Summary report contains a table of the top content filtering policies that were triggered. The table contains a Policies Triggered column and an Incidents Created column. Logically, the number of Incidents Created should never exceed the number of Policies Triggered. However, because of different data sources and timing issues, Incidents Created can sometimes exceed Policies Triggered.</td>
</tr>
</tbody>
</table>

Generated reports layout and data

Use the following information to help you understand the layout and data that appears in the reports that you generate.

Table 21-12 provides information about how reports are displayed.

Table 21-12 Report layout

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphs and tables</td>
<td>You can specify whether you want the report data to appear in a graph, table, or both. Graph and table options are not available for the Executive Summary report. The options for displaying report data for graphs and tables are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Graph—overview</td>
</tr>
<tr>
<td></td>
<td>Graphs each category of report data. This graph does not contain the summary information (sums and averages for the entire time period) listed in the overview table.</td>
</tr>
<tr>
<td></td>
<td>■ Graph—all others (non-overview) Displays bar graph(s) for each item in the report type chosen. For the reports other than the summary reports, a maximum of 20 items can be displayed in a bar graph.</td>
</tr>
<tr>
<td></td>
<td>■ Table Creates numeric a representation of the report data. For all reports, a table report can list more than 20 items.</td>
</tr>
<tr>
<td></td>
<td>The method to save graphs and tables to files depends on the report format, and whether you save or email the report.</td>
</tr>
</tbody>
</table>
Table 21-12  Report layout (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of rows</td>
<td>The maximum size for any report (including a scheduled report) is 1,000 rows. If you encounter this limitation, shorten the time range, group by a longer time interval, or decrease the top entries field (applicable to some reports).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This limitation is not configurable.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you request a report of the top 50 invalid recipients, you may see the following error which you can ignore: <em>The estimated report size is greater than 1000 rows. Please modify available search criteria to limit the size of the report. For example, decrease the Time range or Group by interval.</em></td>
</tr>
<tr>
<td>Extra bars in report graphs</td>
<td>The current fractional hour is included in report graphs in its own bar. This information ensures that the entirety of the selected time range is displayed. This extra bar usually portrays noticeably less data than the rest of the bars. Consider the following examples:</td>
</tr>
<tr>
<td></td>
<td>■ You run a report for the past hour at 2:22 P.M. Tuesday:</td>
</tr>
<tr>
<td></td>
<td>■ The resulting data set is from 1:00 P.M. until 2:22 P.M.</td>
</tr>
<tr>
<td></td>
<td>■ The data appears by hour, spread across two bars.</td>
</tr>
<tr>
<td></td>
<td>■ You run a report for the past 24 hours at 2:22 P.M. Tuesday:</td>
</tr>
<tr>
<td></td>
<td>■ The resulting data is from 2:00 P.M. Monday until 2:22 P.M. Tuesday.</td>
</tr>
<tr>
<td></td>
<td>■ The data appears by hour, spread across 25 bars.</td>
</tr>
<tr>
<td>Time ranges</td>
<td>Report statistics are stored in units from 0 minutes, 0 seconds to 59 minutes, 59 seconds of every hour. For example, from 1:00 A.M. to 1:59 A.M. is one unit and from 2:00 A.M. to 2:59 A.M. is another unit. Because of this scheme, reports cannot be displayed with a time range less than an hour or grouped by a period less than an hour.</td>
</tr>
</tbody>
</table>

Table 21-13 provides the information to help you interpret the information in reports.

Table 21-13  Report data details

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>What constitutes a threat</td>
<td>The summary reports and the dashboard contain threat summary graphs and tables. A threat is a harmful attribute or potentially harmful attribute of an email message. For example, threats include spam, malware, and content filtering policy violations. Similar message verdicts are grouped into threat categories.</td>
</tr>
<tr>
<td>Single threat, multiple threat, and clean messages</td>
<td>The summary reports and the dashboard categorize messages into single threat, multiple threat, and clean messages. Multiple threat messages contain more than one type of threat. For example, a message that contains spam and malware is a multiple threat message. Clean messages contain no known threats.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Message and connection counts</td>
<td>The appliance uses many technologies to track email and filter email. Some of these technologies function at the email connection level before an actual email message can be generated and sent. When a connection is rejected or deferred because it triggered a bad reputation filter, that connection is counted as one message.</td>
</tr>
<tr>
<td>Verdicts of suspect virus messages</td>
<td>If a message is routed to the Suspect Virus Quarantine, the outcome of rescanning the message is not counted toward total threat counts. However, the outcome of rescanning the message is displayed in the Suspect Virus Outcomes graph. The graph indicates whether suspect viruses were deleted, determined to be viruses or not, or are still in the Suspect Virus Quarantine.</td>
</tr>
</tbody>
</table>
Table 21-13 Report data details (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender HELO domain or IP connection shows gateway information</td>
<td>If any Scanners accept relayed messages from a gateway computer, the SMTP HELO name is the name or IP address of the gateway computer. The IP connection address is the IP address of the computer that is connected to the gateway computer. Affected reports are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Top Sender HELO Domains</td>
</tr>
<tr>
<td></td>
<td>All Top Sender HELO Domain reports are affected</td>
</tr>
<tr>
<td></td>
<td>■ Top Sender IP Connections</td>
</tr>
<tr>
<td></td>
<td>All Top Sender IP Connections reports are affected</td>
</tr>
<tr>
<td></td>
<td>■ Top Succeeded Connections SMTP report</td>
</tr>
<tr>
<td></td>
<td>■ Top Failed Connections SMTP report</td>
</tr>
<tr>
<td></td>
<td>■ Top Rejected Connections SMTP report</td>
</tr>
</tbody>
</table>

The process to determine which IP address SMG uses is as follows:

1. SMG first checks if the connecting IP address is outside the internal range. If it is, the connecting IP address is the logical IP address.
2. If the connecting IP address is inside the internal range, SMG walks through the received headers. It starts this process by considering the first received header as the current received header.
3. If the current received header has one IP address, SMG checks if it is outside the internal range. If it is, this IP address is the logical IP address.
4. If the current received header has one IP address and it is inside the internal range, SMG looks for the next received header.
5. If there is a next received header, SMG makes it the new, current received header and loops back to step 3.
6. If there are no more received headers, then the chain successfully ends on an internal IP address. SMG uses the connecting IP address as the logical IP address.
7. If SMG is unable to successfully walk through all of the received headers because one of them contains either 0 or multiple IP addresses, it considers the header chain broken. SMG reports the IP address as 255.255.255.255.

Processed message count | For the reports that list the number of processed messages, the number of processed messages is counted per message, not per recipient. For example, if a single message lists 12 recipients, the processed message count increases by 1, not 12.
### How duplicate verdicts per messages are reported

Each email message can have multiple recipients and multiple threats. Different recipients in the same email message may have different threats triggered. This situation occurs because the different recipients may belong to different policy groups. For example, recipients in group A may have content filtering enabled for employee data protection terms, while recipients in group B may not.

Some verdicts have names associated with them to describe unique instances of that verdict type. For example, a known virus may be called W32.Zoltan or VBS.Throckmorton. Each named verdict is counted separately. If both W32.Zoltan and VBS.Throckmorton are found one or more times in a message, the malware count increases by two. The message is considered a multiple threat message.

The following verdicts have unique names:
- Content filtering policies
- Malware
- Viruses
- Worms

Verdicts that are not included in this list are counted once per message regardless of the number of occurrences of the verdict in the message. For example, a single message is sent to three recipients. The message to recipient A has two matches for encrypted content. The same message that is sent to recipient B has two matches for encrypted content. That same message that is sent to recipient C has no matches. The total count of encrypted content for the message is one. The malware threat count for the message is one (encrypted content counts as a malware without a unique name).

If no other threats are detected in the message, it is considered a single threat message.

See “Threat category components” on page 605.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>How duplicate verdicts per messages are reported</td>
<td>Each email message can have multiple recipients and multiple threats. Different recipients in the same email message may have different threats triggered. This situation occurs because the different recipients may belong to different policy groups. For example, recipients in group A may have content filtering enabled for employee data protection terms, while recipients in group B may not. Some verdicts have names associated with them to describe unique instances of that verdict type. For example, a known virus may be called W32.Zoltan or VBS.Throckmorton. Each named verdict is counted separately. If both W32.Zoltan and VBS.Throckmorton are found one or more times in a message, the malware count increases by two. The message is considered a multiple threat message. The following verdicts have unique names:</td>
</tr>
<tr>
<td></td>
<td>- Content filtering policies</td>
</tr>
<tr>
<td></td>
<td>- Malware</td>
</tr>
<tr>
<td></td>
<td>- Viruses</td>
</tr>
<tr>
<td></td>
<td>- Worms</td>
</tr>
<tr>
<td></td>
<td>Verdicts that are not included in this list are counted once per message regardless of the number of occurrences of the verdict in the message. For example, a single message is sent to three recipients. The message to recipient A has two matches for encrypted content. The same message that is sent to recipient B has two matches for encrypted content. That same message that is sent to recipient C has no matches. The total count of encrypted content for the message is one. The malware threat count for the message is one (encrypted content counts as a malware without a unique name). If no other threats are detected in the message, it is considered a single threat message.</td>
</tr>
<tr>
<td></td>
<td>See “Threat category components” on page 605.</td>
</tr>
</tbody>
</table>
Monitoring Symantec Messaging Gateway's status

This chapter includes the following topics:

- About monitoring system status
- Using the Dashboard
- Monitoring host computers and service status
- Monitoring log data
- Monitoring logs on a remote server
- Working with the message audit log and message queue
- Monitoring scheduled tasks

About monitoring system status

You can monitor the status of Symantec Messaging Gateway from the Control Center. The ability to monitor the status of your product lets you stay up-to-date on product performance and activity. In some cases, you can use filters to customize the status information such as specifying time ranges.

Table 22-1 describes the items that you can monitor.
### Table 22-1 Status items that you can monitor

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>You can monitor the following system statuses:</td>
</tr>
</tbody>
</table>
|          | ▪ Dashboard  
|          | View the Dashboard to obtain a dynamic view of product status and filtering activity for various time frames.  
|          | See “Using the Dashboard” on page 603.  
|          | ▪ Hosts  
|          | You can monitor the status of your hardware and the size and volume of your message queues. You can also view information about the hardware, software, and services that are installed.  
|          | See “Viewing information about your hardware” on page 608.  
|          | See “Software and services status definitions” on page 610.  
|          | See “Viewing the status of your hardware” on page 609.  
|          | See “Monitoring message queue size and volume” on page 647.  
|          | ▪ Logs  
|          | Symantec Messaging Gateway logs information about the Control Center, Spam Quarantine, directory data service, and logs on each Scanner. You can view these logs to monitor the status of your product and troubleshoot issues.  
|          | See “About logs” on page 614.  
| SMTP     | You can monitor the following SMTP statuses: |
|          | ▪ Message audit logs  
|          | Symantec Messaging Gateway provides a message auditing component that lets you search for messages to find out what has happened to them. You can view the message audit log to determine the trail of messages that Scanners accept and process.  
|          | ▪ Message queues  
|          | A message queue is a temporary holding area for messages before they reach their destination. You can view the messages that are queued in any of the message queues.  
|          | See “About message queues” on page 642.  

### Using the Dashboard

The **Dashboard** page displays graphs and tables that summarize the Symantec Messaging Gateway status and mail filtering activity.

- From the drop-down menu, select whether to display summary information for inbound messages, outbound messages, or both inbound messages and outbound messages.  
- From the other drop-down menu, select the time period for the data. **Table 22-2** describes the summary information that Symantec Messaging Gateway displays for your selections.
Table 22-3 describes the System Status tables at the bottom of the Dashboard and the Symantec ThreatCon level display.

This page is the first one you see when you log in to the Control Center. To return to the Dashboard from another Control Center page, select Status > System > Dashboard.

Table 22-2 Dashboard summary information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages graph</td>
<td>Displays the message counts for the following categories:</td>
</tr>
<tr>
<td></td>
<td>■ Single threat messages, which triggered one violation per message.</td>
</tr>
<tr>
<td></td>
<td>■ Multiple threat messages, which triggered more than one violation per message.</td>
</tr>
<tr>
<td></td>
<td>■ Clean messages, which triggered no violations.</td>
</tr>
<tr>
<td></td>
<td>All data is for the time frame that you specified in the drop-down menu.</td>
</tr>
<tr>
<td>Messages table</td>
<td>For the specified time period, shows actual counts and percentages of the overall message volume for single threat, multiple threat, and clean messages.</td>
</tr>
<tr>
<td>Threats graph</td>
<td>For the specified time period, displays the most common message verdicts in proportion to the total volume of perceived threats.</td>
</tr>
<tr>
<td>Threats table</td>
<td>Lists individual counts and percentage of total message volume for common message verdicts, during the specified time period.</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td>See “Threat category components” on page 605.</td>
</tr>
<tr>
<td>Top 5 Named Viruses table</td>
<td>Lists the most prevalent viruses and worms that the malware filters detected during the specified time frame. The table lists the malware types by frequency. Click the Details link to access a more granular report on the viruses that threaten your system.</td>
</tr>
<tr>
<td></td>
<td><img src="image.png" alt="Image" /></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The Top 5 Named Viruses statistics and the linked report do not include data from threat defense scanning.</td>
</tr>
<tr>
<td>Top 5 Content Filtering Policies table</td>
<td>Lists the most numerous content filtering policy violations for the specified time frame, ranked by frequency. Click Details to access more granular data on your top content filtering concerns.</td>
</tr>
</tbody>
</table>
Table 22-3  System Status  

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Status of the hardware components and software components in your system. These statuses include current software version, all Scanners accessible to the Control Center, hardware status, and submission service status. For a detailed status on each item, click on its associated link.</td>
</tr>
<tr>
<td>Licenses</td>
<td>Status of the licenses you purchased from Symantec.</td>
</tr>
<tr>
<td>Definitions</td>
<td>Status of spam, customer-specific spam, and virus definitions available through Symantec LiveUpdate. Click the date that is adjacent to the Virus definitions field to access the LiveUpdate Settings page. Click the link that is adjacent to Customer-specific Spam definitions to access the Customer-specific Spam submissions page. Note: Definitions shows the oldest definition across all the Scanners that are licensed for the feature.</td>
</tr>
<tr>
<td>Symantec ThreatCon level</td>
<td>Rating of the global threat exposure that is delivered as part of Symantec DeepSight Threat Management System. The Symantec ThreatCon indicator is located to the left of the Dashboard.</td>
</tr>
</tbody>
</table>

See "Threat category components" on page 605.

Threat category components

The Dashboard contains data for several threat categories.

Table 22-4 lists the verdicts that make up each threat category so that you can better interpret and analyze the data.
<table>
<thead>
<tr>
<th>Threat category</th>
<th>Verdicts that make up the threat category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content violations</td>
<td>The content violations category includes the following components:</td>
</tr>
<tr>
<td></td>
<td>■ End user and administrator-defined language policies</td>
</tr>
<tr>
<td></td>
<td>■ End user Bad Senders</td>
</tr>
<tr>
<td></td>
<td>■ Local Bad Sender Domains</td>
</tr>
<tr>
<td></td>
<td>The following content filtering policies count as threats if <strong>Track violations of this policy in the dashboard and reports</strong> is checked on the Add/Edit Email Content Filtering Policy page:</td>
</tr>
<tr>
<td></td>
<td>■ Content filtering policies triggered</td>
</tr>
<tr>
<td></td>
<td>■ Incidents Created</td>
</tr>
<tr>
<td></td>
<td>■ Held Messages:</td>
</tr>
<tr>
<td></td>
<td>■ Approved</td>
</tr>
<tr>
<td></td>
<td>■ Rejected</td>
</tr>
<tr>
<td></td>
<td>■ Currently held</td>
</tr>
<tr>
<td></td>
<td>See “<strong>Viewing, editing, adding, and managing your content filtering policies</strong>” on page 323.</td>
</tr>
<tr>
<td>Malware</td>
<td>Malware threat category components are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Viruses</td>
</tr>
<tr>
<td></td>
<td>■ Worms</td>
</tr>
<tr>
<td></td>
<td>■ Malware</td>
</tr>
<tr>
<td></td>
<td>Potential malware threat category components are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Suspect Virus</td>
</tr>
<tr>
<td></td>
<td>■ Encrypted Attachment</td>
</tr>
<tr>
<td>Invalid recipients</td>
<td>■ Invalid recipients</td>
</tr>
<tr>
<td>Bad reputation</td>
<td>Bad reputation threat category components are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Directory Harvest Attacks</td>
</tr>
<tr>
<td></td>
<td>■ Virus Attacks</td>
</tr>
<tr>
<td></td>
<td>■ Local Bad Sender IPs</td>
</tr>
<tr>
<td></td>
<td>■ Connection Class</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Global Bad Senders</td>
</tr>
<tr>
<td></td>
<td>■ Reverse DNS validation failed</td>
</tr>
<tr>
<td></td>
<td>Good reputation threat category components are as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Global Good Senders</td>
</tr>
<tr>
<td></td>
<td>■ Good IPs</td>
</tr>
<tr>
<td></td>
<td>■ Fastpass</td>
</tr>
</tbody>
</table>
Table 22-4  Threat category components (continued)

<table>
<thead>
<tr>
<th>Threat category</th>
<th>Verdicts that make up the threat category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam and unwanted email</td>
<td>■ Sender authentication failure</td>
</tr>
<tr>
<td></td>
<td>■ Spam</td>
</tr>
<tr>
<td></td>
<td>■ Suspected spam</td>
</tr>
<tr>
<td></td>
<td>■ Bounce Attack</td>
</tr>
<tr>
<td></td>
<td>■ Marketing email</td>
</tr>
<tr>
<td></td>
<td>■ Newsletter</td>
</tr>
<tr>
<td></td>
<td>■ Redirect URL content</td>
</tr>
<tr>
<td>Unscannable messages and attachments</td>
<td>■ Unscannable for malware and content filtering for any reason</td>
</tr>
<tr>
<td></td>
<td>■ Unscannable for malware and content filtering due to limits exceeded</td>
</tr>
<tr>
<td></td>
<td>■ Unscannable for malware and content filtering for other reasons</td>
</tr>
<tr>
<td></td>
<td>■ Unscannable for Disarm</td>
</tr>
<tr>
<td>Disarmed Messages</td>
<td>Disarmed attachments</td>
</tr>
<tr>
<td>Threat Defense - Advanced Threat</td>
<td>Advanced threats detected by Symantec Content Analysis</td>
</tr>
</tbody>
</table>

See “Using the Dashboard” on page 603.

Monitoring host computers and service status

Table 22-5 describes how you can monitor the host computer, software, and services. You can perform these tasks as needed in any order.

Table 22-5  Monitor host computers and service status

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View information about the Control Center host and every Scanner that the Control Center administers.</td>
<td>Some hardware information does not apply to the virtual computers that are configured with VMware products. In some cases, a hardware information field may not display for Dell hardware. See “Viewing information about your hardware” on page 608.</td>
</tr>
<tr>
<td>Monitor the hardware status for all of the Scanners that the Control Center administers.</td>
<td>Some items appear in red if there is an error condition. The status that appears is based on stored data, so it may be a few minutes old. A dash (–) in a column indicates that the data is not available for that hardware. See &quot;Viewing the status of your hardware” on page 609.</td>
</tr>
</tbody>
</table>
### Table 22-5  Monitor host computers and service status (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the version of software that is installed on the components that the Control Center administers.</td>
<td>You can also see the status of the services that are running for each component. See &quot;Viewing the status of your software and services&quot; on page 609.</td>
</tr>
<tr>
<td>View the status of your software and services.</td>
<td>Status details for your appliance depend on how each appliance is configured. You can configure an appliance to be a Control Center, a Scanner, or both. See &quot;Software and services status definitions&quot; on page 610.</td>
</tr>
</tbody>
</table>

### Viewing information about your hardware

You can view information about the Control Center host and every Scanner that the Control Center administers. Some hardware information does not apply to the virtual computers that are configured with VMware products. In some cases, a hardware information field may not display for Dell hardware.

The information that appears is as follows:

- Hostname
- Model
- Processor Type
- Processor Cores
- Dell Service Tag
- Total Memory
- Disk

Hardware information is updated dynamically. Some data may not be available while an appliance starts up.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view information about your hardware.

See "Viewing the status of your hardware" on page 609.

See "Software and services status definitions" on page 610.

**To view information about your hardware**

1. In the Control Center, click **Status > System > Hosts**.
2. Click the **Hardware Information** tab.
Viewing the status of your hardware

You can monitor the hardware status for all of the Scanners that the Control Center administers. Some items appear in red if there is an error condition. The status that appears is based on stored data, so it may be a few minutes old. A dash (—) in a column indicates that the data is not available for that hardware.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view information the status of your hardware.

See “Software and services status definitions” on page 610.

To view the status of your hardware

1. In the Control Center, click **Status > System > Hosts**.
2. Click the **Hardware Status** tab.
3. To view additional status information, click the hostname.
   - When you click the hostname, the data is read from the host to provide real-time status.

Viewing the status of your software and services

You can view the version of software that is installed on the components that the Control Center administers. You can also see the status of the services that are running for each component.

See “Software and services status definitions” on page 610.

If you want to enable or make any modifications, the same page provides a shortcut by clicking on a linked word.

To view the status of software and services

1. In the Control Center, click **Status > System > Hosts**.
2. Click the **Software and Services** tab.
3. To view additional information about a host, click the host that you want to examine.
   - Click the plus sign, where available, next to any component to view additional information on that component.
4. To enable or modify a Scanner click any linked word to access the **Edit Host Configuration** page.
   - See “Modifying Scanner configurations” on page 67.
   - See “Scanner Services” on page 73.
Software and services status definitions

Status details for your appliance depend on how each appliance is configured. You can configure an appliance to be a Control Center, a Scanner, or both.

Table 22-6 describes the software and services status for the Control Center.

Table 22-7 describes the software and services status for Scanners.

See “Viewing the status of your software and services” on page 609.

**Table 22-6**  Control Center software and services status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Center</strong></td>
<td>Click the Control Center name link for additional details. The Services page appears in a tree mode. The information for that Host updates when you click Back to Services Status. A green check indicates that the current version of Symantec Messaging Gateway is installed. A yellow exclamation mark (!) indicates that a newer version of Symantec Messaging Gateway is available. A red X indicates that the Control Center version is different than the Scanner version.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>The currently installed version of Symantec Messaging Gateway. The version is displayed in red if a newer version is available.</td>
</tr>
<tr>
<td><strong>Spam Quarantine</strong></td>
<td>Spam Quarantine contains quarantined spam messages. You can search, delete, sort, and release quarantined messages.</td>
</tr>
<tr>
<td><strong>Spam Quarantine Disk Usage</strong></td>
<td>The amount of disk space that Spam Quarantine uses.</td>
</tr>
<tr>
<td><strong>Suspect Virus Quarantine</strong></td>
<td>Suspect Virus Quarantine contains messages that could potentially contain viruses. You can search, delete, sort, and release quarantined messages.</td>
</tr>
<tr>
<td><strong>Suspect Virus Quarantine Disk Usage</strong></td>
<td>The amount of disk space that Suspect Virus Quarantine uses.</td>
</tr>
<tr>
<td><strong>Content Incident Folders</strong></td>
<td>Content incident folders help you organize, monitor, and manage the incidents that trigger content filtering policies in which the action is to create an incident in a content incident folder.</td>
</tr>
<tr>
<td><strong>Content Incident Folders Disk Usage</strong></td>
<td>The amount of disk space that content filtering quarantine uses.</td>
</tr>
<tr>
<td><strong>Directory Data Service</strong></td>
<td>The status of LDAP, either Running or Stopped.</td>
</tr>
</tbody>
</table>
### Table 22-7  Scanner software and services status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scanners</strong></td>
<td>Click the Scanner name link for additional details. The Services page appears in a tree mode. The information for that Host updates when you click <strong>Back to Services Status</strong>. A green check mark indicates that the current version of Symantec Messaging Gateway is installed. A yellow exclamation mark (!) indicates that a newer version of Symantec Messaging Gateway is available. A red X indicates that the Control Center version is different than the Scanner version.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>The currently installed version of Symantec Messaging Gateway. The version is displayed in red if a newer version is available.</td>
</tr>
<tr>
<td><strong>Virus Definitions</strong></td>
<td>The date of the last virus definition update. The date is displayed in red if the virus definitions are out of date or the last LiveUpdate attempt failed.</td>
</tr>
<tr>
<td><strong>Scanner</strong></td>
<td>The status of the Scanner, either enabled or disabled.</td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td>The status of the Agent, either <strong>Running</strong> (in black) or <strong>Stopped</strong> (in red). If the Agent crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. The Agent transfers configuration information between the Control Center and attached and enabled Scanners.</td>
</tr>
<tr>
<td><strong>Conduit</strong></td>
<td>The status of the Conduit, either <strong>Running</strong> (in black) or <strong>Stopped</strong> (in red). If the Conduit crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. The Conduit retrieves new and updated filters from Symantec Security Response through secure HTTPS file transfer.</td>
</tr>
<tr>
<td><strong>Directory Data Service</strong></td>
<td>The status of the directory data service, either <strong>Running</strong> (in black) or <strong>Stopped</strong> (in red). If the directory data service crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. The directory data service lets you use the information that is stored in your Lightweight Directory Access Protocol (LDAP) directories for features in the Symantec Messaging Gateway.</td>
</tr>
</tbody>
</table>
Table 22-7  
Scanner software and services status (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUpdate</td>
<td>The status of LiveUpdate, either Running (in black) or Stopped (in red). If LiveUpdate crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. LiveUpdate automatically downloads virus definitions from Symantec Security Response to the Scanner.</td>
</tr>
<tr>
<td>Brightmail Engine</td>
<td>The status of the Brightmail Engine, either Running (in black) or Stopped (in red). If the Brightmail Engine crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. The Brightmail Engine scans email and attachments for viruses, spam, and content filtering according to the filter polices that you have configured.</td>
</tr>
<tr>
<td>MTA</td>
<td>The status of the mail transfer agent, either Running (in black) or Stopped (in red). If the MTA crashed in the last 24 hours, a red underline appears beneath the status. Hover your mouse over the red underline to view the number of crashes that occurred in the last 24 hours. The MTA routes inbound and outbound messages to the Brightmail Engine for processing and delivers filtered messages to their internal destinations or to the Internet.</td>
</tr>
</tbody>
</table>

Monitoring log data

Symantec Messaging Gateway logs information about the Control Center, Spam Quarantine, directory data service, and logs on each Scanner.

Table 22-8 describes how you can monitor this data.

Table 22-8  
Monitor log data

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about Symantec</td>
<td>Symantec Messaging Gateway keeps log records of component activity on Symantec Messaging Gateway. If any part of Symantec Messaging Gateway does not work properly, you can view logs to investigate the problem. Even if you do not notice any problems, Symantec recommends that you view logs regularly to check the status of the components. See “About logs” on page 614.</td>
</tr>
<tr>
<td>Messaging Gateway.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 22-8  Monitor log data (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about the types of logs that you can use.</td>
<td>View a list of log types that are available for Scanners. See “Log types” on page 615.</td>
</tr>
<tr>
<td>View the events that are logged for the Control Center, Scanners, directory data service, and Quarantine.</td>
<td>If any part of Symantec Messaging Gateway does not work properly, you can view logs to investigate the problem. Even if you do not notice any problems, Symantec recommends that you view logs regularly to check the status of the components. See “Viewing log files” on page 617.</td>
</tr>
<tr>
<td>You may want to periodically view the Control Center error log to troubleshoot issues.</td>
<td>All errors that are related to the Control Center are written to the BrightmailLog.log file. See “Viewing the Control Center error log” on page 618.</td>
</tr>
<tr>
<td>Save a log file to assist in troubleshooting.</td>
<td>When you save a log file, you can view and print the file with a text editor application. You can also email the file. Log files are saved in .txt format. See “Saving log files” on page 619.</td>
</tr>
<tr>
<td>Ensure that your log database does not exceed a maximum limit.</td>
<td>Depending on your environment and the log level that you specify, the log database can quickly increase to an unmanageable size. To prevent expansion, Symantec Messaging Gateway provides controls for specifying a maximum database size (the default is 50 MB). It also provides a log Expunger utility which purges older logs and prevents the database from exceeding the set limit (the default setting is daily). Users may also create custom configurations to meet specific or temporary needs. See “Managing the log database size” on page 620.</td>
</tr>
<tr>
<td>Specify the amount of log data to store for Scanners components.</td>
<td>You can set Scanner log levels in five increments from error level to debug level. Each succeeding log level after errors includes log data for all of the previous log levels. See “Configuring log levels” on page 622.</td>
</tr>
<tr>
<td>Delete logs manually from the log database.</td>
<td>You can clear Scanner log files and directory data service log files from the Control Center log database on the <strong>Status &gt; System &gt; Logs</strong> page. See “Manually deleting log files” on page 624.</td>
</tr>
</tbody>
</table>
### Table 22-8  Monitor log data (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about how log disk space alerts work.</td>
<td>Symantec Messaging Gateway includes an enhanced logging feature that allows system administrators to enable alerts when logging disk space on Scanners nears or reaches capacity. When the default threshold levels are reached, the system shifts to a reduced or halted logging mode and sends an email notification to the specified administrator. You will need to enable the low disk space alerts to receive this notification. See “About log disk space alerts” on page 625.</td>
</tr>
<tr>
<td>Clear disk space.</td>
<td>View a list of options for clearing disk space on the Control Center and Scanner appliances. Use these options if you have determined that low disk space availability currently affects system performance. See “Clear disk space checklist” on page 625.</td>
</tr>
</tbody>
</table>

### About logs

Symantec Messaging Gateway keeps log records of component activity on Symantec Messaging Gateway. If any part of Symantec Messaging Gateway does not work properly, you can view logs to investigate the problem. Even if you do not notice any problems, Symantec recommends that you view logs regularly to check the status of the components.

You can specify the level of information that you want to log for each of your Scanners. Some levels can yield high volumes of data. Set the log levels to the lowest level that meets your monitoring needs. The default log level of warning is usually appropriate.

You view log data in the Control Center. You can sort log data, create log reports, and clear log files from the database. You can also view logs using the command line interface with the `cat`, `grep`, `more`, and `tail` commands. The command line interface displays real-time log data. See “Viewing log files” on page 617.

See “Saving log files” on page 619.

In addition to viewing logs using the Control Center, some Scanner logs can be sent to syslog on a remote server. See “Configuring remote logging to syslog” on page 628.

Symantec Messaging Gateway lets you configure the log database size to prevent the database from filling the hard disk. It also provides a log Expunger utility that lets you set automatic purges at specified intervals. See “Managing the log database size” on page 620.

See “Log types” on page 615.
Scanner logs are made available in the Control Center in two steps: First, incoming data files are captured to a temporary location on the Scanner. Next, the Control Center accesses the temporary location and copies the data to the Control Center log database. Once the log data from the Scanner is transferred to the Control Center, the system deletes log data on the Scanner to conserve disk space.

In some circumstances the Scanner logs can fill up the disk faster than the Control Center can copy the data to the log database. If a Scanner disk nears or reaches capacity, the system reduces or halts logging and no logs are copied to the Control Center log database. You must free disk space for normal logging to resume.

See “About log disk space alerts” on page 625.

See “Clear disk space checklist” on page 625.

Log types

Symantec Messaging Gateway logs let you monitor events for your Scanners, the Control Center, Directory Data Service, and Spam Quarantine.

Table 22-9 describes the log types that are available for Scanners.

Table 22-9  Scanner log types

<table>
<thead>
<tr>
<th>Scanner log type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduit</td>
<td>Records the status about downloading antispam rules and uploading statistics.</td>
</tr>
<tr>
<td>Brightmail Client</td>
<td>Records the status about message filtering.</td>
</tr>
<tr>
<td>Brightmail Engine</td>
<td>Records the status of the Brightmail Engine.</td>
</tr>
<tr>
<td>JLU Controller</td>
<td>Records the status about Java LiveUpdate virus definition downloads. This log is the primary log file that you should use for troubleshooting LiveUpdate issues.</td>
</tr>
<tr>
<td>JLU Client</td>
<td>An auxiliary log file to the JLU Controller log file that records the status about Java LiveUpdate virus definition downloads. Use this log file only when the JLU Controller log file does not contain enough information for troubleshooting an issue.</td>
</tr>
<tr>
<td>MTA</td>
<td>Records the status about sending and receiving email.</td>
</tr>
<tr>
<td>Content Filtering</td>
<td>Records the status about Content Filtering.</td>
</tr>
</tbody>
</table>

Table 22-10 describes the log types that are available for the Control Center console.
### Table 22-10  Control Center log types—Console

<table>
<thead>
<tr>
<th>Console log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BrightmailLog.log</td>
<td>Records the status about Control Center interactions.</td>
</tr>
<tr>
<td>catalina&lt;date&gt;.log and catalina.out</td>
<td>Records the status from the Tomcat Web server. The Control Center runs inside the Tomcat server. These files contain the messages that are generated from the Tomcat Server and also the applications that run within Tomcat.</td>
</tr>
</tbody>
</table>

Table 22-11 describes the log types that are available for the Control Center database.

### Table 22-11  Control Center log types—Database

<table>
<thead>
<tr>
<th>Database log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error.log and error.log.#.gz</td>
<td>Records any errors that occur while the Control Center accesses the MySQL database.</td>
</tr>
<tr>
<td>slow-queries.log and slow-queries.log.#.gz</td>
<td>Records the slow MySQL queries.</td>
</tr>
</tbody>
</table>

Table 22-12 describes the log type that is available for the Control Center events.

### Table 22-12  Control Center log types—Events

<table>
<thead>
<tr>
<th>Event log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brightmail_Admin_Events.&lt;yyy-mm-dd&gt;.log</td>
<td>Records all changes made in the Control Center for the date that is indicated in the log file name.</td>
</tr>
</tbody>
</table>

Table 22-13 describes the log that is available for Spam Quarantine.

### Table 22-13  Quarantine log

<table>
<thead>
<tr>
<th>Quarantine log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Records the To address, From address, and Subject of each message that is released from Spam Quarantine. It also records the user who released each message and a timestamp.</td>
</tr>
</tbody>
</table>

Table 22-14 describes the log that is available for directory data service.

### Table 22-14  Directory data service log

<table>
<thead>
<tr>
<th>DDS log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Data Service</td>
<td>Records the status about directory data service.</td>
</tr>
</tbody>
</table>
Viewing log files

You can view the events that are logged for the Control Center, Scanners, Directory Data Service, and Quarantine. If any part of Symantec Messaging Gateway does not work properly, you can view logs to investigate the problem. Even if you do not notice any problems, Symantec recommends that you view logs regularly to check the status of the components.

When you specify a filter and click **Display**, Symantec Messaging Gateway displays the log events that match the filter. You must have one of the following access levels to view logs:

- **Full Administration Rights**
- **Manage Status and Logs** with **View** or **Modify** rights

For Scanner logs, the amount of log data available depends on the log level that you set for the Scanner component. For example, if you set the Conduit log level to warnings, no log data is saved or available for notice, information, or debug level events. Set the Scanner component log levels on the **Administration > Settings > Logs** page.

The Control Center displays a question mark icon next to the description of error level Scanner logs. Click the icon to display a Web page that contains more information about the error. The Web page opens in a new Web browser window. The Web page may indicate that Symantec has not published information about the error. Symantec tracks the error information requests and adds new error information continually.

**Table 22-15** lists the filter options that you can use to view specific log events.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong> (drop-down)</td>
<td>Select a host from the list. This option is only available for Scanner and directory data service logs.</td>
</tr>
<tr>
<td><strong>Severity</strong> (drop-down)</td>
<td>Select a severity level from the list. This option is only available for Scanner and directory data service logs.</td>
</tr>
<tr>
<td><strong>Time range</strong> (drop-down)</td>
<td>Select a time range from the list or create a custom time range. If you have recently changed time zones on the Control Center, this change is not reflected immediately, but requires that you restart the appliance.</td>
</tr>
</tbody>
</table>
Table 22-15  Log view options (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component (drop-down)</td>
<td>Select a component for which to view logs: Scanner, Control Center,</td>
</tr>
<tr>
<td></td>
<td>Quarantine, or Directory Data Service.</td>
</tr>
<tr>
<td>Log type (drop-down)</td>
<td>Select a log type from the list.</td>
</tr>
<tr>
<td></td>
<td>See “Log types” on page 615.</td>
</tr>
<tr>
<td>Log action (drop-down)</td>
<td>Select the type of actions to display: System Events, Blocking Actions,</td>
</tr>
<tr>
<td></td>
<td>Message Actions, or All.</td>
</tr>
</tbody>
</table>

If a character in a Scanner log is not printable or is not ASCII, the sequence `\xAB` is printed instead of that character. `AB` is the hexadecimal value of the character. For example, a character with decimal value of 128 is displayed as `\x80`.

Since log information is dynamic, you can refresh the view at any time by clicking Display. See “Saving log files” on page 619.

See “Managing the log database size” on page 620.

To view log files

1. In the Control Center, click **Status > System > Logs**.
2. Under **Filter**, specify selection criteria for the log events that you want to view.
3. Click **Display**.

   The results of the filter appear on the Logs page.

Viewing the Control Center error log

You may want to periodically view the Control Center error log to troubleshoot issues. All errors that are related to the Control Center are written to the `BrightmailLog.log` file.

Each issue results in a number of lines in the error log. For example, the following lines are the result of Spam Quarantine receiving a message that is too large to handle:

```java
com.mysql.jdbc.PacketTooBigException:
Packet for query is too large (3595207 > 1048576)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1554)
at com.mysql.jdbc.MysqlIO.send(MysqlIO.java:1540)
at com.mysql.jdbc.MysqlIO.sendCommand(MysqlIO.java:1005)
at com.mysql.jdbc.MysqlIO.sqlQueryDirect(MysqlIO.java:1109)
at com.mysql.jdbc.Connection.execSQL(Connection.java:2030)
```
at com.mysql.jdbc.PreparedStatement.executeUpdate
(PreparedStatement.java:1596)
at org.apache.commons.dbcp.DelegatingPreparedStatement.executeUpdate
(DelegatingPreparedStatement.java:207)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate
(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLManager.handleUpdate
(Unknown Source)
at com.brightmail.dl.jdbc.impl.DatabaseSQLTransaction.create
(Unknown Source)
at com.brightmail.bl.bo.impl.SpamManager.create
(Unknown Source)
at com.brightmail.service.smtp.impl.SmtpConsumer.run
(Unknown Source)

See “About logs” on page 614.

To view the Control Center error log

1. In the Control Center, click Status > Logs.
2. In the Component drop-down list, select Control Center.
3. In the Log Files table, click BrightmailLog.log.
4. Open the log file or save it to your local disk.

Saving log files

Symantec Messaging Gateway lets you save log files. Log files are saved in .txt format.

When you save a log file, you can view and print the file with a text editor application. You can also email the file. You must have Full Administration rights or Manage Status and Logs view or modify rights to save a log file.

Scanner log files do not contain individual log file links like the Control Center logs. When you save a Scanner log file, the text file contains all of the detailed log items that appear on the Control Center page. The Control Center log requires that you save the Log files that you want individually.

To save log files

1. In the Control Center, click Status > System > Logs.
2. Create a log.
3. Do any of the following:

   To save a Scanner log file  
   
   Click Save Log.
To save a Control Center log

Do all of the following:

- In the Log Files column, click on the Log File that you want to save.
- In the File Download dialog box, click Save.

4 In the Save As dialog box, specify the file name and the location where you want to save the file, and click Save.

The default file name is LogDetails.txt.

5 In the Download Complete dialog box, click Close.

See “About logs” on page 614.

See “Viewing log files” on page 617.

Managing the log database size

The Control Center log database acquires log data from Scanners at regularly scheduled intervals. Depending on your environment and the log level that you specify, the log database can quickly increase to an unmanageable size. To prevent expansion, Symantec Messaging Gateway provides controls for specifying a maximum database size (the default is 50 MB). It also provides a log Expunger utility which purges older logs and prevents the database from exceeding the set limit (the default setting is daily). Users may also create custom configurations to meet specific or temporary needs.

Note: The settings you specify here should take into consideration the log levels you set. For example, if you have a log level that produces high volumes of log data (such as Debug level), you may want to temporarily increase the database size and log purge rate. When you resume to normal log levels, you can change these settings back.

See “Configuring log levels” on page 622.

See “About logs” on page 614.

See “About log disk space alerts” on page 625.

Note: If necessary, you can also manually purge files from the log database.

See “Manually deleting log files” on page 624.
### Table 22-16 Log database size control options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum log size</td>
<td>Specifies the maximum size of the database log. The maximum log size is enforced when the Log Expunger runs.  The maximum log size may be exceeded temporarily until the next Log Expunger process runs. The default value is 50 MB.</td>
</tr>
<tr>
<td>Days to store log data before deleting</td>
<td>Specifies the number of days that log files are retained in the database log before they are purged. The default value is 7.</td>
</tr>
<tr>
<td>Log Expunger frequency</td>
<td>Specifies how frequently the Expunger utility runs. The Log Expunger deletes older log files to enforce the maximum log size. The default setting is Every day.</td>
</tr>
<tr>
<td>Log Expunger start time</td>
<td>Specifies the time in which the Expunger starts. The time is based on a 24-hour clock. For example, 23:00 is 11:00 P.M. The default setting is 02:00 (2:00 A.M.). You can check the status of your scheduled task from the Status &gt; Scheduled Tasks page. See &quot;About scheduled tasks&quot; on page 648.</td>
</tr>
</tbody>
</table>

**Note:** When the Log Expunger runs, it deletes log entries in the log database. It does not compact the database. To compact the database and decrease its size, Symantec Messaging Gateway runs an optimization process. This process occurs automatically based on disk usage, so you do not need to configure it. However, because the optimization process is processor-intensive, it normally runs during off-peak hours (the default setting is 2:00 A.M.). So the Expunger may delete rows from the log database, but the size of the database does not decrease until the optimizer runs.

**Note:** You must have Full Administration or Modify rights to change log database settings. See "Administrator rights" on page 661.

**To manage the log database size**

1. In the Control Center, click Administration > Settings > Logs.
2. Click the Local tab.
3 Under **Database Log Storage Limits**, check **Maximum log size**.

4 In the adjacent box, type the maximum size that you want to allocate for the log database.

5 In the **Days to store log data before deleting** box, type the number of days to store log data.

6 Under **Log Expunger**, choose a frequency and a start time when the Control Center runs the Log Expunger to delete log data.

   The hour drop-down list uses 24-hour format. For example, 23:00 is 11:00 P.M.

7 Click **Save**.

### Configuring log levels

You can specify the amount of log data to store for Scanners components. You can set Scanner log levels in five increments from error level to debug level. Each succeeding log level after errors includes log data for all of the previous log levels.

See “About logs” on page 614.

For example, if you set the log level for Conduit to the notice level, Conduit errors and warnings events are stored also. You can only view Conduit log data for the notice, errors, and warnings events. Conduit information and debug events are not stored and are not viewable in the Control Center or syslog in this example.

The level that you select should contain the type of information that you want to monitor. Avoid the information and debug log levels because they can consume large amounts of disk space and require extensive processing resources to create log reports.

You can modify logging levels at any time. For instance, if you need to troubleshoot a problem, you can increase the logging level. When you resolve the problem, you can return the log level to its previous setting.

---

**Note:** You may need to restart Scanner services after changing log levels.

---

**Warning:** High logging levels are those that produce high volumes of data but tend to be of a non-urgent nature. Low logging levels are those that produce lower volumes of data but tend to be of a more urgent nature.

High log levels (such as debug) can affect the logging process. If the Scanner disk cache nears or reaches capacity, the system switches to reduced logging mode or halted logging mode. In reduced mode, only urgent logs are copied to the Control Center log database. In halted mode, no log files are copied to the log database. You must clear disk cache, purge log database, and adjust log levels to resume normal logging.
See “About log disk space alerts” on page 625.

See “About maintaining adequate disk space” on page 703.

See “Managing the log database size” on page 620.

See “Clear disk space checklist” on page 625.

Table 22-17 lists the available log levels.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Provides the most important information.</td>
</tr>
<tr>
<td></td>
<td>This level provides the least amount of log information.</td>
</tr>
<tr>
<td>Warnings</td>
<td>Provides warning and errors level data.</td>
</tr>
<tr>
<td></td>
<td>This level is the default log level for all Scanner components (local and remote).</td>
</tr>
<tr>
<td>Notices</td>
<td>Provides notice information and warnings and errors level data.</td>
</tr>
<tr>
<td>Information</td>
<td>Provides informational messages and warnings, errors, and notices data.</td>
</tr>
<tr>
<td>Debug</td>
<td>Provides debugging information and warnings, errors, notices, and information data.</td>
</tr>
<tr>
<td></td>
<td>This level provides the greatest amount of log information.</td>
</tr>
</tbody>
</table>

**Warning:** Consult Symantec Technical Support before you use this log level.

See “Log types” on page 615.

You can specify log levels for local Scanners and remote Scanners. You can configure different logging levels for each local Scanner, or you can propagate settings to all of your local Scanners. You must have Full Administration rights and Manage Status and Logs modify rights to change log levels. You cannot change the log levels for the Control Center and Spam Quarantine.

See “Viewing log files” on page 617.

To configure log levels for specific local Scanner

1. In the Control Center, click **Administration > Settings > Logs**.
2. Click the **Local** tab.
3. Under **Local Logging**, check **Enable local logs for components of the following host** and click a host for which to store local logs.
4 Use the **Component Local Log Levels** drop-down lists to select the log level for each component.

5 Click **Save**.

**To configure log levels for remote Scanners**

1 In the Control Center, click **Administration > Settings > Logs**.

2 Click the **Remote** tab.

3 Under **Remote Logging**, check **Enable Syslogs for the following host** and click a host from which to send log data.

4 Under **Syslog Settings**, specify the host name, port, and protocol for the remote syslog.

5 Use the **Component Remote Log Levels** drop-down lists to select the log level and the facility for each component.

   See “Configuring remote logging to syslog” on page 628.

6 Click **Save**.

**Manually deleting log files**

The log Expunger utility lets you schedule purges of the log database at regularly recurring intervals. However, in some cases you may want to delete logs manually from the log database. You can clear Scanner log files and directory data service log files from the Control Center log database on the **Status > System > Logs** page. You can also manually delete log files using the **delete** command.

See **delete** on page 752.

---

**Note:** Deleting Scanner and directory data service log files from the Control Center log database does not remove the original log files from the Scanner appliance. To delete the original Scanner and directory data service log files, you must use the command line interface.

See “Clear disk space checklist” on page 625.

---

See “Managing the log database size” on page 620.

See “About log disk space alerts” on page 625.

See “Viewing log files” on page 617.

You must have full Administration, Manage Status, or Logs modify rights to manually delete logs.
To manually delete log files

1. In the Control Center, click **Status > System > Logs**.

2. In the Filter section, select **Scanner** or **Directory Data Service** from the component drop-down menu.

3. Click **Clear All Scanner Logs** for Scanner logs or **Clear All DDS Logs** for directory data service logs.

**About log disk space alerts**

Symantec Messaging Gateway includes an enhanced logging feature that allows system administrators to enable alerts when logging disk space on Scanners nears or reaches capacity. When the default threshold levels are reached, the system shifts to a reduced or halted logging mode and sends an email notification to the specified administrator. You will need to enable the low disk space alerts to receive this notification.

See “Configuring alerts” on page 688.

A logging mode change is typically caused by a change in log levels in the Control Center. If an administrator sets the log level to a level that yields a high volume of data (such as the Debug level), the Control Center may not be able to copy data files from the Scanner to the log database at a rate that keeps pace with the incoming data feeds. Log files remain on the Scanner and disk space quickly fills up.

See “Managing the log database size” on page 620.

When the system shifts to reduced logging mode, only urgent log levels (e.g., Errors and Warnings) are recorded. Log levels that produce excess data of a non-urgent nature (e.g., Notices, Information, and Debug) are suspended until space is freed on the disk. When a halted situation occurs, all log levels are suspended. Normal logging resumes only after the log files have been transferred off the disk.

**Note:** Reduced and halted logging only applies to appliances operating as a Scanner or Directory Data Service (DDS).

See “Clear disk space checklist” on page 625.

**Clear disk space checklist**

The following is a list of options for clearing disk space on the Control Center and Scanner appliances. Use these options if you have determined that low disk space availability currently affects system performance.

See “About log disk space alerts” on page 625.

See “About logs” on page 614.
See "Manually deleting log files" on page 624.

**Note:** Some log files are part of the normal functioning of the appliance that should not be deleted. If you notice a large number of files in these directories or any unusually large files in these directories you should consult with Symantec support prior to deleting any files. Using a subset of these actions may be sufficient to restore the disk to a working condition. Delete data conservatively.

<table>
<thead>
<tr>
<th>Control Center stored data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantined mail</td>
<td>Click Delete All on the Spam &gt; Quarantine &gt; Email Spam page to delete all spam messages that are stored in the Spam Quarantine.</td>
</tr>
<tr>
<td>Content filtering incidents</td>
<td>Old content filtering incidents can be deleted from Content &gt; Incident Management &gt; [Content Incident management folder]. Click Delete or Delete All to delete contents.</td>
</tr>
<tr>
<td>Reporting data</td>
<td>Click Delete Data Now on the Administration &gt; Settings &gt; Reports page to delete all reporting data and dashboard data.</td>
</tr>
<tr>
<td>Scanner data that is stored in the log database</td>
<td>On the Status &gt; System &gt; Logs page, select Scanner from the Component list and click Clear All Scanner Logs to delete Scanner logs from the log database.</td>
</tr>
<tr>
<td>Directory data service (DDS) data that is stored in the log database</td>
<td>On the Status &gt; System &gt; Logs page, select Directory Data Service from the Component list and click Clear All DDS Logs to delete directory data service logs.</td>
</tr>
<tr>
<td>Database backups that are stored locally</td>
<td>Backups are stored on the appliance in /data/backups/ or /data/backups/tmp/. Click Delete on the Administration &gt; Hosts &gt; Version &gt; Restore/Download page to delete the old backups that are stored locally on the appliance.</td>
</tr>
<tr>
<td>Old software update data</td>
<td>Files in /data/apt/ directory and its subdirectories. To delete old software update data, type the following on the command line: delete sudata</td>
</tr>
</tbody>
</table>

You can delete data files using the command line.

See “Administering Symantec Messaging Gateway through the command line” on page 730.
See delete on page 752.
See mta-control on page 794.
### Table 22-19  Scanner data

<table>
<thead>
<tr>
<th>Scanner stored data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core files</td>
<td>Files in <code>/data/scanner/jobs/</code> directory and its subdirectories. To delete core files, type the following on the command line: <code>delete cores</code></td>
</tr>
<tr>
<td>Log files</td>
<td>Files in <code>/data/logs/</code> directory and its subdirectories that the Control Center has not retrieved. To delete all log files, type the following on the command line: <code>delete alllogs</code></td>
</tr>
<tr>
<td>Stats files</td>
<td>Files in the <code>/data/scanner/stats/</code> directory that the Control Center has not retrieved. To delete stats files, type the following on the command line: <code>delete alldata</code> &lt;br&gt;This command deletes other data in addition to the stat files. Only use <code>delete alldata</code> if necessary.</td>
</tr>
<tr>
<td>Tmp files</td>
<td>Files in <code>/tmp/</code> and <code>/var/tmp/</code> directories and their subdirectories. To delete individual files, type the following on the command line: <code>delete file /tmp/filename</code> or <code>delete file /data/tmp/filename</code></td>
</tr>
<tr>
<td>Audit logs</td>
<td>Files in the <code>/data/logs/scanner/</code> directory whose names start with <code>audit_</code>. To delete audit logs, type the following on the command line: <code>delete mallogs</code></td>
</tr>
<tr>
<td>Old messages that are stuck in inbound, outbound, and delivery mail queues</td>
<td>Files in <code>/data/mta/queues/</code> directory and its subdirectories. To delete the messages that are stuck in the queues, type the following on the command line: <code>mta-control all delete-all-msgs</code></td>
</tr>
<tr>
<td>Messages that are stored in bad-messages folder</td>
<td>Files in <code>/data/mta/bad-messages/</code>. To delete bad messages, type the following on the command line: <code>mta-control all bad-msg-delete all</code></td>
</tr>
<tr>
<td>Old software update data</td>
<td>Files in <code>/data/apt/</code> directory and its subdirectories. To delete old software update data, type the following on the command line: <code>delete sudata</code></td>
</tr>
</tbody>
</table>

### Monitoring logs on a remote server

Table 22-20 describes the ways that you can monitor logs on a remote server. You can perform these tasks as needed in any order.
Table 22-20 Monitor logs on a remote server

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Symantec Messaging Gateway to send Scanner log data to a remote syslog.</td>
<td>Some Scanner logs can be sent to syslog on a remote server. Ensure that the remote syslog is configured to match the settings in the Control Center. You must enable either local logging, remote logging, or both. See “Configuring remote logging to syslog” on page 628.</td>
</tr>
<tr>
<td>Familiarize yourself with the standard prefixes for Scanner logs.</td>
<td>You can All Scanner log messages that are sent to the remote syslog take a standard form. See “Standard prefix for Scanner logs sent to remote syslog” on page 629.</td>
</tr>
</tbody>
</table>
| Familiarize yourself with log formats. | The following topics describe the various log formats that are available:  
  ■ See “Log format of boot.log, cron, message, and secure components for remote syslog” on page 630.  
  ■ See “Log format of Conduit, Brightmail Client, Brightmail Engine, and JLU Controller for remote syslog” on page 630.  
  ■ See “Log format of mail transfer agent for remote syslog” on page 632.  
  ■ See “Log format of message audit logs for remote syslog” on page 633. |

Configuring remote logging to syslog

Some Scanner logs can be sent to syslog on a remote server. Ensure that the remote syslog is configured to match the settings in the Control Center. You must enable either local logging, remote logging, or both.

To configure remote logging to syslog

1 In the Control Center, click Administration > Settings > Logs.
2 Click the Remote tab.
3 Click Enable Syslogs for the following host and click a host to send log data from that host to a remote syslog.
4 In the Host field, specify the syslog server's IP address.
5 In the Port field, specify the port on the syslog server that handles log data.
6 In the Protocol field, specify the syslog protocol: UDP or TCP.
7 Under Component Remote Log Levels, specify the logging level and facility for each component.
8 Click Enable message logs to send message logs to the remote syslog.
9  Click a **Message log facility**.

10  Click **Apply these Remote Logging settings to all hosts** if wanted.

11  Click **Save** to save your changes.

Log components may need to be restarted.

### Standard prefix for Scanner logs sent to remote syslog

You can configure Symantec Messaging Gateway to send Scanner log data to a remote syslog. All Scanner log messages that are sent to the remote syslog take the following form:

<table>
<thead>
<tr>
<th>Date and time</th>
<th>Facility Level</th>
<th>IP address</th>
<th>Original log message</th>
</tr>
</thead>
</table>

- **Date and time**: Date in the format month-date-year. Time in the format hour:minute. The time is in 24-hour clock notation.
- **Facility Level**: The facility, a period, and the log level. The facility designates the facility on the remote syslog to which the log data is sent. The log level is the log level configured on the Scanner.
- **IP address**: IP address of the Symantec Messaging Gateway host sending the log message.
- **Original log message**: The original log message as it would appear on the Scanner. The format of this portion depends on the log component.

The first three columns make up a standard prefix that appears before all log messages sent to a remote syslog. The following is a log message for one event as it would appear on the remote syslog.

```
scanner1 jlu-controller: [Brightmail] (INFO:21145.3071248064): [54038] AV definitions are up-to-date.
```

See "Configuring remote logging to syslog" on page 628.
Log format of boot.log, cron, message, and secure components for remote syslog

You can configure Symantec Messaging Gateway to send Scanner log data to a remote syslog. If remote syslog is enabled, log data for the boot.log, cron, message, and secure components is sent to the remote syslog. These are standard UNIX log components. Log data for these components is sent to the standard syslog facility on the remote syslog. The log level for these components cannot be configured. All log messages that are sent to a remote syslog have the same prefix text.

See “Standard prefix for Scanner logs sent to remote syslog” on page 629.

The log messages that are sent to the remote syslog take the following form:

<table>
<thead>
<tr>
<th>Standard prefix</th>
<th>Date and time</th>
<th>Scanner host name</th>
<th>Process[PID]:</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, time, log level, and IP address</td>
<td>Jan 15 11:51:33</td>
<td>scanner1</td>
<td>syslog-ng[25257]:</td>
<td>syslog-ng version 1.6.5 starting</td>
</tr>
</tbody>
</table>

The following is a log message for one event as it would appear on the remote syslog.


Log format of Conduit, Brightmail Client, Brightmail Engine, and JLU Controller for remote syslog

You can configure Symantec Messaging Gateway to send Scanner log data to a remote syslog. All log messages that are sent to a remote syslog have the same prefix text.

See “Standard prefix for Scanner logs sent to remote syslog” on page 629.
The following table contains sample log messages for the following components in the same order listed:

- Conduit
- Brightmail Client
- Brightmail Engine
- JLU Controller

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, time, facility, log level, and IP address</td>
<td>Jan 15 11:34:51</td>
<td>scanner1</td>
<td>conduit: [src/rda_controller.cc: 319:586:initialize]</td>
<td>DEBUG: 19713:3071461056)</td>
<td>Appending HTTP header: 'Spamwall_ID: (null)'</td>
</tr>
<tr>
<td></td>
<td>Jan 15 11:37:05</td>
<td>scanner1</td>
<td>bmserver: [src/rhk_hint.c: 319:497:parse]</td>
<td>DEBUG: 20516:3066324672)</td>
<td>rhk hint for rule 43731290 has been successfully parsed</td>
</tr>
<tr>
<td></td>
<td>Jan 15 11:38:05</td>
<td>scanner1</td>
<td>jlu_controller: [Brightmail] 3071248064)</td>
<td>INFO: 54038</td>
<td>AV definitions are up-to-date.</td>
</tr>
</tbody>
</table>
The following is a log message for one event as it would appear on the remote syslog.

```
[src/rhk_hint.c:497:rhk_hint_parse] rhk hint for rule 43731290 has been successfully parsed
```

**Log format of mail transfer agent for remote syslog**

You can configure Symantec Messaging Gateway to send Scanner log data to a remote syslog. If remote syslog is enabled, MTA log data is sent to the remote syslog. All log messages that are sent to a remote syslog have the same prefix text.

See “Standard prefix for Scanner logs sent to remote syslog” on page 629.

The MTA log messages that are sent to the remote syslog take the following form:

<table>
<thead>
<tr>
<th>Standard prefix</th>
<th>Date and time</th>
<th>Scanner host name</th>
<th>Process: [PID]</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, time, facility, log level, and IP address</td>
<td>Jan 15 11:39 scanner1</td>
<td>ecelerity: [21911]</td>
<td>THPL-00150: Defer_queue_suspect_bad_message thread -1696945232 starting</td>
<td></td>
</tr>
</tbody>
</table>
The following is a log message for one event as it would appear on the remote syslog.


Log format of message audit logs for remote syslog

You can configure Symantec Messaging Gateway to send message audit log data to a remote syslog. All log messages sent to a remote syslog have the same prefix text.

See “Standard prefix for Scanner logs sent to remote syslog” on page 629.

The message audit log messages sent to the remote syslog take the following form:

<table>
<thead>
<tr>
<th>Standard prefix</th>
<th>Date and time</th>
<th>Scanner host name</th>
<th>Process:</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, time, facility, log level, and IP address</td>
<td>Jan 15 15:42 scanner1 ecelerity:</td>
<td>1230876822</td>
<td>0ad9200d-b7b61ae00000 5b81-00-495db08c9df2</td>
<td>DELIVER</td>
</tr>
</tbody>
</table>
The following is a log message for one event as it would appear on the remote syslog.

scanner1 ecelerity: 1230876822|0ad9200d-b7b61ae000005b81-00-495db08c9df2|DELIVER|10.217.32.13|rashu1@symantecs.org

Working with the message audit log and message queue

Table 22-21 describes the ways that you can monitor the SMTP status with the message audit log and message queue. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about Symantec Messaging Gateway message audit logging.</td>
<td>Symantec Messaging Gateway provides a message auditing component that lets you search for messages and find out what has happened to them. When enabled, the message audit log provides administrators with a trail of detailed information about every message that has been accepted and processed by a Scanner. Auditing information is used to track what decisions were made within a single Scanner framework. The message audit log is not intended to replace debug or information level logging. Unlike standard Scanner logging, the message audit log provides information specifically associated with a message.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Familiarize yourself with the audit log format and events.</td>
<td>Each software component that writes message audit information writes to its own audit log. Each entry in the audit log consists of at least three fields. The audit log event ID describes the type of audit event that is logged. Some event IDs are followed by parameters. Each software component uses its own log parameters.</td>
</tr>
<tr>
<td>Enable or disable message audit logging.</td>
<td>By default the message audit log is enabled for local logging and disabled for remote logging. This feature needs to be enabled before any auditing information is available for viewing or searching. Storage for message auditing can become large, and searching the logs can create high demand for Scanner processing time.</td>
</tr>
<tr>
<td>Locate a specific message in the message audit log.</td>
<td>A query facility is provided to search the log to determine if one or more messages meet the criteria for the message you want to find.</td>
</tr>
<tr>
<td>Export message audit log data into a .csv file.</td>
<td>To view a CSV file that contains double-byte characters in Microsoft Excel, specify a comma-delimited, UTF-8 file in the MSExcel Text Import Wizard. Alternatively, you can open the CSV file in a text editor that can convert UTF-8 to Unicode, such as Notepad, and save the CSV file as Unicode.</td>
</tr>
<tr>
<td>Learn more about message queues.</td>
<td>A message queue is a temporary holding area for messages before they reach their destination. The messages queues are: inbound, outbound, and delivery. The message queue size fluctuates based on mail flow. If a queue continually grows without decreasing in size, there is a problem with message delivery.</td>
</tr>
<tr>
<td>View the messages that are queued at any time to troubleshoot an issue.</td>
<td>At a minimum, you must specify the host and the queue that you want to view: inbound, outbound, or delivery. Symantec Messaging Gateway also has filtering options that let you further customize the queued messages to view. Based on your filter criteria, Symantec Messaging Gateway displays the messages that are in that queue at that moment. If there is an error associated with the message, it appears in the Message column.</td>
</tr>
</tbody>
</table>
### Table 22-21  Work with the message audit log and message queue (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reroute a message in the message queue.</td>
<td>You can search for messages in the delivery queue from a specific route or set of routes. You can also reroute messages from one route to a different route. See “Rerouting messages in the delivery queue” on page 643.</td>
</tr>
<tr>
<td>Delete a message from the message queue.</td>
<td>When you view a message queue, you may find that a message has blocked the queue. You can delete that message so that the messages behind it can pass through the queue. Once you delete a queued message, you cannot retrieve it. You can delete all of the messages in a queue. See “Deleting queued messages” on page 644.</td>
</tr>
<tr>
<td>Stop the mail flow.</td>
<td>You may need to stop the flow of mail (for example, before you flush a message queue). Ensure that you understand the implications before you stop the mail flow. See “Stopping the mail flow” on page 645.</td>
</tr>
<tr>
<td>Flush the message queue.</td>
<td>When you flush a message queue, you instruct the MTA to try to resend the messages that were deferred due to delivery problems. You may want to flush your inbound, outbound, and delivery email queues before you turn off an appliance. See “Flushing message queues” on page 646.</td>
</tr>
<tr>
<td>Monitor the status of the message queue to determine if the message queue is clogged.</td>
<td>You can view the number of queued messages and the size of the queues for all of your message queues. You can set the maximum size for each message queue and decide whether to defer messages when the queue is full on the SMTP Advanced Settings page. See “Monitoring message queue size and volume” on page 647.</td>
</tr>
<tr>
<td>Resolve issues with the message queue.</td>
<td>When a message queue becomes too large, Symantec Messaging Gateway can become unresponsive or crash. To attempt to deter this issue, by default, Symantec Messaging Gateway defers new messages when the queue is full. As a best practice, you should leave this setting enabled and keep queue limits below the recommended default thresholds. See “Troubleshooting the message queue” on page 647.</td>
</tr>
</tbody>
</table>
To enable or disable the Message Audit Log for local logging

1. In the Control Center, click **Administration > Settings > Logs**.
2. On the Local tab, under Message Audit Logs, check or uncheck **Enable message logs**.
3. Click **Save**.

To enable or disable the Message Audit Log for remote logging

1. In the Control Center, click **Administration > Settings > Logs**.
2. On the Remote tab, under Message Audit Logs, check or uncheck **Enable message logs**.
3. Select a **Message log facility** from the drop-down list.
4. Click **Save**.

Searching for a message in the Message Audit Log

A query facility is provided to search the log to determine if one or more messages meet the criteria for the message you want to find.

The **Status > SMTP > Message Audit Logs** page enables you to specify either one or two criteria and related supplementary information as follows:

- **Host**: One or more Scanners running the Symantec Messaging Gateway software. In order to find all details about a message, search on all attached Scanners.
- **Time range**: Period of time for the search to query the audit log. While it is possible to search for longer periods, it is recommended that message searches not exceed one week.
- **Mandatory filter**: Select the type of information for filtering messages. See Table 22-22.
- **Mandatory filter value**: Enter a string that corresponds to the Mandatory filter type you selected. For example, if you chose to filter messages by sender, enter a valid email address here.
- **Optional filter**: Select from the list of optional filtering criteria. See Table 22-23.
- **Optional filter value**: If appropriate, enter a string or choose a value that corresponds to the Optional filter type you selected. For example, if you chose to filter messages by Connection IP, enter a valid IP address here. Or, if you choose to filter messages by Action taken, select the action for which you want to find messages.
- **Clear Filters**: Clear the current filtering criteria from memory.
- **Display Filtered**: Search for and display messages that fit your criteria.
Table 22-22 describes the items you can choose for your single required filter.

Table 22-22  Choices for the mandatory search criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Name of the message sender. Specify &lt;&gt; to filter for messages that do not contain Sender names.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Name of the message recipient.</td>
</tr>
<tr>
<td>Subject</td>
<td>Message subject.</td>
</tr>
<tr>
<td>Audit ID</td>
<td>Unique identifier generated by Symantec Messaging Gateway and included as a message header.</td>
</tr>
<tr>
<td>Connection IP</td>
<td>IP address of the connecting server. In cases where Symantec Messaging Gateway rejects an IP connection, this results in a row with the sender identified as none. Message details consist of the IP address and the reason for rejection. Symantec Messaging Gateway supports IPv4 addresses and IPv6 addresses.</td>
</tr>
<tr>
<td>Logical IP</td>
<td>Logical IP address of the connecting server.</td>
</tr>
<tr>
<td></td>
<td>The logical connection IP is used for deployments in which you have internal mail servers that forward messages to Symantec Messaging Gateway server. The logical connection IP address is the address of the first non-internal server connection.</td>
</tr>
<tr>
<td></td>
<td>The logical connection IP address is derived from the &quot;Received:&quot; headers of the message content. Symantec Messaging Gateway uses this IP address for filtering purposes. Based on your deployment, this address may be identical to the &quot;Accepted from&quot; IP address.</td>
</tr>
<tr>
<td></td>
<td>When you select <strong>Logical IP</strong>, you may specify IPv4 addresses, IPv6 addresses, or IPv6 CIDR ranges. CIDR ranges are only accepted where the prefix is a multiple of 4.</td>
</tr>
</tbody>
</table>

Table 22-23 describes the items you can choose for your single optional filter.

Table 22-23  Choices for the optional search criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Name of the message sender. Specify &lt;&gt; to filter for messages that do not contain Sender names.</td>
</tr>
<tr>
<td>Authenticated sender</td>
<td>Name of an authenticated sender.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Name of the message recipient.</td>
</tr>
<tr>
<td>Subject</td>
<td>Message subject.</td>
</tr>
<tr>
<td>Criteria</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Message ID</td>
<td>Unique identifier typically generated by the email software initiating the sending of the message and included as a message header. Spammers have used this header to mask the identity of a message originator.</td>
</tr>
<tr>
<td>Verdict</td>
<td>The verdict and/or other characteristics of a message. When this filter option is selected, a list of possible verdicts appears in the <strong>Optional filter value</strong> drop-down list. Use these values to filter messages that resulted in a given verdict. For example, you can set the <strong>Optional filter value</strong> to <em>The message is a newsletter</em>.</td>
</tr>
<tr>
<td>Untested verdict</td>
<td>An available verdict for which the Scanner did not test. A drop-down list of verdict choices is provided.</td>
</tr>
</tbody>
</table>
| Action taken     | What happened to the message. When this filter option is selected, a list of possible actions appears in the Option filter value drop-down list. Use these values to filter messages that triggered policies that applied the given action.  
If you select Reject message from the Option filter value drop-down list, the reason for rejection appears in the message detail.  
  - Rejected message for a nonlocal recipient  
  - Rejected message for exceeding size limit  
  - Rejected message by MTA  
  - Reject messages failing bounce attack validation  
  - Reject invalid recipients rejected message for exceeding size limit  
  - All recipients are invalid |
| Connection IP    | Connection IP used to receive the message. Symantec Messaging Gateway supports IPv4 addresses and IPv6 addresses.                             |
| Logical IP       | Logical IP address of the connecting server.  
The logical connection IP is used for deployments in which you have internal mail servers that forward messages to Symantec Messaging Gateway server. The logical connection IP address is the address of the first non-internal server connection.  
The logical connection IP address is derived from the "Received:" headers of the message content. Symantec Messaging Gateway uses this IP address for filtering purposes. Based on your deployment, this address may be identical to the "Accepted from" IP address.  
When you select **Logical IP**, you may specify IPv4 addresses, IPv6 addresses, or IPv6 CIDR ranges. CIDR ranges are only accepted where the prefix is a multiple of 4. |
Table 22-23  Choices for the optional search criteria (continued)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target IP</td>
<td>IP address of the message destination.</td>
</tr>
<tr>
<td>Policy group</td>
<td>Name of the group (either the recipient's group or the sender's group) that determined which filter policy applied to the message.</td>
</tr>
<tr>
<td>Filter policy</td>
<td>Name of the filter policy applied to the message.</td>
</tr>
<tr>
<td>Virus</td>
<td>Name of the virus attached to the message.</td>
</tr>
<tr>
<td>Attachment</td>
<td>Name of a message attachment.</td>
</tr>
<tr>
<td>Suspect attachment</td>
<td>Name of a message attachment that triggered a content filtering policy.</td>
</tr>
<tr>
<td>Reason for unscannable verdict</td>
<td>Reason that the message matched the &quot;If a message is unscannable for malware and content filtering for any reason&quot; condition. A drop-down list of unscannable reasons is provided.</td>
</tr>
<tr>
<td>Source</td>
<td>Whether the message is internal or external.</td>
</tr>
<tr>
<td>Disarmed content</td>
<td>Whether the message's attachments contain potentially malicious content.</td>
</tr>
</tbody>
</table>

While searching, the following rules are used:

- No more than 1,000 messages are allowed per search on each Scanner being searched.
- Freeform text fields are non-case-sensitive substring searches.

**Note:** The Message Audit Log provides information on each message received by each recipient. For example, if the same message is received by 10 recipients, you see 10 entries in the Message Audit Log. To reach the limit of 1,000 messages returned, Symantec Messaging Gateway counts multiple entries for the different recipients of the same message as one message.

Email messages that fail delivery are tracked as delivery failures in the Message Audit Log. For example, messages to non-existent users that bounce are considered delivery failures. Delivery failures are indicated with a Delivery Failure heading on the Audit Logs page in the Delivery section. In addition to being indicated on the Audit Logs page, undelivered messages are logged with the new DELIVERY_FAILURE audit log event. DELIVERY_FAILURE events are logged in the following format: utc|uid|DELIVERY_FAILURE|recipient|reason

The **Actions** column indicates actions taken by the Scanner on messages, but does not indicate actions taken by administrators or users on messages. For example, if an administrator or user releases a message from Spam Quarantine, this activity is listed under **Spam Quarantine**, not **Actions**.
To search the message audit log and view message details

1. In the Control Center, click **Status > SMTP > Message Audit Logs**.
2. Select the Scanner whose logs you wish to search from the **Hosts** drop-down list, or select **All Scanners**.
3. Complete the desired search criteria.
4. Click **Display Filtered**.
   
   Use the **Entries per page** drop-down list to specify the number of records to show per page. Use the **Display _ of _** drop-down list to choose a range of data to display.
5. Click a message recipient in the **To** column to view processing details on that message.

To search the message audit log for content filtering incidents

1. In the Control Center, click **Status > SMTP > Message Audit Logs**.
2. Select the Scanner whose logs you want to search from the **Host** drop-down list, or select **All Scanners**.
3. Choose a selection from the **Mandatory filter** drop-down list and enter an appropriate value in the **Mandatory filter value** field.
4. Choose **Action taken** from the **Optional filter** drop-down list.
5. Choose either **Create an informational incident** or **Create a quarantine incident** from the **Optional filter value** drop-down list.
6. Click **Display Filtered**.
   
   Use the **Entries per page** drop-down list to specify the number of records to show per page. Use the **Display _ of _** drop-down list to choose a range of data to display.
7. Click a message recipient in the **To** column to view processing details on that message.

To view the TLS encryption delivery status of a message in the message audit log

1. Locate the message in the message audit log.
2. Expand **Recipient data > Delivery**.
3. Click **Details**.

See “How the Message Audit Log helps to fine-tune and troubleshoot content filtering policies” on page 351.

Exporting Message Audit Log data

After you select your filter criteria and click **Display Filtered**, you can export the log data to a CSV file.
To view a CSV file that contains double-byte characters in Microsoft Excel, specify a comma-delimited, UTF-8 file in the MS Excel Text Import Wizard. Alternatively, you can open the CSV file in a text editor that can convert UTF-8 to Unicode, such as Notepad, and save the CSV file as Unicode.

To export Message Audit Log data

1. In the Control Center, click **Status > SMTP > Message Audit Logs**.
2. Select the Scanner whose logs you want to search from the **Host** drop-down list, or select **All Scanners**.
3. Complete the search criteria.
4. Click **Display Filtered**.
5. Click **Export CSV**.
7. Click the **CSV Delimiter** drop-down list and choose a delimiter for the CSV file. Symantec Messaging Gateway places the chosen delimiter between entries in the file.

About message queues

A message queue is a temporary holding area for messages before they reach their destination. The messages queues are: inbound, outbound, and delivery. The message queue size fluctuates based on mail flow.

If a queue continually grows without decreasing in size, there is a problem with message delivery. You can view the messages that are queued at any time to troubleshoot an issue. The message queue provides details about why the MTA could not deliver a message, how many times delivery was attempted, and when the next delivery attempt is scheduled.

See “Monitoring message queue size and volume” on page 647.
See “Viewing queued messages” on page 643.
See “Deleting queued messages” on page 644.
See “Stopping the mail flow” on page 645.
See “Flushing message queues” on page 646.
See “Troubleshooting the message queue” on page 647.
Viewing queued messages

You can view the messages that are in the message queues. At a minimum, you must specify the host and the queue that you want to view: inbound, outbound, or delivery. Symantec Messaging Gateway also has the filtering options that let you further customize the queued messages to view. Based on your filter criteria, Symantec Messaging Gateway displays the messages that are in that queue at that moment.

The message queue provides details about why the MTA cannot deliver a message, how many times it attempted to deliver the message, and when the next delivery attempt is scheduled.

You may have a situation in which you want to determine if a specific message is in the queue. You can filter for messages to or from specific email addresses. For the delivery queue only, you can also search for messages from a specific route or set of routes. You can also reroute messages from one route to a different route.

See “Rerouting messages in the delivery queue” on page 643.

You can perform wildcard searches for senders (From field) or recipients (To field). These searches are case sensitive. The asterisk (*) and question mark (?) wildcard characters are supported. For the delivery queue you can also perform wildcard searches for custom routes.

If you do not stop mail flow, the messages in the queue can continually fluctuate as new messages enter the queue and older messages exit. You can refresh the view as needed.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view message queues.

To view queued messages

1. In the Control Center, click Status > SMTP > Message Queues.
2. On the Message Queues page, select a host and queue.
3. Type search values for the fields that are provided.
4. Click Display Filtered.
5. To clear the To and From fields to begin a new search, click Clear Filters.
   - All of the other drop-down menu selections that you made are retained.

To refresh the view

- On the Message Queues page, click Refresh.

See “Viewing the Content Analysis queue” on page 468.

Rerouting messages in the delivery queue

You can search for messages in the delivery queue from a specific route or set of routes. You can also reroute messages from one route to a different route.
See “Viewing queued messages” on page 643.

You can perform wild card searches for senders, recipients, or custom routes. Search is not case sensitive.

To reroute messages in the delivery queue

1. In the Control Center, click **Status > SMTP > Message Queues**.
2. On the Message Queues page, select a host and the **Delivery** queue.
3. In the **Route** field, select one of the following:
   - **Default Local Route**: The default route for local domains.
   - **Default Non-local Route**: The default route for non-local domains.
   - **Control Center**: The route this Scanner uses to communicate with the Control Center.
   - **DLP**: The route this Scanner uses to communicate with a Symantec Network Prevent server.
   - **Custom**: A route that you specify in the **Custom route** field. After you select **Custom**, the **Custom route** field appears.

4. If you selected **Custom**, enter the hostname or IP address:port for the route you want to search for in the **Custom route** field. If you made another selection, skip this step.
   - If you specify a CIDR block that returns messages from more than one route, you cannot reroute messages. If your filtered messages are all from the same route, the **Reroute All** button becomes active.
5. Optionally, complete additional search fields.
6. Click **Display Filtered**.
7. Under **Reroute all the messages originally destined for the filtered route**, type the hostname, IP address:port, CIDR block, or subnet for the new route in the **New Route** field.
8. If you typed a hostname, you can check **MX Lookup**, if desired.
9. Click **Reroute All**.

Deleting queued messages

When you view a message queue, you may find that a message has blocked the queue. You can delete that message so that the messages behind it can pass through the queue.
You can access the messages that are queued, and save them, via the mta-control command. See mta-control on page 794.

Once you delete a queued message, you cannot retrieve it.

You can delete all of the messages in a queue. When you choose to Delete All, you delete the messages that are in that queue at that moment in time, including messages on additional pages. Before you delete all queued messages, you might want to temporarily stop the mail flow.

See “Stopping the mail flow” on page 645.

You must have Full Administration rights or Manage Status and Logs modify rights to delete queued messages.

See “Setting up local and LDAP administrator accounts” on page 658.

**To delete queued messages**

1. In the Control Center, click Status > SMTP > Message Queues.
2. Specify the queue that you want to view.
   
   See “Viewing queued messages” on page 643.
3. Do any of the following:
   
   To delete a message  
   Select the message that you want to delete and click Delete.
   
   To delete all of the messages in the queue, including messages on additional pages  
   Click Delete All.

### Stopping the mail flow

You may need to stop the flow of mail (for example, before you flush a message queue).

See “Flushing message queues” on page 646.

See “Deleting queued messages” on page 644.

Consider the following implications before you stop the mail flow:

- If you stop the inbound mail flow, no inbound mail is accepted. The mail in the inbound message queue is not scanned, and mail delivery continues.
- If you stop the outbound mail flow, no outbound mail is accepted. The mail in the outbound message queue is not scanned, and mail delivery continues.
If you stop the delivery mail flow, no mail is delivered to downstream local or remote mail servers. Mail in the inbound message queue and outbound message queue is scanned and accumulates in the delivery message queue.

See “MTA and message queue behavior” on page 74.
See “Turning off an appliance” on page 703.
See “Services and MTA operations” on page 71.

To stop the mail flow

1. In the Control Center, click **Status > SMTP > Message Queues**.
2. In the **Host** drop-down list, select a server.
3. From the **Queue** drop-down list, select **Inbound** and click **Display Filtered**.
4. If the queue is started, click **Stop**.
5. From the **Queues** drop-down list, select **Outbound** and click **Display Filtered**.
6. If the queue is started, click **Stop**.
7. From the **Queue** drop-down list, select **Delivery** and click **Display Filtered**.
8. If the queue is started, click **Stop**.

Flushing message queues

When you flush a message queue, you instruct the MTA to try to resend the messages that were deferred due to delivery problems. You may want to flush your inbound, outbound, and delivery email queues before you turn off an appliance.

Before you flush a message queue, temporarily stop the flow of inbound email.

---

**Note:** After you stop the mail flow or determine that a mail flow has stopped, Symantec recommends that you wait two minutes before flushing that message queue.

---

See “Stopping the mail flow” on page 645.
See “MTA and message queue behavior” on page 74.
See “Services and MTA operations” on page 71.

You must have Full Administration rights or Manage Status and Logs modify rights to flush message queues.

You can also flush email queues from the command line.

See **mta-control** on page 794.
To flush email queues from the Control Center

1. In the Control Center, click **Status > SMTP > Message Queues**.
2. Choose a host from the **Host** drop-down list.
3. In the **Queue** drop-down list, select the queue you want.
   - See “Viewing queued messages” on page 643.
4. Click **Flush All**.
   - All messages, including those on additional pages, will be flushed.
5. Wait until the message queue is empty (repeat the previous step as needed).

Monitoring message queue size and volume

You can view the number of queued messages and the size of the queues for all of your message queues. Monitor this status to determine if the message queue is clogged.

You must have Full Administration rights or Manage Status and Logs view rights.

To monitor message queue size and volume

1. In the Control Center, click **Status > System > Hosts**.
2. Click the **Message Queues** tab.
   - You can set the maximum size for each message queue and decide whether to defer messages when the queue is full on the SMTP Advanced Settings page.
   - See “Configuring SMTP advanced settings” on page 54.
   - You can configure alerts for message queues on the Alerts page.
   - See “Configuring alerts” on page 688.

Troubleshooting the message queue

When a message queue becomes too large, Symantec Messaging Gateway can become unresponsive or crash. To attempt to deter this issue, by default, Symantec Messaging Gateway defers new messages when the queue is full. As a best practice, you should leave this setting enabled and keep queue limits below the recommended default thresholds.

See “Configuring SMTP advanced settings” on page 54.

If you experience issues with the message queue, try the following:

- Make sure that your downstream delivery host is functioning and accepting mail.
  - See “Software and services status definitions” on page 610.
- Configure the MTA to reject incoming messages.
  - See “Services and MTA operations” on page 71.
Watch and monitor the queues until they reach acceptable limits.
See “Viewing queued messages” on page 643.
Repeat these measures until the issue is resolved.

Monitoring scheduled tasks

Table 22-24 describes how you can monitor scheduled tasks. You can perform these tasks as needed in any order.

Table 22-24 Monitor scheduled tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn what Symantec Messaging Gateway tasks you can schedule to occur automatically.</td>
<td>The Symantec Messaging Gateway has a number of automated and scheduled tasks which you configure throughout the Control Center. When a scheduled task fails, Symantec Messaging Gateway provides an email alert option which contains details about the failure. If you enable the email alert option, the system notifies the designated administrator when any of the Control Center's scheduled tasks fail. See “About scheduled tasks” on page 648.</td>
</tr>
<tr>
<td>Schedule a task to run automatically.</td>
<td>Each scheduled task shows a start time, a finish time, and the time the task runs next. See “Scheduled task types” on page 649.</td>
</tr>
<tr>
<td>Set up an alert to be notified if a scheduled task fails.</td>
<td>If a task fails, an email notification is sent to the designated administrator, indicating which task failed and on which host. Control Center logs provide further details about the failure. See “Configuring alerts” on page 688.</td>
</tr>
</tbody>
</table>

About scheduled tasks

The Symantec Messaging Gateway has a number of automated and scheduled tasks which you configure throughout the Control Center. You can view and track the status of your scheduled tasks under the Status tab. Scheduled tasks are grouped into subtabs by associated task types. Each subtab page contains the name and status of the scheduled task. If a task completes successfully, the table displays the start time, the finish time, and the time that the task is scheduled to run next. If a task fails to complete, the Finished column displays a status of Failed.

When a scheduled task fails, Symantec Messaging Gateway provides an email alert option which contains details about the failure. If you enable the email alert option, the system notifies the designated administrator when any of the Control Center's scheduled tasks fail.
The system tracks the following types of scheduled tasks:

- Backups
- Expungers
- Notifications
- Quarantine
- Reports
- Preferences

See “Scheduled task types” on page 649.

See “Configuring alerts” on page 688.

Scheduled task types

The Symantec Messaging Gateway has a number of automated and scheduled tasks. You can view the status of all Control Center tasks on the Status > System > Scheduled Tasks page.

Tasks are grouped by type under the following tabs:

- Backup
- Expungers
- Notifications
- Quarantine
- Reports
- Preferences

Under each tab you see a page that contains a table of related tasks. Each scheduled task shows a start time, a finish time, and the time the task runs next. If a task fails for any reason, the term Failed appears in the Finished column.

You can set up an alert to be notified if a scheduled task fails.

The Backups tab reports on tasks that create copies of the Control Center database or database configurations such as content filtering messages, incidents, logs, and reports.

Note: This table is blank until you add a backup configuration.
The **Expungers** tab reports on tasks that delete data from the Control Center repository, such as messages in the spam quarantine, log files in the log database, reports, and data in your content incident folders.

### Table 22-26  Expungers

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Expunger</td>
<td>See “Specifying when and how often Spam Quarantine is expunged” on page 289.</td>
</tr>
<tr>
<td>Log Expungers</td>
<td>See “Managing the log database size” on page 620.</td>
</tr>
<tr>
<td>Reports Expungers</td>
<td></td>
</tr>
<tr>
<td>Content Expungers</td>
<td>See “Scheduling the content incident folder Expungers” on page 426.</td>
</tr>
</tbody>
</table>

The **Notifications** tab reports on tasks that produce automatic emails to system administrators, such as alerts involving system changes or conditions that potentially require attention.

### Table 22-27  Notifications

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert Notifications</td>
<td>See “Configuring alerts” on page 688.</td>
</tr>
<tr>
<td>Content Filtering notifications (Informational Incidents)</td>
<td>See “Creating incident notifications” on page 430.</td>
</tr>
<tr>
<td>Content Filtering notifications (Quarantine Incidents)</td>
<td>See “Creating incident notifications” on page 430.</td>
</tr>
<tr>
<td>Spam Notifications</td>
<td>See “Specifying when to notify users of spam messages in their quarantine” on page 301.</td>
</tr>
</tbody>
</table>

The **Quarantine** tab reports on the task that releases quarantined suspect viruses.

### Table 22-28  Quarantine

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspect Virus Message Quarantine Release</td>
<td>See “Specifying how long suspect virus messages are retained in quarantine” on page 241.</td>
</tr>
</tbody>
</table>
The **Reports** tab reports on the tasks that run **Favorite** reports at specified intervals which are then emailed to a specified recipient. Report types include, Summary, Content Filtering, Email Message, Invalid Recipients, IP Connection, Spam and Virus reports.

**Table 22-29** Reports

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>See “Schedule reports to generate automatically” on page 581.</td>
</tr>
</tbody>
</table>

The **Preferences** tab reports on the task that propagates Directory Data Service data to Scanners.

**Table 22-30** Preferences

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Preferences</td>
<td>See “Configuring the replication of end user preference data” on page 682.</td>
</tr>
</tbody>
</table>

See “About scheduled tasks” on page 648.
Administering your product through the Control Center

This chapter includes the following topics:

- Managing administrators
- Configuring the Control Center
- Customizing user preferences in the Control Center
- Setting up alerts
- Managing passwords
- Maintaining an appliance
- About Symantec Messaging Gateway and Symantec Protection Center
- Managing backups
- Keeping your product current
- Working with diagnostics

Managing administrators

Table 23-1 describes the task that you can perform to manage administrators. You can perform these tasks as needed in any order.
### Manage administrators

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new administrator locally (one at a time).</td>
<td>When you add a new local administrator, you enter user data manually, then select a level of access and enable specific rights. See “Setting up local and LDAP administrator accounts” on page 658.</td>
</tr>
<tr>
<td>Add new LDAP administrators.</td>
<td>You can add new administrators (singly or in groups) using LDAP directory structures to authorize them. You can then assign levels of access and enable specific rights using Administration policies and policy groups. See “Setting up local and LDAP administrator accounts” on page 658.</td>
</tr>
<tr>
<td>Familiarize yourself with what rights an administrator has at each level.</td>
<td>Administrators have access to different pages in the Control Center based on whether they have None, View, or Modify rights. Each type of limited administrator rights grants the administrator the ability to view a subset of the pages of the Control Center. See “Administrator rights” on page 661.</td>
</tr>
<tr>
<td>Edit an existing administrator.</td>
<td>You can modify rights or information about an existing administrator as needed. See “Editing an administrator” on page 667.</td>
</tr>
<tr>
<td>Delete an administrator.</td>
<td>You can delete an administrator at any time. However, when an administrator is deleted, the settings cannot be retrieved. If the administrator might still need access to the Control Center, you may want to consider modifying the administrator’s rights rather than delete the administrator. See “Deleting an administrator” on page 668.</td>
</tr>
<tr>
<td>Set up administrator/end user hybrid view for viewing and managing quarantine</td>
<td>You can set up hybrid views for administrators so that they can access their own end-user quarantine and also perform administrative tasks without separate credentials. See “About administrator and end user views” on page 658.</td>
</tr>
</tbody>
</table>

**About adding and authorizing administrators using LDAP sources**

You can add new administrators based on attributes and group memberships that are found in your LDAP directory structures. You can then configure administration policies and assign those policies to specific LDAP-based groups. You can also assign default policies to existing administrators (called "local" because they were added manually, or locally, to the Control Center in the past). You can create new policies and apply them to individuals or groups. Existing administrators keep their pre-upgrade privileges, which are mapped to five default administration policies.
To add and configure administrators' accounts using LDAP groups (required tasks)

You must perform the following tasks to add and authorize administrators from LDAP structures. The tasks must be performed in order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a directory data source (DDS)</td>
<td>To add administrators using LDAP directories, you first create a new data source or configure an existing one to enable authentication and address resolution. You must configure the DDS with both authentication and address resolution enabled. On the Authentication tab, enable authentication for the Control Center. On the Address Resolution tab, enable authorization for email scanning.</td>
</tr>
</tbody>
</table>
| Create an Administration policy group | Assign newly added LDAP-based administrators or existing local administrators to a policy group that uses one of the five default administration policies:  
  - Full: View and modify all Control Center and scanner functions  
  - Monitor: View status, logs, reports, policies, and settings  
  - Full Report: View and modify reports  
  - Quarantine: View and modify spam and virus quarantines  
  - Content Control: View and modify informational and quarantine incident folders  
  You can also create new administration policies from scratch, or by copying and modifying one of the default policies. You can then assign those policies to an administration policy group. |
| Add members | You add members to administration policy groups on the Administration > Policy Groups > Edit Policy Groups > Members tab. Click the Add button to display the Add Policy Group Members page. Add group members by typing email addresses or LDAP distinguished names, or by specifying the LDAP distinguished name of an Organizational Unit (OU) or Container entry. Any user entries in the sub-tree that is formed by the OU path are also added to the group. |
| Enable administration policy | After adding members to your administration policy group, navigate to the Administration > Policy Groups > Edit Policy Groups > Members tab and check the Enable an Administration Policy for this policy group box. Then select an administration policy from the drop-down list, and click Save. |
The precedence in which policies take effect is determined by their position in the list on the Administration > Policy Groups tab. The administration policy must be first in the list to ensure that your administrators receive the rights you have specified for them. If the administration policy group is not first in the list, then move it to the top by clicking the group name to select it, and then dragging it into position.

To add and configure administrators' accounts using LDAP groups (optional tasks)

If desired, you can perform the following tasks to enable functionality related to LDAP-based groups (End-User Quarantine, notifications and alerts, and applying policies to individual administrators). The tasks can be performed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the administration policy takes precedence over all others to which administrators belong</td>
<td>The precedence in which policies take effect is determined by their position in the list on the Administration &gt; Policy Groups tab. The administration policy must be first in the list to ensure that your administrators receive the rights you have specified for them. If the administration policy group is not first in the list, then move it to the top by clicking the group name to select it, and then dragging it into position.</td>
</tr>
</tbody>
</table>

**Configure End-User Quarantine**

You must enable end-user quarantine in two places (globally on the Spam > Quarantine Settings > End User Settings tab, AND for a specific policy group on the Administration > Users > Add Policy Groups > End Users tab) to allow members of a policy group to access End-User Quarantine.

To enable end-user quarantine for a policy group, you must first configure a directory data source for Control Center Authentication and Email Only Address Resolution (on the Administration > Settings > Directory Integration > Edit Directory Data Source > Authentication and Address Resolution tabs).

**Update notes**

Administrators of the control center are also users, and as such they need to be able to view and manage their own quarantines. Before this release, administrators needed two separate logins (an administrator and a user login, neither based on LDAP structures) to access their quarantines. This release introduces a “hybrid view” that allows administrators to do their administrative tasks and also access their own end-user quarantines with a single LDAP-based account.

**Configure content incident notifications**

If you want content incident notifications to be sent to your Administration policy groups, specify the DL for each policy group on the Content > Settings > Content Incident Folders > Edit Content Incident Folder tab.

**Configure email alerts**

If you want email alerts to be sent to your administration policy groups, specify the DL for each policy group on the Administration > Settings > Alerts tab.
Task | Description
--- | ---
Apply administration policies to local administrators, although they’re not part of policy groups | Instead of specifying permissions for each local administrator, you can apply the same administration policies to them that you can to administration policy groups on the Administration > Users > Administrators > Add Administrator page.

About default administration policies

SMG installs with pre-configured administration policies. These policies are enabled by default and can be applied to a policy group. You can disable or modify the policy actions and the policy groups to which the policies apply. The policy name and the administrator rights cannot be modified for the pre-configured administrator policies that are labeled as default. However, you can copy the default policies and modify them, and then apply them to policy groups.

For a particular administrator who is a member of more than one policy group, only the group with the highest group precedence applies. Policy group precedence is determined by the order of groups on the Policy Groups page.

Policy group precedence can lead to undesired results in cases where the administrator rights (that would often allow other rights to be modified) are not the highest in the list. For example, consider the following scenario. An administrator is a member of two policy groups, with rights as follows:

<table>
<thead>
<tr>
<th>Group name</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>All IT</td>
<td>Spam: delete</td>
</tr>
<tr>
<td></td>
<td>Virus: delete</td>
</tr>
<tr>
<td></td>
<td>Content Filtering: delete</td>
</tr>
<tr>
<td></td>
<td>Administrator rights: none</td>
</tr>
<tr>
<td>Symantec Messaging</td>
<td>Spam: add header</td>
</tr>
<tr>
<td>Gateway Admins</td>
<td>Virus: quarantine</td>
</tr>
<tr>
<td></td>
<td>Content Filtering: deliver normally</td>
</tr>
<tr>
<td></td>
<td>Administrator rights: Full view and modify</td>
</tr>
</tbody>
</table>

An administrator who belongs to both of these groups (if they are listed in this order) would not be able to log into SMG, because the policy group that grants that right is listed below the one that denies the right.

The Default policy group is always the last group in the list. You cannot change the precedence of the Default policy group.

The Table 23-2 table lists the rights conferred by each default administration policy.
Table 23-2  Default administration policies

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Administrator rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Admin Rights</td>
<td>View and modify:</td>
</tr>
<tr>
<td></td>
<td>■ Status and logs</td>
</tr>
<tr>
<td></td>
<td>■ Reports</td>
</tr>
<tr>
<td></td>
<td>■ Policies</td>
</tr>
<tr>
<td></td>
<td>■ Settings</td>
</tr>
<tr>
<td></td>
<td>■ Administrators</td>
</tr>
<tr>
<td></td>
<td>■ Spam submissions</td>
</tr>
<tr>
<td></td>
<td>■ Quarantine</td>
</tr>
<tr>
<td></td>
<td>■ Informational Incident Folders</td>
</tr>
<tr>
<td></td>
<td>■ Quarantine Incident Folders</td>
</tr>
<tr>
<td>Monitoring Access</td>
<td>■ Status and logs</td>
</tr>
<tr>
<td></td>
<td>■ Reports</td>
</tr>
<tr>
<td></td>
<td>■ Policies</td>
</tr>
<tr>
<td></td>
<td>■ Settings</td>
</tr>
<tr>
<td>Full Report Rights</td>
<td>Modify:</td>
</tr>
<tr>
<td></td>
<td>■ Reports</td>
</tr>
<tr>
<td>Quarantine Admin Rights</td>
<td>Modify:</td>
</tr>
<tr>
<td></td>
<td>■ Manage Spam Quarantine</td>
</tr>
<tr>
<td></td>
<td>■ Manage Virus Quarantine</td>
</tr>
<tr>
<td></td>
<td>■ Manage Spam Quarantine</td>
</tr>
<tr>
<td></td>
<td>■ Manage Virus Quarantine</td>
</tr>
<tr>
<td>Content Control Admin Rights</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Informational Incident Folders</td>
</tr>
<tr>
<td></td>
<td>■ Quarantine Incident Folders</td>
</tr>
</tbody>
</table>

See “Editing, deleting, enabling, or disabling a policy group” on page 195.
See “Setting policy group precedence” on page 203.
See “Researching policy group membership for a user” on page 194.
See “Creating a policy group” on page 190.
See “Importing and exporting policy group members” on page 193.
About administrator and end user views

Control Center administrators can be given quarantine administration rights, which allows them to manage the quarantines of all users. However, if administrators do not have these rights, they still need to be able to view and manage their own personal quarantines when end-user quarantine is enabled. Symantec Messaging Gateway supports two views (the Administrator View and the End User View) to allow administrators to view and manage their own quarantines, regardless of their administrator rights concerning quarantine.

In order to have access to the hybrid view, Administrators must be LDAP-based (i.e. with both authentication and address resolution configured in a directory data source) as opposed to local (email addresses and hosts typed in manually in the Control Center). If you want your existing local administrators to have access to this functionality, you must add them to an LDAP-based group. See “Setting up local and LDAP administrator accounts” on page 658.

End-user quarantine must be enabled both globally (configured on the Spam > Quarantine Settings > End User Settings page) and on a per-group basis (configured on the Policy Groups > Edit Policy Group’s End User tab). You receive a warning message if you try to enable it in one location and not in the other. If end-user quarantine is not enabled, then only administrators with rights to view or manage quarantines can view or manage them, and only the Administrator view is displayed.

See “Configuring end user quarantine” on page 284.

Setting up local and LDAP administrator accounts

When you add a new administrator, you select a level of access and enable specific rights. You can set up accounts for one administrator at a time, or for groups of administrators. You can add local administrators by entering information manually, or you can add administrators using information present in LDAP directory structures.

To set up accounts for local administrators

You add local administrators by entering user data manually. Once the administrator's information has been entered, you can apply an existing administration policy to that administrator, or create a new, custom policy. Follow the steps below to add a single administrator and assign an administration policy that specifies the administrator's rights.

Setting up accounts for local administrators

1. In the Control Center, click Administration > Users > Administrators.
2. Click Add.
3. In the User name box, type the user name (in US ASCII characters).
4. In the Password box, type a password.
5. In the Confirm password box, type the password again to confirm it.
6 In the **Email address** box, type the email address of the administrator.

7 If this administrator is to receive system alerts, check **Receive Alert Notifications**.

8 In the **Content Incident Folder Notifications**, choose the folders for which this administrator should receive notifications when incidents are added:

- **Folders**: Selects/deselects all Content Incident folders (both Informational and Quarantine)
- **Informational Incidents**: Selects/deselects Informational Incident folders only
- **Quarantine Incidents**: Selects/deselects Quarantine Incident folders only

9 In the **Administration Policy** area, do one of the following:

- Choose an existing administration policy from the list.
- Type the name of a new administration policy that you want to create, and then type a description of the policy.

If you added a new administration policy, choose the administration rights that you want to assign to the new policy as follows:

- **Full Administration Rights**: Click **Full Administration Rights** to let the administrator view and modify all available rights.
- **Limited Administration Rights**: Click **Limited Administration Rights** and choose the specific rights for this administrator as follows:
  - **None**: Administrators do not have any rights on selected task or content incident folder.
  - **View**: Administrators can view appropriate pages and content incident folders but cannot manage them.
  - **Modify**: Administrators have full rights to view and modify selected tasks and content incident folders.

See “Administrator rights” on page 661.
System features and functions to which full and limited administration rights apply

- Status and Logs
- Reports
- Policies
- Settings
- Administration
- Spam Submissions
- Quarantine
- Informational Incident folders
- Quarantine Incident folders

10 If this is a new administration policy, choose the Content Incident Folders access for the policy:

Informational Incidents: Administrators can view incidents in the indicated content incident folder but cannot manage them. Administrators with View permissions cannot perform any actions on incidents in the indicated content incident folder.

Quarantine Incidents: Administrators can view and modify all incidents in the indicated content incident folder.

11 Click Save.

To set up accounts for LDAP administrators

To add administrators using LDAP directories, you first create a new data source or configure an existing one to enable authentication and address resolution. See “Adding a data source” on page 496.

Once your data source is configured, follow the steps below to add LDAP administrators.

Setting up accounts for LDAP administrators

- In the Control Center, click Administration > Users > Policy Groups, and do one of the following:
  - If the policy group to which you want to add administrators exists, click to select it, and then click Add. The Edit Policy Group page appears. See “Adding members to a policy group” on page 191.
  - If the policy group to which you want to add administrators does not exist, click Add with no group name selected. The Edit Policy Group page appears. See “Creating a policy group” on page 190.
  - Once you have added members to the policy group, click the Administration tab and then enable and select an Administration policy for the group. If you want to change
the specific rights for the administration policy, click Administration > Policies > Administration, select the policy, and click Edit. Edit the Administration policy as desired.

Administrator rights

An administrator with Full Administration Rights can view, access, and modify any page in the Control Center.

You can grant administrators Limited Administration Rights with the following access:

- None: Administrators do not have any rights to perform the selected task and cannot view the corresponding pages.
- View: Administrators can view appropriate pages, but cannot manage them.
- Modify: Administrators have full rights to view and modify tasks.

Each type of Limited Administration Rights grants the administrator the ability to view a subset of the pages of the Control Center. You can grant Limited Administration Rights to the following functions:

- Status and Logs
- Reports
- Policies
- Settings
- Administration
- Spam Submissions
- Quarantine

In addition, under Content Incident Folders, you can choose None, View, or Modify for each content incident folder that you create. You can also check Receive Incident Notifications for any content incident folder.

Any administrator without either Full Administration Rights or Manage Administration rights can see the Administration > Users > Administrators page. But the administrator will only be able to change his or her own password on that page. Only an administrator with Full Administration Rights can modify another administrator with Full Administration Rights.

**Note:** To view or modify the contents of a content incident folder, you must have View or Modify rights for that folder under Content Incident Folders on the Add Administrator or Edit Administrator page. Many types of Limited Administrator Rights let you view the pages for all content incident folders but not the content of those folders.
Table 23-3 shows the pages that are available to administrators with Manage Status and Logs View or Modify rights.

Table 23-3  Manage Status and Logs pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>System</td>
<td>■ Dashboard&lt;br&gt; ■ Hosts&lt;br&gt; ■ Logs&lt;br&gt; ■ Scheduled Tasks</td>
</tr>
<tr>
<td>Status</td>
<td>SMTP</td>
<td>■ Message Audit Logs&lt;br&gt; ■ Message Queues</td>
</tr>
<tr>
<td>Status</td>
<td>Submissions</td>
<td>Submission Detail</td>
</tr>
<tr>
<td>Content</td>
<td>Incident Management</td>
<td>■ Content Incident Folder Overview&lt;br&gt; ■ Informational Incidents&lt;br&gt; ■ Quarantine Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following message appears when administrators do not have appropriate rights to view the contents of incident folders: &quot;You do not have sufficient rights to view these content filtering incidents. See your system administrator to gain access to this content incident folder.&quot;</td>
</tr>
<tr>
<td>Administration</td>
<td>Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>Administration</td>
<td>Settings</td>
<td>Logs</td>
</tr>
<tr>
<td>Administration</td>
<td>Hosts</td>
<td>■ Configuration&lt;br&gt; ■ Licenses&lt;br&gt; ■ Utilities</td>
</tr>
</tbody>
</table>

Table 23-4 shows the pages that are available to administrators with Manage Reports View or Modify rights.
Table 23-4  Manage Reports pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports</td>
<td>View</td>
<td>■ Create a Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Favorite Reports</td>
</tr>
<tr>
<td>Content</td>
<td>Incident Management</td>
<td>The following message appears when administrators do not have appropriate rights to view the contents of incident folders:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;You do not have sufficient rights to view these content filtering incidents. See your system administrator to gain access to this content incident folder.&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>Administration</td>
<td>Settings</td>
<td>Report</td>
</tr>
</tbody>
</table>

Table 23-5 shows the pages that are available to administrators with Manage Policies View or Modify rights.

Table 23-5  Manage Policies pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation</td>
<td>Policies</td>
<td>■ Bad Senders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Connection Classification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Good Senders</td>
</tr>
<tr>
<td>Reputation</td>
<td>Reputation Tools</td>
<td>■ Find Sender</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ IP Reputation Lookup</td>
</tr>
<tr>
<td>Spam</td>
<td>Policies</td>
<td>Email</td>
</tr>
<tr>
<td>Spam</td>
<td>Settings</td>
<td>Sender Authentication</td>
</tr>
<tr>
<td>Malware</td>
<td>Policies</td>
<td>Email</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>Policies</td>
<td>Email</td>
</tr>
<tr>
<td>Content</td>
<td>Policies</td>
<td>Email</td>
</tr>
</tbody>
</table>
### Table 23-5  Manage Policies pages (continued)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Resources</td>
<td>■ Annotations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Attachment Lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Dictionaries</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Notifications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Patterns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Records</td>
</tr>
<tr>
<td>Administration</td>
<td>Users</td>
<td>■ Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Find User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Policy Groups</td>
</tr>
</tbody>
</table>

**Table 23-6** shows the pages that are available to administrators with **Manage Settings** View or Modify rights.

### Table 23-6  Manage Settings pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>SMTP</td>
<td>■ Address Masquerading</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Aliases</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Invalid Recipients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Settings</td>
</tr>
<tr>
<td>Spam</td>
<td>Settings</td>
<td>■ Probe Accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Quarantine Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Scan Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Submission Settings</td>
</tr>
<tr>
<td>Malware</td>
<td>Settings</td>
<td>■ LiveUpdate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Scan Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Suspect Virus Settings</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>Settings</td>
<td>■ CA Connect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Scan Settings</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>SMTP</td>
<td>CA Queue</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>SMTP</td>
<td>CA Queue</td>
</tr>
</tbody>
</table>
Table 23-6  Manage Settings pages (continued)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Settings</td>
<td><img src="#" alt="List of options" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Archive</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Content Encryption</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Content Incident Folders</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>DLP Connect</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following message appears when administrators do not have</td>
</tr>
<tr>
<td></td>
<td></td>
<td>appropriate rights to view the contents of incident folders:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;You do not have sufficient rights to view these content filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>incidents. See your system administrator to gain access to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this content incident folder.&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administration</th>
<th>Users</th>
<th>Administrators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Settings</td>
<td><img src="#" alt="List of options" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Alerts</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Certificates</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Control Center</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Directory Integration</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Logs</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Reports</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>SNMP</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>UPS</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administration</th>
<th>Hosts</th>
<th>Configuration</th>
</tr>
</thead>
</table>

Table 23-7 shows the pages that are available to administrators with **Manage Administration** View or Modify rights.

Table 23-7  Manage Administration pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Users</td>
<td><img src="#" alt="Administrators" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="#" alt="End Users" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administration</th>
<th>Hosts</th>
<th><img src="#" alt="Licenses" /></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><img src="#" alt="Shutdown" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="#" alt="Version" /></td>
</tr>
</tbody>
</table>
Table 23-7  Manage Administration pages (continued)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Informational Management</td>
<td>■ Informational Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Quarantine Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following message appears when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>administrators do not have appropriate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rights to view the contents of incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>folders:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;You do not have sufficient rights to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>view these content filtering incidents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See your system administrator to gain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access to this content incident folder.&quot;</td>
</tr>
</tbody>
</table>

Table 23-8 shows the pages that are available to administrators with Manage Submissions View or Modify rights.

Table 23-8  Manage Spam Submissions pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>System</td>
<td>Dashboard</td>
</tr>
<tr>
<td>Status</td>
<td>Submissions</td>
<td>Submissions Detail</td>
</tr>
<tr>
<td>Spam</td>
<td>Settings</td>
<td>Submission Settings</td>
</tr>
<tr>
<td>Spam</td>
<td>Submissions</td>
<td>Submit Messages</td>
</tr>
<tr>
<td>Content</td>
<td>Incident</td>
<td>■ Informational Incidents</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>■ Quarantine Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Custom content incident folders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following message appears when</td>
</tr>
<tr>
<td></td>
<td></td>
<td>administrators do not have appropriate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rights to view the contents of incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>folders:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;You do not have sufficient rights to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>view these content filtering incidents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See your system administrator to gain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access to this content incident folder.&quot;</td>
</tr>
<tr>
<td>Administration</td>
<td>Users</td>
<td>Administrators</td>
</tr>
</tbody>
</table>
Table 23-9 shows the pages that are available to administrators with Manage Quarantine View or Modify rights.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Settings</td>
<td>Quarantine Settings</td>
</tr>
<tr>
<td>Spam</td>
<td>Quarantine</td>
<td>Email Spam</td>
</tr>
<tr>
<td>Virus</td>
<td>Settings</td>
<td>Suspect Virus Settings</td>
</tr>
<tr>
<td>Virus</td>
<td>Quarantine</td>
<td>Email Suspect Virus</td>
</tr>
<tr>
<td>Content</td>
<td>Incident Management</td>
<td>Informational Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quarantine Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Custom content incident</td>
</tr>
<tr>
<td></td>
<td></td>
<td>folders</td>
</tr>
</tbody>
</table>

The following message appears when administrators do not have appropriate rights to view the contents of incident folders:

"You do not have sufficient rights to view these content filtering incidents. See your system administrator to gain access to this content incident folder."

Editing an administrator

You can edit an administrator to modify any of the following:

- Administrator's name
- Administrator's email address
- Administrator's password
- Whether the administrator receives notifications
- Administrator's rights
  See “Administrator rights” on page 661.
- Whether the administrator receives notifications about content incident folder incidents

See “Setting up local and LDAP administrator accounts” on page 658.
To edit an administrator

1. In the Control Center, click **Administration > Users > Administrators**.
2. Select an Administrator from the list and click **Edit**.
3. Change the Administrator definition as needed.
4. Click **Save**.

Deleting an administrator

You can delete an administrator at any time. However, when an administrator is deleted, the settings cannot be retrieved. If the administrator might still need access to the Control Center, you may want to consider modifying the administrator’s rights rather than deleting the administrator.

See “Editing an administrator” on page 667.

To delete an administrator

1. In the Control Center, click **Administration > Users > Administrators**.
2. Check the box beside the administrator that you want to remove.
3. Click **Delete**.
4. In the confirmation dialog box, click **OK** to confirm the deletion.

Configuring the Control Center

The Control Center is a browser-enabled application that interfaces with the Symantec Messaging Gateway system.

Table 23-10 describes the ways that you can configure the Control Center. You can perform these tasks as needed in any order.

**Table 23-10** Configure the Control Center

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how multiple users can access the Control Center at the same time.</td>
<td>Multiple end users can access the Control Center at the same time, for example to review messages in Spam Quarantine. Multiple administrators can access the Control Center at the same time and perform administration tasks. See “About simultaneous Control Center access” on page 671.</td>
</tr>
</tbody>
</table>
### Table 23-10  Configure the Control Center (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how you can let clients connect to the Control Center.</td>
<td>When you specify host names for Control Center access, you enable the Control Center to let clients connect based on the Control Center's DNS perspective. If the client's IP address resolves to a name that matches an allowed host name (a “reverse lookup”), then the Control Center permits access to the client.  See “About specifying host names for Control Center access” on page 672.</td>
</tr>
<tr>
<td>Specify the hosts that are permitted to access the Control Center.</td>
<td>You access the Control Center through a Web browser. By default, anyone with the correct address and logon information has access from any host. But you can also choose to specify which hosts can access to the Control Center. Users that attempt to log in to the Control Center from unauthorized computers receive a 403 Forbidden page message in their Web browser. Reverse Domain Name Server (DNS) lookup must be enabled in your DNS software for this feature to work with host names. See “Specifying which hosts can access the Control Center” on page 672.</td>
</tr>
<tr>
<td>Monitor Control Center events through SNMP.</td>
<td>Simple Network Management Protocol (SNMP) lets administrators monitor network devices, such as the Control Center and Scanners. You can specify an SNMP community string and trap. You can also manage access privileges to the SNMP agent for up to four hosts in your environment. If you enable SNMP v3, you can also specify authentication and encryption settings. See “Configuring SNMP settings to monitor network devices” on page 673.</td>
</tr>
<tr>
<td>Change the listener port, if necessary.</td>
<td>By default, Spam Quarantine, Suspect Virus Quarantine, and content incident folders accept messages from the Scanner on port 41025. However, you can change this port if necessary. You do not need to change any Scanner settings to match the change in the listener port. You can also disable the listener port. See “Configuring the Control Center listener port” on page 675.</td>
</tr>
<tr>
<td>Install a self-signed certificate or a CA-signed certificate for Control Center access.</td>
<td>By default, the Control Center uses a demo certificate to authenticate access to the Control Center. The demo certificate causes a security warning in your browser when you access the Control Center. You can ignore the security warning and proceed to access the Control Center. However, you can install a certificate to enhance the security of the browser-to-Control Center communication and to prevent the security warning. See “Bypassing the security warning when you access the Control Center” on page 675.</td>
</tr>
<tr>
<td>Designate a user interface HTTPS certificate through the Control Center.</td>
<td>This certificate enhances the security for the Control Center and those logging into it. See “Designating a Control Center certificate” on page 676.</td>
</tr>
</tbody>
</table>
Table 23-10  Configure the Control Center (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Control Center for single- and double-byte character sets and for appropriate number, date, and time settings with the Locale setting.</td>
<td>For example, the Locale setting affects the format of email messages that the Control Center sends, such as notifications, alerts, and reports. You can also select a fallback encoding option for the Control Center to use in cases when the language identification feature is unable to correctly determine the language of a quarantined email message. See “Setting the locale encoding and fallback encoding” on page 676.</td>
</tr>
<tr>
<td>Convert 8-bit MIME messages.</td>
<td>If you encounter issues with MTAs that cannot handle 8-bit MIME, you can force the sending MTA to convert the 8-bit MIME messages to 7-bit MIME. See “Converting 8-bit MIME messages to 7-bit MIME” on page 677.</td>
</tr>
<tr>
<td>Modify the default date format and time formats.</td>
<td>Symantec Messaging Gateway installs with default date and time formats. However, you can modify these formats. See “Customizing the date format and time format” on page 677. See “Date format and time format pattern syntax” on page 678.</td>
</tr>
</tbody>
</table>

Configuring Control Center settings

Table 23-11  Process for configuring Control Center settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set up host and client mappings.</td>
<td>Specify host names to enable Reverse DNS lookup. See “About specifying host names for Control Center access” on page 672. Specify which computers or networks can access the Control Center. See “Specifying which hosts can access the Control Center” on page 672.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add enhanced security for the Control Center.</td>
<td>Designate a user interface certificate HTTPS. See “Designating a Control Center certificate” on page 676. Modify default demo certificate to prevent security warning. See “Bypassing the security warning when you access the Control Center” on page 675.</td>
</tr>
</tbody>
</table>
Table 23-11  Process for configuring Control Center settings (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 3 | Modify default settings. | Change or disable the listener port.  
See “Configuring the Control Center listener port” on page 675.  
Specify host settings for product generated alert and report notifications.  
See “Configuring Control Center SMTP settings for alerts and reports” on page 694.  
Configure the Control Center for single- and double-byte character sets and for number, date, and time settings.  
See “Setting the locale encoding and fallback encoding” on page 676. |
| Step 4 | Customize user login experience. | Customize the Login help page.  
See “Specifying a custom user Login help page” on page 680.  
Enable "Remember me" feature for automatic login.  
See “Enabling users to bypass Control Center login credentials” on page 681.  
Extend user preferences to attached Scanners.  
See “Configuring the replication of end user preference data” on page 682. |

About simultaneous Control Center access

Multiple end users can access the Control Center at the same time, for example to review messages in Spam Quarantine.

Multiple administrators can access the Control Center at the same time and perform administration tasks. However, each administrator may see errors in certain cases. In particular, errors can occur if each administrator attempts resource-intensive tasks in the Control Center at the same time. For example, querying message audit logs and IP reputation at the same time can cause errors.

See “Configuring Control Center settings” on page 670.
About specifying host names for Control Center access

When you specify host names for Control Center access, you enable the Control Center to let clients connect based on the Control Center's DNS perspective. If the client's IP address resolves to a name that matches an allowed host name (a “reverse lookup”), the Control Center permits access to the client. The Control Center resolves and accepts both IPv4 address ranges and IPv6 address ranges for access control.

The owner of a netblock (a range of IP addresses usually belonging to the same organization) controls the reverse lookup of an IP address. Typically, users do not control what name their IP addresses resolve to. Additionally, DNS servers may have unique mappings for the same netblock.

Consider the following information:

- A client's authoritative DNS server has a reverse lookup record of \texttt{m1.symantecexample.com} for the client's IP address.
- The DNS that is configured to be the Control Center's primary DNS server has a reverse mapping of \texttt{dhcp23.symantecexample.com} for the same IP address.

In this case, the Control Center sees the \texttt{dhcp23.symantecexample.com} name whenever the client connects. Therefore, the name the Control Center sees is the name you type in the host access control list in the Control Center. This situation happens more frequently on private networks than on the public Internet.

See “Specifying which hosts can access the Control Center” on page 672.

Specifying which hosts can access the Control Center

You access the Control Center through a Web browser. By default, anyone with the correct address and logon information has access from any host. But you can also choose to specify which hosts can access to the Control Center. Users that attempt to log in to the Control Center from unauthorized computers receive a 403 Forbidden page message in their Web browser.

Reverse Domain Name Server (DNS) lookup must be enabled in your DNS software for this feature to work with host names.

See “About specifying host names for Control Center access” on page 672.

\textbf{Note:} If you make an error when you type the host name, you block all access to the Control Center. If this situation occurs, use the command-line \texttt{delete bcchostacl} command to clear the list of computers that are permitted to access the Control Center.

See \texttt{delete} on page 752.
To specify which hosts can access the Control Center

1. In the Control Center, click **Administration > Settings > Control Center.**
2. Click the **Access** tab.
3. Under **Control Center Access**, do one of the following tasks:
   - **To permit any host access to the Control Center**: Check **All hosts**.
   - **To assign specific hosts to access the Control Center**: Check **Only the following hosts**, and then type a host name, IP address, IP address with subnet mask, or Classless Inter-Domain Routing (CIDR) netblock. Specify additional computers or networks as needed. Hosts that are not in this list are not able to access the Control Center. IPv4 addresses and IPv6 addresses are supported.

4. Click **Add**.
5. Click **Save**.

Configuring SNMP settings to monitor network devices

Simple Network Management Protocol (SNMP) lets administrators monitor network devices, such as the Control Center and Scanners. You can specify an SNMP community string and trap. You can also manage access privileges to the SNMP agent for up to four hosts in your environment. If you enable SNMP v3, you can also specify authentication and encryption settings.

Before you configure SNMP settings, you must first download the Management Information Base (MIB) database and import it to your SNMP client.

For information on how to query and test the most relevant SNMP Object Identifiers (OID) for Messaging Gateway 10.x, go to [https://support.symantec.com/en_US/article.TECH227540.html](https://support.symantec.com/en_US/article.TECH227540.html).

To configure SNMP settings for monitoring network devices

1. In the Control Center, click **Administration > Settings > SNMP.**
2. On the **Server** tab, check **Enable SNMP**.
3. In the **SNMP trap host IP address** box, type the IP address of the device that receives SNMP trap alerts.
   - Fully qualified domain names (FQDN) are not supported.
4 In the **SNMP listening port** box, type the port at which the SNMP agent listens for network traffic.

5 Click the **Versions** tab.

6 Check the versions that you want to use.

   You can choose SNMP v2, SNMP v3, or both. If you chose SNMP v3 only, proceed to step 12.

7 In the **SNMP community string** box, type the SNMP Agent’s community string.

8 Under **SNMP Client Access**, specify which hosts can access the SNMP agent by doing one of the following tasks:
   - Click **All hosts** to grant all hosts access to the SNMP client.
   - Click **Only the following hosts**. Then type the IP addresses, host names, or CIDR ranges of specific hosts that you want to have access to the SNMP client.

9 Click **Add**.

10 You can delete any currently SNMP-access-enabled hosts by checking the box next to their names and clicking **Delete**.

11 If you did not choose SNMP v3, click **Save**. If you chose SNMP v3, continue with the following steps.

12 Click to choose the **Authentication type**.

   You can choose either message digest algorithm 5 (MD5) or secure hash algorithm (SHA).

13 In the **Authentication user name** field, type the user name.

14 In the **Authentication password** field, type the password.

   The password must be at least eight characters long.

15 Type the password again in the **Confirm password** field.

16 If you want to use encryption, click **Enable SNMP v3 encryption**.

17 Click to choose the **Encryption type**.

   You can choose Advanced Encryption Standard (AES) or data encryption standard (DES).

18 In the **Encryption password** field, type the password.

   The password must be at least eight characters long.

19 Type the password again in the **Confirm password** field.

20 On the **MIBs** tab, click **SNMP MIBs**.

21 Click on a MIB to download it. Import the MIB into your SNMP client.

22 Click **Save**.
Configuring the Control Center listener port

By default, Spam Quarantine, Suspect Virus Quarantine, and content incident folders accept messages from the Scanner on port 41025. However, you can change this port if necessary. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify these settings. You do not need to change any Scanner settings to match the change in the listener port.

You can also disable the listener port. Disable the listener port if your computer is not behind a firewall, and you are concerned about security risks. If you disable the listener port, disable any policies that quarantine messages. Otherwise, quarantined messages back up in the delivery mail flow queue until the expiration time elapses and then bounce back to the original sender.

See “About content incident folders” on page 419.

See “About quarantining spam” on page 280.

See “About quarantining suspected viruses” on page 237.

To modify or disable the listener port through which the Control Center accepts messages

1 In the Control Center, click **Administration > Settings > Control Center**.

2 Click the **Listeners** tab.

3 Under **Listener Port** in the **Port** box, do one of the following:
   - Type the new port number.
   - Type 0 to disable the listener port.

4 Click **Save**.

Bypassing the security warning when you access the Control Center

By default, the Control Center uses a demo certificate to authenticate access to the Control Center. The demo certificate causes a security warning in your browser when you access the Control Center. You can ignore the security warning and proceed to access the Control Center. However, you can install a certificate to enhance the security of the browser-to-Control Center communication and to prevent the security warning.

Determine if you want to use a self-signed certificate or a CA-signed certificate. A self-signed certificate does not provide the same level of security as a CA-signed certificate. To get a CA-signed certificate, you must submit a CSR to a Certificate Authority.

The following procedure assumes that you use a CA-signed certificate.
To bypass the security warning when you access the Control Center

1. Add a certificate in the Control Center and submit the CSR to a Certificate Authority to get a certificate.
   
   Ensure that the hostname in the CSR matches the hostname of the Control Center.
   
   See "Requesting a Certificate Authority signed certificate" on page 176.

2. Import the certificate that you receive from a Certificate Authority.
   
   See "Importing a Certificate Authority signed certificate" on page 177.

3. Install an intermediate certificate, if needed.
   
   See “Adding a CA or an intermediate certificate” on page 175.

4. Assign the certificate as the Control Center HTTPS certificate.
   
   See "Assigning a user interface HTTPS certificate to the Control Center" on page 186.

5. Access the Control Center with the fully qualified domain name that you supplied on the CSR.

Designating a Control Center certificate

You can designate a user interface HTTPS certificate through the Control Center. This certificate enhances the security for the Control Center and those logging into it.

See "Bypassing the security warning when you access the Control Center" on page 675.

To designate a Control Center certificate

1. In the Control Center, click Administration > Settings > Control Center.

2. Click the Certificates tab.

3. Under Control Center Certificate, click the User interface HTTPS certificate drop-down list to select the certificate that you want to use.
   
   See “About certificates” on page 169.

4. Click Save.

Setting the locale encoding and fallback encoding

Configure the Control Center for single- and double-byte character sets and for appropriate number, date, and time settings with the Locale setting. For example, the Locale setting affects the format of email messages that the Control Center sends, such as notifications, alerts, and reports.

You can also select a fallback encoding option for the Control Center to use in cases when the language identification feature is unable to correctly determine the language of a quarantined email message.
Language identification may fail if the message headers or body contain any of the following items:

- Raw 8-bit characters with missing or corrupted encoding information
- Too few characters with missing or corrupted encoding information
- Only a few characters with a mix of two or more types of encodings

Set the fallback encoding to the most common encoding that is used in your region or country.

See “Customizing the date format and time format” on page 677.

To set the locale encoding and fallback encoding

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Click the **Locale** tab.
3. Under **System Locale and Fallback Encoding**, click the **System locale** drop-down list and select an encoding.
4. Click the **Quarantine fallback encoding** drop-down list and select an encoding.
5. Click **Save**.

### Converting 8-bit MIME messages to 7-bit MIME

If you encounter issues with MTAs that cannot handle 8-bit MIME, you can force the sending MTA to convert the 8-bit MIME messages to 7-bit MIME.

See “About email message flow” on page 100.

To convert 8-bit MIME messages to 7-bit MIME

1. In the Control Center, click **Protocols > SMTP > Settings**.
2. On the **SMTP** tab, under **Mime Handling**, check **Do not advertise 8BITMIME**.
3. Click **Save**.

### Customizing the date format and time format

Symantec Messaging Gateway installs with default date and time formats. However, you can modify these formats. You must have Full Administration rights or Manage Settings rights to modify date and time formats.

#### Table 23-12  Configurable date and time formats

<table>
<thead>
<tr>
<th>Format</th>
<th>Syntax and default value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>hh:mm:ss a</td>
<td>02:29:34 PM</td>
</tr>
</tbody>
</table>
Table 23-12  Configurable date and time formats (continued)

<table>
<thead>
<tr>
<th>Format</th>
<th>Syntax and default value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short date</td>
<td>MM/dd/yy</td>
<td>2/25/10</td>
</tr>
<tr>
<td>Long date</td>
<td>MMMM dd, yyyy</td>
<td>February 25, 2010</td>
</tr>
<tr>
<td>Full date and time</td>
<td>EEEE, MMMM dd, yyyy:hh:mm:ss:zz</td>
<td>Thursday, Feb 25, 2010 01:23:45 PM PST</td>
</tr>
<tr>
<td>AM/PM symbols</td>
<td>AM/PM</td>
<td>AM</td>
</tr>
</tbody>
</table>

Symantec Messaging Gateway applies the date format and time formats that you configure as follows:

- **Detail view**
  - Full date and time
- **List view**
  - Long date
- **Mailbox**
  - Combination of long date format and time
  - Uses the time format for same day’s email; uses the long format for everything else
- **Reports**
  - Short date and time

The maximum syntax length that you can specify is 32 characters. The 32-character limit does not include spaces.

See “Date format and time format pattern syntax” on page 678.

The option to customize the date format and time format is disabled by default. You must enable this feature to modify date and time formats.

**Configuring the date format and time format**

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Click the **Locale** tab.
3. Check **Apply custom date and timestamp format**.
4. Specify the custom date and timestamp formats that you want to use.
5. Click **Save**.

**Date format and time format pattern syntax**

Table 23-13 provides the supported date format and time format syntax.
Table 23-13  Date and time format syntax

<table>
<thead>
<tr>
<th>Letter</th>
<th>Component</th>
<th>Presentation</th>
<th>Example in US locale</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>Era</td>
<td>Text</td>
<td>AD</td>
</tr>
<tr>
<td>yyyy: yy</td>
<td>Year</td>
<td>Year</td>
<td>2010; 10</td>
</tr>
<tr>
<td>MMMM;MMM;MM</td>
<td>Month in year</td>
<td>Month</td>
<td>July; Jul; 07</td>
</tr>
<tr>
<td>w</td>
<td>Week in year</td>
<td>Number</td>
<td>27</td>
</tr>
<tr>
<td>W</td>
<td>Week in month</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>DDD</td>
<td>Day in year</td>
<td>Number</td>
<td>189</td>
</tr>
<tr>
<td>d</td>
<td>Day in month</td>
<td>Number</td>
<td>10</td>
</tr>
<tr>
<td>F</td>
<td>Day of week in month</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>EEEE; EEE</td>
<td>Day in week</td>
<td>Text</td>
<td>Tuesday; Tue</td>
</tr>
<tr>
<td>a</td>
<td>AM/PM mark</td>
<td>Text</td>
<td>PM</td>
</tr>
<tr>
<td>H</td>
<td>Hour in day 24H (0-23)</td>
<td>Number</td>
<td>0</td>
</tr>
<tr>
<td>k</td>
<td>Hour in day 24H (1-24)</td>
<td>Number</td>
<td>24</td>
</tr>
<tr>
<td>K</td>
<td>Hour in day 12H (0-11)</td>
<td>Number</td>
<td>0</td>
</tr>
<tr>
<td>h</td>
<td>Hour in day 12H (1-12)</td>
<td>Number</td>
<td>12</td>
</tr>
<tr>
<td>m</td>
<td>Minute in hour</td>
<td>Number</td>
<td>20</td>
</tr>
<tr>
<td>s</td>
<td>Second in minute</td>
<td>Number</td>
<td>55</td>
</tr>
<tr>
<td>S</td>
<td>Millisecond</td>
<td>Number</td>
<td>978</td>
</tr>
<tr>
<td>z</td>
<td>Time zone</td>
<td>Time zone</td>
<td>Pacific Daylight Time; PDT</td>
</tr>
<tr>
<td>zz</td>
<td>Time zone</td>
<td>RFC822</td>
<td>-0800</td>
</tr>
<tr>
<td>zzzz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td>Time zone</td>
<td>RFC822</td>
<td>-0800</td>
</tr>
</tbody>
</table>

See "Customizing the date format and time format" on page 677.

**Customizing user preferences in the Control Center**

Table 23-14 describes the tasks that you can perform to customize the Control Center. You can perform these tasks as needed in any order.
You can customize the Login help with a custom Login help page URL. Create a Web page that tells your users how to log in and make it available on your network. The Web page should be accessible from any computer where users log in. See “Specifying a custom user Login help page” on page 680.

Let Symantec Messaging Gateway place a cookie on users' computers so they can bypass login credentials. Symantec Messaging Gateway contains a feature that, when enabled, remembers users' login credentials. A Remember me option appears on the Symantec Messaging Gateway Login page when the administrator enables the Remember me feature. When this feature is enabled, it is available to all users, including end users. See “Enabling users to bypass Control Center login credentials” on page 681.

Specify how often the users preferences are replicated to the Control Center. In the Control Center, replication refers to the process by which user preferences are propagated from the Control Center to attached and enabled Scanners. Global settings in the Control Center control the replication process. See “Configuring the replication of end user preference data” on page 682.

Modify the default SMTP greeting and postmaster address. When Symantec Messaging Gateway connects with other mail servers to initiate inbound or outbound messaging traffic, the SMTP protocol conversation begins with a greeting. You can also change the postmaster address. Symantec Messaging Gateway includes the postmaster address in bounce messages. See “Setting up your SMTP greetings and postmaster address” on page 683.

**Specifying a custom user Login help page**

By default, when users click the Need help logging in? link on the Control Center Login page, the Symantec online help window opens. You can customize the Login help with a custom Login help page URL. This change only affects the Login help page, not the rest of the online help.

Create a Web page that tells your users how to log in and make it available on your network. The Web page should be accessible from any computer where users log in.

See “Viewing spam and suspected spam messages in quarantine” on page 292.

See “Enabling users to bypass Control Center login credentials” on page 681.

To specify a custom user Login help page

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Click the **Users** tab.
3 Under User Help in the Login help URL box, type the URL to the Web page that you want to use.

To disable your custom logon help page, delete the contents of the Login help URL box.

4 Click Save.

Enabling users to bypass Control Center login credentials

Symantec Messaging Gateway contains a feature that, when enabled, remembers users' login credentials. A Remember me option appears on the Symantec Messaging Gateway Login page when the administrator enables the Remember me feature. When this feature is enabled, it is available to all users, including end users.

When users check the Remember me option as they log onto the Control Center, Symantec Messaging Gateway places a cookie on their computer. (No personal information is stored on the client computer or in the browser.) Thereafter, when users access the Control Center URL, they bypass the Login screen and go directly to the Symantec Messaging Gateway Dashboard page. If the user session times out (sessions timeout after 30 minutes of inactivity), the user is directed to the Dashboard page.

Warning: When users enable this feature, anyone who has access to their computer also has access to the Control Center. This feature is not recommended for administrator logins.

The Remember me feature is browser-specific. For example, assume the user logs onto the Control Center through Internet Explorer and enables the Remember me option. If the user subsequently logs onto the Control Center through Firefox, the user must enter login credentials.

The cookie expires after the number of days that you specify, up to 180 days. However, the expiration might change if you use the strong passwords feature.

The ability to use the Remember me feature with strong passwords depends on the order in which the features are enabled, as follows:

- Strong passwords are enabled first, then the administrator subsequently enables the Remember me feature.
- When the Remember me feature is enabled, if the bypass duration is greater than 60 days (the maximum number of days permitted for strong passwords), then the login bypass duration is set to the same expiration date as the strong password.
- This change is not reflected in the Control Center settings.
- The Remember me feature is enabled first, then the administrator subsequently enables strong passwords.
- The Remember me feature is disabled in the Control Center.
Enabling users to bypass Control Center login credentials

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Click the **Users** tab.
3. Under **User Help**, check **Enable ‘Remember me’ feature**.
4. In the **Login bypass duration** box, type the number of days in which the users' login credentials are valid.
   
   You can enter a value from 1 to 180. The default value is 30 days.
   
   If you modify this value, the change applies to users the next time they select the **Remember me** option at login.
5. Click **Save**.

Configuring the replication of end user preference data

In the Control Center, replication refers to the process by which user preferences are propagated from the Control Center to attached and enabled Scanners. Global settings in the Control Center control the replication process.

You can check the status of automated user preferences from the **Status > Scheduled Tasks** page.

See “About scheduled tasks” on page 648.

To configure the replication of end user preference data

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Click the **Users** tab.
3. In the **Replication frequency** box and drop-down list, you can set the replication frequency.
   
   You can choose **Never** to turn off replication.
4. In the **Replication start time** drop-down lists, you can specify the time at which replication starts.
5. You can click **Replicate Now** to have LDAP data replicated to all attached and enabled Scanners immediately.
6. You can click **Delete Now** to delete all end user preference data.
7. Click **Save**.
Setting up your SMTP greetings and postmaster address

When Symantec Messaging Gateway connects with other mail servers to initiate inbound or outbound messaging traffic, the SMTP protocol conversation begins with a greeting.

By default, Symantec Messaging Gateway uses the following greeting:

Symantec Messaging Gateway

You can change both the inbound SMTP greeting and the outbound SMTP greeting that Symantec Messaging Gateway uses.

You can also change the postmaster address. Symantec Messaging Gateway includes the postmaster address in bounce messages.

See “Configuring Control Center SMTP settings for alerts and reports” on page 694.

To set up your SMTP greetings and postmaster address

1. In the Control Center, click **Protocols > SMTP > Settings**.

2. On the **SMTP** tab, highlight the text in the **Inbound SMTP greeting** field and type the text you want to use.

3. Highlight the text in the **Outbound SMTP greeting** field and type the text you want to use.

4. Highlight the text in the **Postmaster address** field and type the email address that you want to use.
   
   The postmaster address must be a valid email address or 'postmaster'.

5. Click **Save**.

Setting up alerts

Table 23-15 describes the tasks that you can perform to set up various types of alerts. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Familiarize your self with the types of alerts that you can configure for Symantec Messaging Gateway.</td>
<td>Alerts are automatic email notifications sent to inform administrators of the conditions that potentially require attention. You can choose the types of alerts sent, the From: header that appears in alerts messages and which administrators receive them. See “Types of alerts” on page 684.</td>
</tr>
</tbody>
</table>
Table 23-15  Set up alerts (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the alerts that you want.</td>
<td>You can configure alerts for Symantec Messaging Gateway events such as email queue size, Spam Quarantine size, license expiration, and hardware issues. You can specify the email address that appears in the alert notification email and how frequently alerts are sent. Except for the UPS status alert, alerts are not sent at the exact time that the alert condition occurs. Instead, alerts are sent at configurable intervals (the default is hourly). See “Configuring alerts” on page 688.</td>
</tr>
<tr>
<td>Have alerts sent to you to notify you of low disk space on the appliance.</td>
<td>To ensure that the system notifies you when Scanner disk space nears or reaches capacity, you must enable low disk space alerts.</td>
</tr>
<tr>
<td>Have alerts sent to you to notify you that a scheduled task failed.</td>
<td>Symantec Messaging Gateway lets you set an email alert when a scheduled task fails to execute. If a task fails, an email notification is sent to the designated administrator, indicating which task failed and on which host. Control Center logs provide further details about the failure. See “Setting scheduled task failure alerts” on page 693.</td>
</tr>
<tr>
<td>Specify SMT alert and report settings.</td>
<td>You must supply the SMTP host IP address and port number to which you want the Control Center to send information. See “Configuring Control Center SMTP settings for alerts and reports” on page 694.</td>
</tr>
</tbody>
</table>

Types of alerts

Alerts are automatic email notifications sent to inform administrators of the conditions that potentially require attention. You can choose the types of alerts sent, the From: header that appears in alerts messages, and which administrators receive them.

See “Configuring alerts” on page 688.

Table 23-16 describes the available alert settings.

Table 23-16  Alerts page

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification Sender</td>
<td>These settings apply to all alerts</td>
</tr>
<tr>
<td>Notification Frequency</td>
<td>The interval at which notifications are sent. The default is hourly.</td>
</tr>
<tr>
<td>Send from</td>
<td>The email address that appears in the alert notification’s From: header.</td>
</tr>
</tbody>
</table>
### Table 23-16  
**Alerts page (continued)**

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alert Recipients</strong></td>
<td>The email addresses of non-local administrators to whom you want to send alerts.</td>
</tr>
<tr>
<td><strong>Administrator Alerts</strong></td>
<td>Select and deselect local administrators to whom you want to send alerts.</td>
</tr>
<tr>
<td><strong>Outbreaks</strong></td>
<td>Alerts related to virus outbreaks</td>
</tr>
<tr>
<td><strong>Outbreak detection</strong></td>
<td>An alert is sent when a designated number of viruses have been detected over the specified number of hours, days, weeks, or months.</td>
</tr>
<tr>
<td><strong>Filters</strong></td>
<td>Alerts related to spam or virus filters</td>
</tr>
<tr>
<td><strong>Spam filters are older than</strong></td>
<td>An alert is sent because of the period of time between updates of spam filters. Spam filters update periodically, at different intervals for different types of filters. To avoid unnecessary alerts, a minimum setting of two hours is recommended.</td>
</tr>
<tr>
<td><strong>Virus filters are older than</strong></td>
<td>An alert is sent because of the period of time between the virus filter updates which typically occur several times a week. To avoid unnecessary alerts, a minimum setting of seven days is recommended. The default setting is 10 days.</td>
</tr>
<tr>
<td><strong>New virus filters are available</strong></td>
<td>An alert is sent because new virus rules are available for download.</td>
</tr>
<tr>
<td><strong>Queues</strong></td>
<td>Alerts related to message queues</td>
</tr>
<tr>
<td><strong>The combined message queue is larger than</strong></td>
<td>An alert is sent when the total combined size of all message queues exceeds the size specified next to the alert description. Message queues include Inbound, Outbound, Content Analysis, and Delivery. Inbound, Outbound, and Delivery queues can grow if the particular queue has stopped or paused, or if an undeliverable message is blocking a queue. Content Analysis queues can grow if a Content Analysis server is busy or unavailable.</td>
</tr>
<tr>
<td><strong>A queue reaches the message limit</strong></td>
<td>An alert is sent when the inbound, outbound, or delivery queue exceeds the maximum number of messages set on the SMTP Advanced Settings page for a scanner. An alert is also sent when the Content Analysis queue exceeds the maximum number of messages set on the Threat Defense &gt; Settings &gt; Scan Settings &gt; Threat Defense Scan Settings page. See “Configuring SMTP advanced settings” on page 54.</td>
</tr>
<tr>
<td><strong>Disk Space</strong></td>
<td>Alerts related to available disk space</td>
</tr>
</tbody>
</table>
Table 23-16  Alerts page (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available disk space is less than</td>
<td>An alert is sent when the amount of free disk space on the appliance is less than the size that you specify. Low disk space can cause performance and stability issues in Symantec Messaging Gateway.</td>
</tr>
<tr>
<td>Usage of the maximum configured disk space for Spam Quarantine exceeds</td>
<td>An alert is sent when the disk space used by Spam Quarantine exceeds the percentage of the configured maximum size of Spam Quarantine. Set the maximum size of Spam Quarantine on the Spam &gt; Settings &gt; Quarantine Settings page. See “Modifying Spam Quarantine thresholds” on page 287.</td>
</tr>
<tr>
<td>Usage of the maximum configured disk space for a Content Incident Folder exceeds</td>
<td>An alert is sent when the disk space that is available for any content incident folder exceeds the percentage that is specified. See “About managing the size of content incident folders” on page 420.</td>
</tr>
<tr>
<td>Low disk space prompts reduced or halted logging</td>
<td>An alert is sent when the Scanner disk space nears or reaches capacity and the system reduces or halts logging. See “About log disk space alerts” on page 625.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Alerts related to SMTP authentication</td>
</tr>
<tr>
<td>Login failures occur for a single user</td>
<td>An alert is sent when a user attempts to login using SMTP authentication and fails, if the failures for that user are equal or exceed the number specified during the time interval specified. You can also specify maximum number of users to display in each notification.</td>
</tr>
<tr>
<td>Login failures occur from a single IP</td>
<td>An alert is sent when a user attempts to login using SMTP authentication and fails, if the failures for that IP address are equal or exceed the number specified during the time interval specified. You can also specify maximum number of IP addresses to display in each notification.</td>
</tr>
<tr>
<td>DDS</td>
<td>Alerts related to directory data service</td>
</tr>
<tr>
<td>Directory Data access errors</td>
<td>An alert is sent because the directory data service failed to read data from an LDAP server.</td>
</tr>
<tr>
<td>Directory data integrity errors</td>
<td>Indicates a problem with the customer’s directory data that prevents a directory data service operation from succeeding.</td>
</tr>
<tr>
<td>Undersized data source cache</td>
<td>An alert is sent because a directory data source cache or cache index is not large enough to hold all of the requested data in memory.</td>
</tr>
<tr>
<td>User preference replication errors</td>
<td>An alert is sent because of an error replicating user preferences to the Scanner.</td>
</tr>
</tbody>
</table>
Table 23-16  Alerts page (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>License/Updates</td>
<td>Alerts related to licenses, certificates, and software updates</td>
</tr>
<tr>
<td>Symantec Premium Content Control license expired</td>
<td>An alert is sent when the PCC license approaches expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Symantec Antivirus license expired</td>
<td>An alert is sent when your antivirus license approaches expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Symantec Antispam license expired</td>
<td>An alert is sent when your Symantec Antispam license approaches expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Symantec Content Encryption license expired</td>
<td>An alert is sent when your Symantec Content Encryption license approaches expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Software Updates license expired</td>
<td>An alert is sent when your software update license approaches expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>SSL/TLS certificate expiration warning</td>
<td>An alert is sent when a certificate expires. You can check the status of your certificates by going to the Certificate Settings page and clicking View. The first expiration warning is sent seven days before the expiration date. A second warning is sent one hour later. No more than two warnings per certificate are sent.</td>
</tr>
<tr>
<td>New software release update available</td>
<td>An alert is sent to indicate that a new software update release is available.</td>
</tr>
<tr>
<td>Frequency of checking for updates:</td>
<td>Specify the frequency in minutes, hours, or days at which Symantec Messaging Gateway checks for new software updates.</td>
</tr>
<tr>
<td>Events</td>
<td>An alert related to system operations</td>
</tr>
<tr>
<td>Swap space utilization exceeds</td>
<td>An alert is sent when the available memory for swap exceeds the percentage you specify.</td>
</tr>
<tr>
<td>A service is not responding or working</td>
<td>An alert is sent because of a nonresponsive service. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, and directory data service.</td>
</tr>
<tr>
<td>Hardware failures</td>
<td>An alert is sent due to a hardware problem such as a fan or disk failure.</td>
</tr>
</tbody>
</table>
Table 23-16 Alerts page (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service start after improper shutdown</td>
<td>An alert is sent because a service restarted after an improper shutdown. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, and directory data service.</td>
</tr>
<tr>
<td>Service shutdown</td>
<td>An alert is sent because a service was shut down normally. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, and directory data service.</td>
</tr>
<tr>
<td>Service start</td>
<td>An alert is sent because a service was started. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, Agent, and directory data service.</td>
</tr>
<tr>
<td>UPS status</td>
<td>An alert is sent because the uninterruptible power supply status has changed. This alert can be sent as frequently as every seven minutes.</td>
</tr>
<tr>
<td>Failed Scheduled Tasks</td>
<td>An alert is sent when a task you have scheduled fails to execute. Scheduled tasks are configured in their respective tabs but the status of all scheduled tasks can be viewed on the Status &gt; System &gt; Scheduled Tasks page.</td>
</tr>
</tbody>
</table>

Configuring alerts

Alerts are automatic email notifications that Symantec Messaging Gateway sends to administrators when certain conditions may require attention. You can choose the types of alerts to send, the From: header that appears in alerts messages, and which administrators receive alerts.

Note: For an administrator to receive alerts, you must select Enable alert notifications for this Administrator when you add or edit the administrator from the Administration > Users > Administrators page.

See “Setting up local and LDAP administrator accounts” on page 658.

To set up alerts

1. Select Administration > Settings > Alerts.
2. From the Notification Frequency menus, select how often you want SMG to send notifications.
   SMG does not send alerts at the exact time that the alert condition occurs. The Notification Frequency that you set determines when all alerts except UPS status alerts are sent.
3. In the Send from box, type the email address from which you want to send all alerts.
4. In the Alert recipient addresses box, type the email addresses of the non-local administrators to whom you want to send alerts.
5  In the **Administrator Alerts** list, select or deselect the local administrators to whom you want to send alerts.

6  Click through each tab and set up the alert conditions for each type of alert.

   See the section called “Outbreaks” on page 689.

   See the section called “Filters” on page 689.

   See the section called “Queues” on page 690.

   See the section called “Disk Space” on page 690.

   See the section called “SMTP” on page 691.

   See the section called “DDS” on page 691.

   See the section called “License/Updates” on page 692.

   See the section called “Events” on page 693.

7  Click **Save**.

**Outbreaks**

Set up alerts for virus outbreaks.

**Table 23-17**  Outbreaks tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbreak detection</td>
<td>Enable <strong>Outbreak detection</strong> to send an alert when a designated number of viruses are detected over the specified number of hours, days, weeks, or months.</td>
</tr>
<tr>
<td>Threshold value</td>
<td>Select the minimum number of virus detections to trigger an alert.</td>
</tr>
<tr>
<td>Interval</td>
<td>Select the time period over which the threshold number of viruses must be reached to trigger an alert.</td>
</tr>
</tbody>
</table>

**Filters**

Set up alerts that are related to spam or virus filter updates

**Table 23-18**  Filters tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam and unwanted email filters are older than</td>
<td>An alert is sent because of the period of time between updates of spam filters. Spam filters update periodically, at different intervals for different types of filters. To avoid unnecessary alerts, a minimum setting of two hours is recommended.</td>
</tr>
</tbody>
</table>
Table 23-19  Filter tab (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus filters are older than 7 days</td>
<td>An alert is sent because of the period of time between virus filter updates which typically occur several times a week. To avoid unnecessary alerts, a minimum setting of 7 days is recommended. The default setting is 10 days.</td>
</tr>
</tbody>
</table>

Queues

Set up alerts for message queue limits

Table 23-19  Queues tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The combined message queue is larger than 10</td>
<td>An alert is sent when the total combined size of all message queues exceeds the size specified next to the alert description. Message queues include Inbound, Outbound, Content Analysis, and Delivery. Inbound, Outbound, and Delivery queues can grow if the particular queue has stopped or paused, or if an undeliverable message is blocking a queue. Content Analysis queues can grow if a Content Analysis server is too busy or is unavailable.</td>
</tr>
<tr>
<td>A queue reaches the message limit</td>
<td>An alert is sent when the inbound, outbound, or delivery queue exceeds the maximum number of messages set on the SMTP Advanced Settings page for a scanner. See “Configuring SMTP advanced settings” on page 54. An alert is also sent when the Content Analysis queue exceeds the maximum number of messages set on the Threat Defense &gt; Settings &gt; Scan Settings &gt; Threat Defense Scan Settings page. See “Configuring threat defense scan settings” on page 458.</td>
</tr>
</tbody>
</table>

Disk Space

To ensure that the system notifies you when Scanner disk space nears or reaches capacity, set up low disk space alerts.

Table 23-20  Disk Space tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available disk space is less than 500MB</td>
<td>An alert is sent when the amount of free disk space on the appliance is less than the size that you specify. Low disk space can cause performance and stability issues in Symantec Messaging Gateway.</td>
</tr>
</tbody>
</table>
Table 23-20  Disk Space tab (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage of the maximum configured disk space for Spam Quarantine exceeds</td>
<td>An alert is sent when the disk space used by Spam Quarantine exceeds the percentage of the configured maximum size of Spam Quarantine. Set the maximum size of Spam Quarantine on the Spam &gt; Settings &gt; Quarantine Settings page.</td>
</tr>
<tr>
<td></td>
<td>See “Modifying Spam Quarantine thresholds” on page 287.</td>
</tr>
<tr>
<td>Usage of the maximum configured disk space for a Content Incident Folder</td>
<td>An alert is sent when the disk space that is available for any content incident folder exceeds the percentage that is specified.</td>
</tr>
<tr>
<td>exceeds</td>
<td>See “About managing the size of content incident folders” on page 420.</td>
</tr>
<tr>
<td>Low disk space prompts reduced or halted logging</td>
<td>An alert is sent when the Scanner disk space nears or reaches capacity and the system reduces or halts logging.</td>
</tr>
<tr>
<td></td>
<td>See “About log disk space alerts” on page 625.</td>
</tr>
</tbody>
</table>

SMTP

Set up alerts for failed SMTP authentications.

You must supply the SMTP host IP address and port number to which you want the Control Center to send information.

See “Configuring Control Center SMTP settings for alerts and reports” on page 694.

Table 23-21  SMTP tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login failures occur for a single user</td>
<td>An alert is sent when a user attempts to login using SMTP authentication and fails, if the failures for that user equal or exceed the number specified during the time interval specified. You can also specify maximum number of users to display in each notification.</td>
</tr>
<tr>
<td>Login failures occur from a single IP</td>
<td>An alert is sent when a user attempts to login using SMTP authentication and fails, if the failures for that IP address equal or exceed the number specified during the time interval specified. You can also specify maximum number of IP addresses to display in each notification.</td>
</tr>
</tbody>
</table>

DDS

Set up alerts for directory data service (DDS) issues.
### Table 23-22 DDS tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Data access errors</td>
<td>An alert is sent because the directory data service failed to read data from an LDAP server.</td>
</tr>
<tr>
<td>Directory data integrity errors</td>
<td>Indicates a problem with the customer's directory data that prevents a directory data service operation from succeeding.</td>
</tr>
<tr>
<td>Undersized data source cache</td>
<td>An alert is sent because a directory data source cache or cache index is not large enough to hold all of the requested data in memory.</td>
</tr>
<tr>
<td>User preference replication errors</td>
<td>An alert is sent because of an error replicating user preferences to the Scanner.</td>
</tr>
</tbody>
</table>

### License/Updates

Set up alerts for issues with licenses, certificates, and software updates.

### Table 23-23 License/Updates tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Premium Content Control license expired</td>
<td>An alert is sent when the PCC license is approaching expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Symantec Antivirus license expired</td>
<td>An alert is sent when your antivirus license is approaching expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Symantec Antispam license expired</td>
<td>An alert is sent when your Symantec AntiSpam license is approaching expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Symantec Content Encryption license expired</td>
<td>An alert is sent when your Symantec Content Encryption license approaches expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>Software Updates license expired</td>
<td>An alert is sent when your software update license is approaching expiration. Another alert is sent when your license expires. Contact your Symantec sales representative for assistance.</td>
</tr>
<tr>
<td>SSL/TLS certificate expiration warning</td>
<td>An alert is sent when a certificate expires. You can check the status of your certificates by going to the Certificate Settings page and clicking View. The first expiration warning is sent seven days prior to the expiration date. A second warning is sent one hour later. No more than two warnings per certificate are sent.</td>
</tr>
</tbody>
</table>
Table 23-23  License/Updates tab (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>New software release update available</td>
<td>An alert is sent when a new software update release is available.</td>
</tr>
<tr>
<td>Frequency of checking for updates:</td>
<td>Specify the frequency in minutes, hours, or days at which Symantec Messaging Gateway checks for new software updates.</td>
</tr>
</tbody>
</table>

**Events**

Set up alerts for issues with system operations.

Table 23-24  Events tab

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swap space utilization exceeds</td>
<td>An alert is sent when the available memory for swap exceeds the percentage you specify.</td>
</tr>
<tr>
<td>Service is not responding or working</td>
<td>An alert is sent because of a nonresponsive service. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, and directory data service.</td>
</tr>
<tr>
<td>Hardware failures</td>
<td>An alert is sent due to a hardware problem such as a fan or disk failure.</td>
</tr>
<tr>
<td>Service start after improper shutdown</td>
<td>An alert is sent because a service restarted after an improper shutdown. Services include the Agent, Conduit, LiveUpdate, Brightmail Engine, MTA, and directory data service.</td>
</tr>
<tr>
<td>Service shutdown</td>
<td>An alert is sent because a service was shut down normally. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, and directory data service.</td>
</tr>
<tr>
<td>Service start</td>
<td>An alert is sent because a service was started. Services include the Conduit, LiveUpdate, Brightmail Engine, MTA, Agent, and directory data service.</td>
</tr>
<tr>
<td>UPS status</td>
<td>An alert is sent because the uninterruptible power supply status has changed. This alert can be sent as frequently as every seven minutes.</td>
</tr>
<tr>
<td>Scheduled tasks failures</td>
<td>An alert is sent when a scheduled task fails to execute. Control Center logs provide additional details about the failure. Scheduled tasks are configured in their respective tabs but the status of all scheduled tasks can be viewed on the <strong>Status &gt; System &gt; Scheduled Tasks</strong> page.</td>
</tr>
</tbody>
</table>

**Setting scheduled task failure alerts**

Symantec Messaging Gateway lets you set an email alert when a scheduled task fails to execute. If a task fails, an email notification is sent to the designated administrator, indicating
which task failed and on which host. Control Center logs provide further details about the failure.

To set scheduled tasks failures alerts

1. In the Control Center, click Administration > Settings > Alerts.
2. Under the Events tab, check Scheduled tasks failures, and click Save.

See “About scheduled tasks” on page 648.
See “Scheduled task types” on page 649.

Configuring Control Center SMTP settings for alerts and reports

The Control Center sends the following information to designated email addresses and repositories at your site:

- Alert notifications
- Reports
- Spam Quarantine messages

You must supply the SMTP host IP address and port number to which you want the Control Center to send information.

---

**Note:** Symantec Messaging Gateway verifies that the product version that runs on the Control Center and the Scanner are the same. If the product versions are not the same, Symantec Messaging Gateway issues an error message. You should perform a software update on the Scanner and define the SMTP host on the Control Center Setting page again.

See “Downloading and installing a software update” on page 721.

---

To configure Control Center SMTP settings for alerts and reports

1. In the Control Center, click Administration > Settings > Control Center.
2. Click the SMTP tab.
3 Under **Control Center SMTP Settings** do one of the following:

To specify that the email that the Control Center generates should use the non-local relay to send email

Click **Use existing non-local relay settings**.

See “Configuring Scanner inbound email delivery settings” on page 48.

To specify the IP address or fully-qualified domain name of a computer that has a working MTA on it

Click **Define new host**.

Change this setting from the default if a Scanner is not installed on the same appliance as the Control Center. Specify the port to use for SMTP. The default is 25.

4 Click **Save**.

**Managing passwords**

Table 23-25 describes the tasks that you can perform to manage passwords. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset a password.</td>
<td>You may need to reset a Control Center administrator password if an administrator has forgotten the password. See “Resetting an administrator password” on page 696.</td>
</tr>
<tr>
<td>Require strong passwords to enhance Control Center access security.</td>
<td>Strong passwords make access to the Control Center more secure. When you enable the strong password feature, the current passwords for all administrators expire. However, the password for the admin administrator does not expire. Administrators must set new strong passwords the next time that they access the Control Center. See “Enforcing strong passwords” on page 696.</td>
</tr>
<tr>
<td>Know the strong password criteria.</td>
<td>When you enable the strong password feature, passwords must meet a minimum criteria (such as eight characters or longer). See “Strong password criteria” on page 698.</td>
</tr>
<tr>
<td>Familiarize yourself with some best practices for passwords.</td>
<td>View suggestions for creating secure passwords. See “Password best practices” on page 697.</td>
</tr>
</tbody>
</table>
Resetting an administrator password

You may need to reset a Control Center administrator password if an administrator has forgotten the password.

**Note:** Only the admin administrator can change another administrator's password if the "Require strong passwords" setting is enabled and the one-day minimum password age is not met. In other cases, any administrator with Manage Administration rights can change another administrator’s password.

See “Administrator rights” on page 661.

After resetting an administrator's password, use a secure method (such as a phone call) to notify the administrator of the new password. Email is not typically a secure method.

See “Enforcing strong passwords” on page 696.

See “Editing an administrator” on page 667.

To reset an administrator password

1. In the Control Center, click **Administration > Users > Administrators**.
2. Check the box beside the administrator whose password you want to change, and click **Edit**.
3. In the **Password** box, type the new password.
4. In the **Confirm password** box, type the password again.
5. Click **Save**.

Enforcing strong passwords

You can enable or disable strong passwords. Strong passwords make access to the Control Center more secure. When you enable the strong password feature, the current passwords for all administrators expire. However, the password for the admin administrator does not expire. Administrators must set new strong passwords the next time that they access the Control Center.

If you disable the strong password feature, the password history is erased. If you later turn on strong passwords again, administrators may reuse their old passwords that would not have been allowed if strong passwords were enabled.

The ability to use strong passwords with the **Remember me** feature depends on the order in which the features are enabled, as follows:
When the **Remember me** feature is enabled, if the bypass duration is greater than 90 days (the maximum number of days permitted for strong passwords), then the login bypass duration is set to the same expiration date as the strong password. This change is not reflected in the Control Center settings.

The **Remember me** feature is enabled first, then the administrator subsequently enables strong passwords.

The **Remember me** feature is disabled in the Control Center.

To enforce strong passwords

1. In the Control Center, click **Administration > Users > Administrators**.

2. Do one of the following:
   - To enable strong passwords, check **Require strong passwords**.
   - To disable strong passwords, uncheck **Require strong passwords**.

   The new strong password policy takes effect immediately.

3. In the **Password Expiration** box, type the number of days after which users must change their passwords.

   You can type a value between 1 and 90. The default value is 60 days.

See “Strong password criteria” on page 698.

See “Resetting an administrator password” on page 696.

See “Enabling users to bypass Control Center login credentials” on page 681.

**Password best practices**

To create secure passwords, consider the following suggestions:

- Do not create a password that uses any of the following formats:
  - A word that is found in a dictionary (in any language or jargon)
  - A name (such as the name of a spouse, parent, child, pet, fantasy character, famous person, or location)
  - Any variation of your personal name or account name
  - Accessible information about you (such as your phone number, license plate, or social security number) or your environment
  - A birthday or a simple pattern (such as backwards, followed by a digit, or preceded by a digit)
Create a password that is based on the following recommendations:

- Use a mixture of upper and lower case letters, as well as digits or punctuation
- Make sure the password is unrelated to any previous password
- Use long passwords (eight characters or longer)
- Consider using a pair of words with punctuation inserted
- Consider using a pass phrase (an understandable sequence of words)
- Consider using the first letter of each word in a pass phrase

See “Strong password criteria” on page 698.

After you reset an administrator’s password, use a secure method (such as a phone call) to notify the administrator of the new password. Email messages are not typically secure methods.

**Strong password criteria**

Strong passwords must contain all of the following requirements:

- US-ASCII character encoding
- At least eight characters
- At least one uppercase character
- At least one lowercase character
- At least one number

See “Enforcing strong passwords” on page 696.

Strong passwords cannot be changed more frequently than once a day, but they must be changed every 60 days. They cannot be the same password as any of the user’s last five passwords.

**Maintaining an appliance**

Administrators can monitor disk and power usage to ensure that the Control Center, Scanners, and attached devices have adequate disk space and are performing properly.

_Table 23-26_ describes the tasks that you can perform to maintain your appliance. You can perform these tasks as needed in any order.
### Table 23-26  Maintain an appliance

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Learn more about how to maintain adequate disk space. | Symantec Messaging Gateway performs better with more available disk space. Certain features such as extended reporting data and spam quarantine can use a large quantity of disk space and tax system resources. Periodically compare the disk usage to the disk capacity to ensure that the Control Center and Scanners have adequate disk space.  
  See “About maintaining adequate disk space” on page 703. |
| Turn off your appliance when necessary.         | Before you turn off the appliance, first stop the mail flow. As a precaution, you might also want to flush your inbound, outbound, and delivery message queues.  
  See “Turning off an appliance” on page 703. |
| Restart your appliance as needed.               | You can also restart all of your appliances at once. Restarting an appliance entails the appliance turning itself off and then restarting itself.  
  See “Restarting an appliance” on page 699. |
| Return an appliance to the factory default condition. | The reset is the most recent version that is installed on the appliance.  
  See “Resetting an appliance to its factory defaults” on page 700. |
| Configure UPS settings in the event of a power loss. | Symantec Messaging Gateway can monitor USB attached APC UPS devices. It can also perform a graceful shutdown due to loss of power.  
  See “Configuring UPS settings” on page 701. |
| Restore an appliance from a different network configuration. | You may want to perform this task in the following situations:  
  ■ Disaster recovery  
  ■ Datacenter migration  
  ■ Hardware upgrade migration  
  ■ Physical appliance to virtual appliance migration  
  ■ Virtual appliance to physical appliance migration  
  See “Restoring an appliance from a different network configuration” on page 701. |

### Restarting an appliance

You can restart an appliance when needed. You can also restart all of your appliances at once. Restarting an appliance entails the appliance turning itself off and then restarting itself.  

See “Turning off an appliance” on page 703.
To restart an appliance

1. In the Control Center, click Administration > Hosts > Shutdown.
2. Under System Shutdown, click the Host drop-down list and select the appliance that you want to restart. To restart all of your appliances, select All hosts.
3. Click Reboot.

All connections close and the system restarts.

Resetting an appliance to its factory defaults

You can return an appliance to the factory default condition of the most recent version that is installed on the appliance.

When you enable this feature, Symantec Messaging Gateway does all of the following actions for the Host that you select:

- Stops the Scanner host
- Clears the host from the host table
- Clears the logs from the database
- Clears the reports from the database
- Clears the status information from the database
- Resets all settings and policies to their default values
- Deletes all of the backup files that are stored on the appliance
- Disables the spam submission feature and reverts all associated spam submission features back to the factory default settings.
  - This function includes removing all submitter types and submitter addresses and clearing the submitter ID.
  - See “About submitting messages for customer-specific spam rules” on page 265.

**Note:** After you perform a factory reset on a particular Scanner, you must delete the Scanner through the Control Center and then add it again.

See “Adding Scanners” on page 35.

After you reset the appliance, you are automatically logged out.
To reset an appliance to its factory default

1. In the Control Center, click **Administration > Hosts > Version**.

2. On the **Factory Reset** tab, click the **Host** drop-down list and select a single host or **All hosts**.

   The option **All hosts** simultaneously returns all of your hosts to the factory default condition of the most recent version that is installed on the appliance.

3. Click **Reset**.

   A confirmation window appears.

4. Click **Reset** to confirm reset, or click **Cancel** to stop the process.

See “Restarting an appliance” on page 699.

Configuring UPS settings

Symantec Messaging Gateway can monitor USB attached APC UPS devices. It can also perform a graceful shutdown due to loss of power when any one of the following conditions are met:

- **Battery level**: If during a power failure, the remaining battery percentage (as reported by the UPS) is less than or equal to the specified value
- **Runtime minutes**: If during a power failure, the remaining runtime in minutes (as calculated internally by the UPS) is less than or equal the specified value
- **Timeout minutes**: If during a power failure, the UPS has run on batteries for the timeout minutes

   **Note**: If you have a Smart UPS, you can disable the Timeout minutes feature and use the other settings to control when a shutdown is initiated.

See [shutdown](#) on page 815.

To configure UPS settings

1. In the Control Center, click **Administration > Settings > UPS**.

2. Check **Enable UPS Monitoring** and select the conditions under which the appliance turns itself off.

Restoring an appliance from a different network configuration

You can restore an appliance from a different network configuration in any of the following circumstances:

- Disaster recovery
- Data center migration
- Hardware upgrade migration
- Physical appliance to virtual appliance migration
- Virtual appliance to physical appliance migration

**Note:** If you are reconfiguring the Control Center host, delete all logs, configuration, and data. You can delete through the Control Center or the command line interface.

See “Manually deleting log files” on page 624.

See delete on page 752.

Scanner services are not started by default after a restore operation. If you bypass the site setup wizard and execute the `db-restore` command from the command line interface, Scanner services must be started manually after the restore operation.

When the backup is taken from one network configuration and restored on another network configuration, the restore will not be successful, unless the IP addresses of BCC/AIO and additional scanners match the IP addresses taken in the backup.

**To restore an appliance from a different network configuration**

1. Install and configure the new host.
   - The host role that you chose during configuration must be identical to the role of the backup. For example, if the backup is taken from an all-in-one deployment, the new host role must be Control Center and Scanner.

2. Register the new host by importing the license file from the site setup wizard.

3. Optionally, complete the site setup wizard.
   - If you complete the site setup wizard, the setup information is overwritten by the restore operation. However, completing the site setup wizard enables you to perform a software update and restore through the Control Center instead of the command line interface. The site setup wizard also lets you create virtual IPs before the restore operation.
   - See `db-restore` on page 749.

4. Exit the setup wizard by logging out of the Control Center.

5. Ensure that the software version on the new host is the same version present at the time of backup.
   - If the software version is different:
     - Update the host through the command line interface.
     - Update the host through the Control Center if you have completed the site setup.
Log on to each scanner host. Add the new Control Center IP address to the list of allowed IPs in the `/data/scanner/etc/agentconfig.xml` file.

You can add the list of allowed IPs using the `agent-config` command through the command line interface.

See `agent-config` on page 737.

Execute the `db-restore` command on the new host through the command line interface.

See `db-restore` on page 749.

Ensure that the MTA and Control Center certificates are valid on the new host.

If content encryption is enabled, contact a Symantec provisioning representative to provision the new host for content encryption.

About maintaining adequate disk space

Symantec Messaging Gateway performs better with more available disk space. Certain features such as extended reporting data and spam quarantine can use a large quantity of disk space and tax system resources. Periodically compare the disk usage to the disk capacity to ensure that the Control Center and Scanners have adequate disk space.

See “Viewing the status of your hardware” on page 609.

Check Scanners and Control Center for old or unnecessary log files and manually delete them.

See “Clear disk space checklist” on page 625.

To mitigate the burden to the system from over-production of log data, configure the log database size, log levels, and set the purge frequency rate of older log data.

See “Managing the log database size” on page 620.

Specify a smaller disk space usage for spam virus quarantine and content incident folders.

See “Modifying the disk space allotted for Suspect Virus Quarantine” on page 241.

See “About managing the size of content incident folders” on page 420.

Schedule Expungers to run at regular intervals.

See “Scheduled task types” on page 649.

Turning off an appliance

When you turn off an appliance, the process begins immediately. If you have emails in your message queues, those emails remain in the queues. Before you turn off the appliance, first stop the mail flow. As a precaution, you might also want to flush your inbound, outbound, and delivery message queues.
See “MTA and message queue behavior” on page 74.

See “Services and MTA operations” on page 71.

See “Restarting an appliance” on page 699.

To turn off an appliance

1. In the Control Center, click Administration > Hosts > Configuration.
2. Check the box beside the Scanner that you want to turn off and click Edit.
   
   The Edit Host Configuration page appears, showing the Services tab.
3. Under MTA Operation, click Do not accept incoming messages.
4. Click Save.
5. On the Status > SMTP > Message Queues page, view each of the message queues to see if they are empty.
6. Click Flush All to flush any queues that contain messages.
   
   You can also click Delete to delete a message or Delete All to delete all messages in a queue.
7. Repeat the previous step until all queues are empty.
8. On the Administration > Hosts > Shutdown page, click the Host drop-down list to select the host to turn off.
9. Click Shutdown.
   
   Before you turn off power to the appliance, be sure the message Power Down appears on a locally connected video console or through a serial connection.

About Symantec Messaging Gateway and Symantec Protection Center

Symantec Protection Center lets you integrate management of eligible Symantec security products into a single environment. Integrating Symantec Messaging Gateway and your other Symantec security products into Symantec Protection Center gives you the following:

- A Dashboard that provides a common user interface for your eligible security products and lets assess and remediate threats from a single location.
- Aggregated reports that let you combine or compare data from all of your integrated products.
- Real-time feedback from the Symantec Global Intelligence Network (GIN) that provides you with up-to-date information about detected vulnerabilities, threats detected inside customers’ networks, and malicious traffic exiting those networks.
For more information about the Symantec Protection Center, see the Symantec Protection Center product documentation.

See “Integrating Symantec Messaging Gateway with Symantec Protection Center” on page 705.

See “How Symantec Protection Center uses Symantec Messaging Gateway data for enhanced reporting” on page 705.

Integrating Symantec Messaging Gateway with Symantec Protection Center

The Symantec Protection Center implements a new Web service layer that enables Protection Center to communicate with Symantec Messaging Gateway and other integrated applications.

Before you integrate Symantec Messaging Gateway, you must install and configure your Protection Center. Symantec then provides a simple guided process to help you add Symantec Messaging Gateway and other supported products to the Protection Center. For detailed information about how to set up your Protection Center and add products see the Protection Center documentation.

To integrate Symantec Messaging Gateway with Protection Center, ensure that the Protection Center server(s) can communicate with all Symantec Messaging Gateway appliances over port 8443. Depending on your environment, this may require firewall changes.

See “About Symantec Messaging Gateway and Symantec Protection Center” on page 704.

See “How Symantec Protection Center uses Symantec Messaging Gateway data for enhanced reporting” on page 705.

How Symantec Protection Center uses Symantec Messaging Gateway data for enhanced reporting

In addition to the standard reports already available from the Symantec Messaging Gateway, Protection Center provides reports that can combine data from multiple integrated products. For example, if you have integrated Symantec Messaging Gateway and Symantec Endpoint Protection into your protection center console, you can run reports that combine data from both.

You can filter and save these reports and distribute them through email. For more information about Protection Center reports, see the Protection Center documentation.

See “About Symantec Messaging Gateway and Symantec Protection Center” on page 704.

Managing backups

Table 23-27 describes the tasks that you can perform to manage backups. You can perform these tasks as needed in any order.
Table 23-27  Manage backups

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule backups to occur automatically at a designated time.</td>
<td>You can schedule a full backup, a partial backup, or a backup of system configurations only. See “Scheduling backups” on page 706.</td>
</tr>
<tr>
<td>Modify a backup schedule.</td>
<td>Make modifications to the scheduled backup as needed, such as the time of the backup and what gets backed up. See “Editing a scheduled backup” on page 709.</td>
</tr>
<tr>
<td>Delete a backup schedule when you no longer need it.</td>
<td>Once you delete a scheduled backup, it cannot be restored. See “Deleting a scheduled backup” on page 709.</td>
</tr>
<tr>
<td>Perform a manual backup as needed.</td>
<td>You may want to perform this task before you do any maintenance on your appliance or purge or delete data. See “Performing an on-demand backup” on page 709.</td>
</tr>
<tr>
<td>Restore your appliance from a backup.</td>
<td>If you have previously backed up your databases, it is possible to restore them from any of the available backup stores. If you restore a backup from one appliance to a different physical appliance, make sure that the date is set correctly on the new appliance. This verification ensures that messages in quarantine at the time of the original backup are displayed correctly after the restore. See “Restoring an appliance from backups” on page 711.</td>
</tr>
<tr>
<td>Understand best practices for backing up log data.</td>
<td>In general, there is no reason to backup log files. For troubleshooting purposes, the logs that are not set to Information or Debug (which provides the most detail) have limited use. See “About backing up log data” on page 713.</td>
</tr>
</tbody>
</table>

Scheduling backups

As a best practice, schedule frequent backups to ensure that you have current configuration information and data available should you need it.

You can schedule a full backup, a backup of policies only, or a configuration backup of the items that you specify. Once your backup schedule is set, you can monitor the backup status from the Status > Scheduled Tasks page.

See “About scheduled tasks” on page 648.

The ability to customize your backup type gives you greater flexibility. For example, assume that you want to back up and maintain messages in incident folders or compliance requirements but do not have enough storage space. You can back up policies plus content incidents and
store the backup off-box. Or you may have a situation where you want to copy the policies that you have on one Control Center to another. You can back up the policies and restore them on the other Control Center.

Backups do not include the actual license files (license files have the extension .slf). So when you restore a backup, you must re-register your licenses. If you cannot locate your license files, you must request new ones.

See “Obtaining replacement license files” on page 716.

You can restore your backup when needed; however, there are considerations you should keep in mind before you do.

See “Restoring an appliance from backups” on page 711.

---

**Note:** The `db-backup` command can back up your appliance with SCP. The Control Center also offers this option.

See `db-backup` on page 744.

---

**To schedule backups**

1. **In the Control Center, click Administration > Hosts > Version.**

2. On the **Backup** tab, click **Add**.

   The **Add Scheduled Backup** page appears.

3. Under **Backup description**, give the backup a name.

4. Under **Backup Data**, choose from the following backup types:

   - **Full Backup**: Backs up the complete database, as well as the following items:
     - Spam Quarantine messages
     - Suspect Virus Quarantine messages
     - Spam submission submitter ID
     - Spam submission submitters list
     - Content filtering messages in Informational Incidents folders that are stored on disk
     - Content filtering messages in the Quarantine Incidents folders that are stored on disk.
The Custom backup option includes the following sub-options:

- **Policies only**
  Backs up spam, malware, reputation, and content filtering policies, Threat Defense policies, policy groups, and all policy resources.

- **Configuration (includes policies)**
  Backs up all configuration data, which includes all modifiable settings in the Control Center, the spam submission submitter ID, and the submitters list, and policies. Also backs up the additional items that you select as follows:
  - Include content incident messages
    In addition to configuration data and policies, backs up all of the messages that are in all of the content incident folders.
  - Include report data
    In addition to configuration data and policies, backs up all of the report data.
  - Include log data
    In addition to configuration data and policies, backs up all of the log data.

5. Under **Backup Schedule**, define the time and frequency to run the backup.

6. Under **Backup To**, select one of the following:

   - **Store backup on server**
     This option stores backups on the local server. Specify how many backup versions to keep using the **Number of backups to store** field.
     You only need to specify the number of backup versions that are retained when you store files locally. Enter a value between 1 and 25. The default value is 3.

   - **Store backup on a remote location**
     Specify the following values:
     - **Protocol**: Select FTP or SCP from drop-down
     - **Host/IP Address**: example: host.symantecs.org (or 192.168.2.42)
     - **Port number**
     - **Enter the path. For example**: /home/username/backups/
     - **Check to indicate if the transfer requires authentication.**
       If it does, specify the following:
       - **User name**
       - **Password**

7. Click **Save**.
Editing a scheduled backup

You can modify a scheduled backup as needed.

To edit a scheduled backup

1. In the Control Center, click **Administration > Hosts > Version**.
2. On the **Backup** tab, check the box beside the backup that you want to edit.
3. Click **Edit**.

   The **Edit Scheduled Backup** page appears.

4. Edit options for the scheduled backup.
5. Click **Save**.

Deleting a scheduled backup

You can delete a scheduled backup when it is no longer needed.

See “Scheduling backups” on page 706.

To delete a scheduled backup

1. In the Control Center, click **Administration > Hosts > Version**.
2. On the **Backup** tab, check the box beside the backup that you want to delete.
3. Click **Delete**.

Performing an on-demand backup

You can perform a full backup, a backup of policies only, or a configuration backup of the items you specify at any time.

The ability to customize your backup type gives you greater flexibility. For example, assume that you want to back up and maintain messages in incident folders for compliance requirements but do not have enough storage space. You can back up policies plus content incidents and store the backup off-box. Or you may have a situation where you want to copy the policies that you have on one Control Center to another. You can backup the policies and restore them on the other Control Center.

Backups do not include the actual license files (license files have the extension .slf). So when you restore a backup, you must re-register your licenses. If you cannot locate your license files, you must request new ones.

See “Obtaining replacement license files” on page 716.

You can restore your backup when needed; however, there are considerations you should keep in mind before you do.
See “Restoring an appliance from backups” on page 711.

Note: The db-backup command can back up your appliance with SCP. The Control Center also offers this option.
See db-backup on page 744.

To perform an on-demand backup

1 In the Control Center, click Administration > Hosts > Version.
2 On the Backup tab, click Backup Now.
3 Under Backup Data, choose from among the following backup types:

**Full Backup**

Backs up the complete database, as well as the following items:
- Spam Quarantine messages
- Suspect Virus Quarantine messages
- Spam submission submitter ID
- Spam submission submitters list
- Content filtering messages in Informational Incidents folders that are stored on disk
- Content filtering messages in the Quarantine Incidents folders that are stored on disk.

**Custom backup**

The Custom backup option includes the following sub-options:
- **Policies only**
  Backs up spam, malware, reputation, and content filtering policies, Threat Defense policies, policy groups, and all policy resources.
- **Configuration (includes policies)**
  Backs up all configuration data, which includes all modifiable settings in the Control Center, the spam submission submitter ID, and the submitters list, and policies. Also backs up the additional items that you select as follows:
  - Include content incident messages
    In addition to configuration data and policies, backs up all of the messages that are in all of the content incident folders.
  - Include report data
    In addition to configuration data and policies, backs up all of the report data.
  - Include log data
    In addition to configuration data and policies, backs up all of the log data.
4 Under **Backup To**, select one of the following:

- **Store backup on server**
  This option stores backups on the local server. Specify how many backup versions to keep using the **Number of backups to store** field.
  
  You only need to specify the number of backup versions that are retained when you store files locally. Enter a value between 1 and 25. The default value is 3.

- **Store backup on a remote location**
  Specify the following values:
  - Protocol: Select FTP or SCP from drop-down
  - Host/IP Address: example: host.symantecs.org (or 192.168.2.42)
  - Port number.
  - Enter the path. For example: /home/username/backups/
  - Check to indicate if the transfer requires authentication.
    
    If it does, specify the following:
    - User name
    - Password

5 Click **Backup Now**.

**Restoring an appliance from backups**

You can restore manual or scheduled backups as needed.

The following are some things you should know about restoring a backup:

- You must restore a backup must to the same product version on which it was created.
- For a policies only back up, policy group membership backup details must align with the DDS configuration of the Control Center on which you restore the backup.
  DDS configuration is not included in a policies only back up, but it is included in full and configuration backups.
- For a policies only backup, content filtering policy actions must align with the incident folder configuration of the Control Center on which you restore the backup.
- For a policies only backup, after restoration a policy group can contain the LDAP members that do not exist in the configured address resolution data sources.
- For a policies only backup, after restoration you must ensure that the policy group members are valid with respect to the configured address resolution data sources.
- If you restore a backup from one appliance to a different physical appliance, make sure that the date is set correctly on the new appliance. This verification ensures that messages in quarantine at the time of the original backup are displayed correctly after the restore.
If you enabled the customer-specific spam feature before you performed the backup, if the backup could be restored but the submission settings could not, a message to that effect appears on the login page. To resolve the issue, go to the Spam > Settings > Submission Settings page and click Save. The Control Center synchronizes your settings with the settings on the Symantec server, and thereby restores your customer-specific spam submissions configuration.

**Note:** When the backup is taken from one network configuration and restored on another network configuration, the restore will not be successful, unless the IP addresses of BCC/AIO and additional scanners match the IP addresses taken in the backup. After you restore an appliance that functions as your Control Center from a different IP address than the original IP address, restart the appliance. If that appliance also hosts a Scanner, stop the Scanner first.

See “Restoring an appliance from a different network configuration” on page 701.

After you restore a backup, a message appears. The message provides a brief summary of the restore process and describes any subsequent steps that you should take.

See “Restarting an appliance” on page 699.

See “Stopping and starting Scanners” on page 68.

**To restore the appliance from a local backup**

1. In the Control Center, click Administration > Hosts > Version.
2. On the Restore/Download tab, click Restore/Download backup from server.
3. Under Available Backups, check the box beside the backup that you want to restore.
4. Click Restore.

**To download a backup file from the appliance running the Control Center**

1. In the Control Center, click Administration > Hosts > Version.
2. On the Restore/Download tab, click Restore/Download backup from server.
3. Under Available Backups, check the box beside the backup that you want to download.
4. Click Download.
To restore your appliance from a remote backup

1 In the Control Center, click Administration > Hosts > Version.

2 On the Restore/Download tab, click Restore backup from a remote location.
   Supply the protocol, domain (host name) or IP address, port, and fully qualified (absolute) path to the file. Supply authentication information if required.
   The following are sample values for restoring the system from a remote backup:

   | Host/IP address | 192.168.2.42 |
   | Port | 21 |
   | Path | /home/username/backups/file.bz2 |

3 Click Restore.

To restore your system from a local file

1 In the Control Center, click Administration > Hosts > Version.

2 On the Restore/Download tab, click Upload a backup file from your local computer.
   This step assumes that you have a local copy of the backup file, such as from backing up using FTP.

3 Click Restore.

See db-restore on page 749.

See “Scheduling backups” on page 706.

See “Performing an on-demand backup” on page 709.

About backing up log data

In general, there is no reason to back up log files. For troubleshooting purposes, logs that are not set to Information or Debug (which provides the most detail) have limited use. The best practice is to view and save current logs as needed and set the appropriate retention period for logging data.

See “Managing the log database size” on page 620.

Keeping your product current

Table 23-28 describes the tasks that you can perform to keep your appliance current. You can perform these tasks as needed in any order.
### Table 23-28  
**Keep your product current**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Install your license to get updated definitions.** | You obtain a license file from Symantec when you purchase Symantec Messaging Gateway or renew an existing license. You must register the license for each Scanner that you install and enable to use Symantec Messaging Gateway features. You can use the same license file to register multiple Scanners.  
In addition to this license, you can also obtain a separate license to enable Symantec Content Encryption. Content encryption lets you encrypt outbound messages for greater security and to track statistics for those messages through the Control Center.  
See "Licensing your product" on page 714. |
| **View the status of your licenses to determine which features are licensed for each Scanner and when a license expires.** | The **Licenses** page in the Control Center contains all of the Symantec Messaging Gateway features that require licenses. The page also list whether the feature is licensed and when the license expires.  
See “Viewing license statuses” on page 715. |
| **Learn about Symantec Messaging Gateway software updates.** | Symantec periodically releases new versions of the Symantec Messaging Gateway software. New versions contain new features and fixes for software defects. Symantec recommends that you keep your appliance up to date with the latest version of the software. However, some software updates may contain changes to the underlying architecture of Symantec Messaging Gateway.  
See “About software updates” on page 720.  
See “Updating Symantec Messaging Gateway software” on page 717. |
| **Perform Symantec Messaging Gateway software updates.** | You can update your software from the Control Center or at the command line.  
See "Downloading and installing a software update" on page 721.  
See update on page 827.  
See “Monitoring software update using the command line interface” on page 721. |
| **Check your software version number.** | You may want to perform this task before you contact Technical Support.  
See “Determining which version of software is installed” on page 721. |

---

### Licensing your product

You obtain a license file from Symantec when you purchase Symantec Messaging Gateway or renew an existing license. You must register the license for each Scanner that you install.
and enable to use Symantec Messaging Gateway features. You can use the same license file to register multiple Scanners.

**Note:** The basic product functionality for Symantec Messaging Gateway requires a single license. In addition to this license, you can also obtain a separate license to enable Symantec Content Encryption. Content encryption lets you encrypt outbound messages for greater security and to track statistics for those messages through the Control Center.

See “Encrypting data with Symantec Content Encryption” on page 449.

When you obtain your license file from Symantec, save it to a location that you can access from the Control Center.

Symantec Messaging Gateway stores the license serial numbers locally on the appliance. These serial numbers appear on the Administration > Hosts > Licenses page. As a best practice, you should write down these license numbers.

A backup restoration does not affect your licenses. However, if you restore a backup on an unlicensed appliance, no serial numbers appear.

See “Performing an on-demand backup” on page 709.

See “Scheduling backups” on page 706.

See “Restoring an appliance from backups” on page 711.

**To license your product**

1. In the Control Center, click **Administration > Hosts > Licenses**.
2. Click **Browse** and locate the license file.
3. Click **Register License**.

See “Viewing license statuses” on page 715.

See “Obtaining replacement license files” on page 716.

**Viewing license statuses**

You can view the status of your licenses to determine which features are licensed for each Scanner and when a license expires.

The Licenses page in the Control Center contains all of the Symantec Messaging Gateway features that require licenses. The page also list whether the feature is licensed and when the license expires.

**Note:** An alert is sent when a license approaches expiration. Another alert is sent when it expires. Contact your Symantec sales representative for assistance renewing licenses.
To view license statuses

1. In the Control Center, click **Administration > Hosts > Licenses**.
2. In the **Host** drop-down list, select a host name.
   The status of the licenses and their expiration dates appear.

**Obtaining replacement license files**

You may have an instance in which you must obtain new license files. For example, backups do not include the actual license files. So when you restore a backup, you must re-register your licenses. If you cannot locate your license files, you can obtain new ones on the Symantec Licensing Portal.

---

**Note:** The basic product functionality for Symantec Messaging Gateway requires a single license. However, in addition to this license, you can obtain a license to enable Symantec Content Encryption. Content encryption lets you encrypt outbound messages for greater security and to track statistics for those messages through the Control Center.

See “Encrypting data with Symantec Content Encryption” on page 449.

---

Symantec Messaging Gateway stores the license serial numbers locally on the appliance. These serial numbers appear on the **Administration > Hosts > Licenses** page. As a best practice, you should write down these numbers.

A backup restoration does not affect your licenses. However, if you restore a backup on an unlicensed appliance, no serial numbers appear.

See “Restoring an appliance from backups” on page 711.

**To obtain replacement license files**

1. In the Control Center, click **Administration > Hosts > Licenses**.
   The serial numbers for all of the licenses that you registered appear on the **Licenses** page.

2. Make a note of all of the serial numbers for the license files that you need to obtain.

3. On the Internet, go to the following URL:
   
   [https://licensing.symantec.com/acctmgmt/home/LicensePortalHome.jsp](https://licensing.symantec.com/acctmgmt/home/LicensePortalHome.jsp)

4. Type in your Login ID and password, and click **LOGIN**.
   If you do not have a Login ID and password, you must register for one to proceed.

5. On the **Home** page, click **New and Renewal Purchase**.
6 On the **Get a License Key for a New Purchase** page, type the serial number.

7 Click **Submit**.

A list of the serial numbers that you can register together for this product appears.

8 Do one of the following tasks:

   All of the serial numbers that you had previously registered appears.
   - Check the boxes for all of the serial numbers for which you want to obtain new license files, and then click **Next**.

   None or only some of the serial numbers that you had previously registered appears.
   - Do all of the following tasks:
     - Check the boxes for any of the serial numbers that appear for which you want to obtain new license files.
     - Then for any serial numbers that do not appear in the list, type them in the **Serial Number** box, and then click **Add**.
     - Click **Next**.

9 Type the email address and a message to the person to whom you want the license file emailed.

10 Specify the technical contacts who can contact Symantec support.

11 Optionally, add any comments.

12 Click **Complete Registration**.

   Your license file is emailed to the address that you specified. The license file is contained in a .zip file and has an .slf extension.

---

**Warning:** Attempts to modify the contents of the .slf license file may corrupt the file and render it invalid.

---

13 Install your license file.

   See “**Licensing your product**” on page 714.

### Updating Symantec Messaging Gateway software

**Note:** Do not restart or shut down an appliance while the software update runs. The appliance can become corrupted, and you may not be able login to the Control Center afterwards. You can view the Linux console for details. Most likely you will need to reinstall the product.

---

**Table 23-29** describes the steps to prepare and run a software update.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Download current version and burn it on the DVD.</td>
<td>Download current version from <a href="https://fileconnect.symantec.com/">https://fileconnect.symantec.com/</a> and burn it in a DVD for recovery purposes.</td>
</tr>
</tbody>
</table>
| Step 2 | Read software update documentation. | Read the software update notes, release notes, and late-breaking news for the software update. The documentation may describe special steps to prepare for the software update.  
See “About software updates” on page 720.  
See “Downloading and installing a software update” on page 721. |
| Step 3 | Reduce stored data before performing a backup. | Symantec recommends you to reduce storage utilization before upgrading the Control Center appliance. Reducing stored data before performing a backup frees disk space for a backup operation and also reduces the software update time.  
You can reduce stored data by performing any or all of the following steps:  
- Spam and content quarantined messages are stored in the Control Center disks.  
  Delete all messages from spam quarantine and content quarantine to free the Control Center disk space.  
  See delete on page 752.  
- Reports and logging data are stored in the Control Center database.  
  To reduce the Control Center database:  
  - Purge all reports.  
  - If your site policies let you, delete all log files.  
  See “Manually deleting log files” on page 624. |
| Step 4 | Perform a backup. | Perform a backup to save your configuration settings and incidents.  
See “Performing an on-demand backup” on page 709.  
See db-backup on page 744. |
### Table 23-29 Software update procedure (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 5 | Stop incoming messages and drain the queues. | If you are running software update on a Scanner or a combination Control Center and Scanner, set the MTA operation to **Do not accept incoming messages**. Incoming messages are temporarily rejected. After you stop incoming messages, flush messages to drain them from the queues. 

See “Services and MTA operations” on page 71. 

Do not stop the Scanner Services as described in that section. |
| Step 6 | Validate the database. | Ensure that you validate the database using the `cc-config database --check` command. 

See `cc-config` on page 740. |
| Step 7 | Run the software update. | Run the software update either using the Control Center or the `update` command from the command line interface. 

See “Downloading and installing a software update” on page 721. 

See `update` on page 827. |
| Step 8 | Monitor the update progress. | You can monitor the progress of the update through the **Software Update Progress** page. 

Optionally, you can monitor the update process by running the `tail -f update.log` on the command line. Run the command before the software update so you can see the data being written to the log. 

See “Monitoring software update using the command line interface” on page 721. |
| Step 9 | Restart incoming messages. | After the update completes, your Web browser window restarts and displays the login page. Log into the Control Center. If you ran the software update on a Scanner or a combination Control Center and Scanner, set the MTA operation to **Accept and deliver messages normally**. 

See “Services and MTA operations” on page 71. |
About software updates

Symantec periodically releases new versions of the Symantec Messaging Gateway software. New versions contain new features and fixes for software defects. Symantec recommends that you keep your appliance up to date with the latest version of the software. However, some software updates may contain changes to the underlying architecture of Symantec Messaging Gateway. Always read the software update notes and release notes for specific instructions before you run the update.

See “Downloading and installing a software update” on page 721.

See “Updating Symantec Messaging Gateway software” on page 717.

You must run software update on the Control Center and all Scanners. The order in which you apply the software updates to your appliances does not matter. For example, you can update the Control Center before you update Scanners or update a Scanner before the Control Center. Update one appliance at a time.

Table 23-30 Where to get more information about software updates

<table>
<thead>
<tr>
<th>Document</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software update notes</td>
<td>In the Control Center, click Administration &gt; Hosts &gt; Version &gt; Updates. Click Check for Updates and select the version for update. Click View Description.</td>
<td>The Software Update Notes contains abbreviated update information and a list of issues that are addressed in the new version.</td>
</tr>
<tr>
<td>Release notes</td>
<td>To view the release notes for your software version:</td>
<td>The Release Notes contains more detailed information about updating to the new version. The Release Notes also describes new features and lists the known issues that are not fixed in the new version.</td>
</tr>
<tr>
<td></td>
<td>1 On the Internet, go to the Symantec Support site:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://support.symantec.com">https://support.symantec.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 On the ribbon, click the Documentation link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 From the Version drop-down, select your software version.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 From the All Document Types drop-down, select Release Notes.</td>
<td></td>
</tr>
<tr>
<td>Late-breaking news</td>
<td>The URL for the late-breaking news is listed in the software update notes and release notes.</td>
<td>The late-breaking news Web page may contain information about the release that is not in the software update notes or release notes.</td>
</tr>
</tbody>
</table>
Determining which version of software is installed

You can determine what version of software is installed on your appliance.

See “Downloading and installing a software update” on page 721.

To determine which version of software is installed

1 In the Control Center, click Administration > Hosts > Version.
2 On the Updates tab, click the Host drop-down list and select a host.
   The version and status of your software appears.

Downloading and installing a software update

If a new version is available, you can update your Control Center and Scanners.

Note: Symantec recommends that you download the software update using the Download Only option and then install it using the Install Now or Install Later options.

See “About software updates” on page 720.
See “Updating Symantec Messaging Gateway software ” on page 717.

You can also update using the command line interface.

See update on page 827.

To update your software from the Control Center

1 In the Control Center, click Administration > Hosts > Version.
2 On the Updates tab, select a host.
3 Click Check for Updates.
4 If a software update is available, select a software update version and click View Description.
5 If you want to download the software update and install the downloaded software later, click Download Only. The download begins.
   Or
   If you want to install the software update, click Install. This option downloads the software update and completes the installation.

Monitoring software update using the command line interface

The software update process can take several minutes or several hours. If you update using the Control Center, it is difficult to determine if the software update has encountered a problem. You can monitor the progress of the software update by viewing the update.log file as the
update process writes to it. If you see information being written to `update.log` periodically, it usually means that the update is proceeding normally.

See “About software updates” on page 720.

You can start this process before you run the software update or after you have started the software update. You can use this process if you update using the Control Center or command line. If you update using an SSH client on the command line, run the `tail -f update.log` in a separate SSH client window than the `update install` command. If you update using the console to access the command line, it is not possible to run the `tail -f update.log` simultaneously with the update on that console.

See `tail` on page 821.

To monitor the software update using the command line interface

1. Using an SSH client or the console, log into the appliance that you want to update.
2. Type the following command:
   ```
   tail -f update.log
   ```

## Working with diagnostics

Administrators can generate diagnostic reports to help support troubleshoot system slowdowns and failures.

Table 23-31 describes the tasks that you can perform with Symantec Messaging Gateway diagnostics. You can perform these tasks as needed in any order.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn more about how you can use diagnostic packages to troubleshoot issues.</td>
<td>If you experience trouble with Symantec Messaging Gateway, Symantec Support may request that you create a diagnostic package to send to them. The diagnostic package helps Symantec Support troubleshoot issues with your product. See “About troubleshooting issues with Symantec Messaging Gateway with diagnostics” on page 723.</td>
</tr>
<tr>
<td>Run network utilities to troubleshoot issues.</td>
<td>The Control Center has network utilities to help you troubleshoot issues (such as traceroute and ping). See “Running network utilities from the Control Center” on page 724.</td>
</tr>
<tr>
<td>Specify what data you want to include in a diagnostic package.</td>
<td>A diagnostic package has default data, but you can modify what goes into a diagnostic package. See “Specifying what to include in diagnostic packages” on page 725.</td>
</tr>
</tbody>
</table>
About troubleshooting issues with Symantec Messaging Gateway with diagnostics

If you experience trouble with Symantec Messaging Gateway, Symantec Support may request that you create a diagnostic package to send to them. The diagnostic package helps Symantec Support troubleshoot issues with your product.

By default, all diagnostic packages contain certain components. However, you can also specify any additional components that you want to include in the package. If you do not specify any components, a default diagnostic package is generated.

See “Specifying what to include in diagnostic packages” on page 725.

When you generate a diagnostic package, Symantec Messaging Gateway creates the package on the host for which you are running the package. You can then use a transfer protocol to transfer a copy of the package to the location that you specify. You can also download the package locally on the computer on which you run your browser. This feature only works with those hosts that use the same version of Symantec Messaging Gateway as the Control Center. You can only generate one package at a time.

See “Generating diagnostic packages and transferring them to a remote location” on page 728.

See "Generating and downloading diagnostic packages" on page 726.
You can delete a package from the Control Center host when it is no longer needed, which frees up disk space on the Control Center.

See “Deleting diagnostic packages” on page 729.

You can also perform this task from the command line.

See diagnostics on page 757.

Running network utilities from the Control Center

You can run the following network utilities from the Control Center:

- **Nslookup**: Query for DNS info about a computer on the Internet
- **Traceroute**: List the IPv4 hosts that used to transmit Internet data between the selected host and a computer on the Internet, as well as elapsed time
- **Traceroute6**: List the IPv6 hosts that are used to transmit Internet data between the selected host and a computer on the Internet, as well as elapsed time
- **Ping**: Test for a response from a computer with an IPv4 address on the Internet.
- **Ping6**: Test for a response from a computer with an IPv6 address on the Internet.

See “About troubleshooting issues with Symantec Messaging Gateway with diagnostics” on page 723.

To run network utilities from the Control Center

1. In the Control Center, click **Administration > Hosts > Utilities**.
2. Click the **Troubleshooting** tab.
3. From the **Host** drop-down list, select a host name.
4. Under **Select Utility** area, use the drop-down lists to specify a utility name and host name or IP address.
   - If you select Nslookup in the **Utility** drop-down list, you must also specify a DNS query type in the **Record type** drop-down list.
5. Click **Run**.

   The results of the operation appear in the **Results** box.
Specifying what to include in diagnostic packages

A diagnostic package consist of the following default contents:

■ Configuration data
■ Five latest core directories for each job under /data/scanner/jobs (without the core files in those directories)
■ Log data (up to 100,000 lines per file)

For more detailed information about what content is included in a default diagnostic package, refer to the command-line description for creating diagnostic packages.

See diagnostics on page 757.

When you run diagnostics from the Control Center, the default diagnostics package is always included. When you run diagnostics from the command line, you only see what you explicitly included as a command option. If you do not want to export the default contents in a diagnostics package, you must run the diagnostics from the command line.

On the Administration > Hosts > Utilities > Diagnostics tab, you can also specify what additional data you want to include in the package.

■ If you select Message tracking, the report contains all of the message tracking that is on disk.
■ If you select All log data, the report contains all of the log data that is currently available.
■ If you select any core file option, the report contains the most recent core files that are available.

After you specify what to include in the report package, generate the package and transfer or download it to the location that you choose. You can only generate one package at a time. To generate a diagnostic package, you must have Full Administration rights or rights to manage status.

See “Generating diagnostic packages and transferring them to a remote location” on page 728.
See “Generating and downloading diagnostic packages” on page 726.
See “About troubleshooting issues with Symantec Messaging Gateway with diagnostics” on page 723.

Specifying what to include in diagnostic packages

1 In the Control Center, click Administration > Hosts > Utilities.
2 Click the Diagnostics tab.
3 Click the Host drop-down menu and select the host for which you want to run the diagnostic package.
4 Under **Select Components**, check the items that you want to include in the diagnostic package.

If you select no components, a default diagnostic package is generated.

If you select a host that is a Control Center only, then the only component options that are available are as follows:

- All log data
- All core files - Agent core files
- All core files - Other core files

5 In the **Maximum number of cores included in diagnostics package** field, specify the number of cores that you want to include in the diagnostics report.

The default value is 5.

See “Generating diagnostic packages and transferring them to a remote location” on page 728.

**Generating and downloading diagnostic packages**

When you generate a diagnostic package to download, Symantec Messaging Gateway creates the package on the host for which you are running the package. After Symantec Messaging Gateway creates the package, it appears in the **Available Diagnostic package** list in the Control Center. You can download the package to the Control Center computer immediately after you generate it or later on at your convenience.

You can only generate one diagnostic package at a time, so only one package appears in the **Available Diagnostic package** list at a time.

---

**Note:** Symantec Messaging Gateway does not support downloading any diagnostic packages that exceed 2 GB. If the diagnostic package exceeds 2 GB, an error message appears. Regenerate the package and transfer it through one of the supported protocols to a remote location.

See “Generating diagnostic packages and transferring them to a remote location” on page 728.

When a package is successfully generated, it appears in the **Available Diagnostic package** list. If the generation does not complete successfully, an error appears on the Control Center. The error message only appears if you do not navigate from the page. The error is also logged to the Symantec Messaging Gateway BrightmailLog.log log.

If you navigate away from the Diagnostics page and return, you may not see the diagnostic package in the **Available Diagnostic package** list.

One of the following events occurred:
The package generation is successful. Refresh your browser. The package appears in the **Available Diagnostic package** list.

The package is still being generated. No status appears on the Control Center. Do not click **Generate** again. Instead, refresh your browser to see if the package generation is finished. If it is finished, the package appears in the **Available Diagnostic package** list.

The package generation is unsuccessful. No error message appears, but an error is logged to the Symantec Messaging Gateway BrightmailLog.log log.

See “About troubleshooting issues with Symantec Messaging Gateway with diagnostics” on page 723.

When you no longer need a diagnostic package, delete it from the Control Center to free up space.

See “Deleting diagnostic packages” on page 729.

To generate diagnostic packages, you must have Full Administration rights or rights to manage status.

**Generating and downloading diagnostic packages**

1. Specify what you want to include in a diagnostic package and the host.
   See “**Specifying what to include in diagnostic packages**” on page 725.

2. In the **Protocol type** drop-down list, select **Download to desktop**.

3. Click **Generate**.

4. Do one of the following tasks:
   - To download the package immediately after you generate it
     In the **Save As** dialog box, type the location where you want the diagnostic package saved, and then click **Save**.
   - To download the package at a later time
     Do all of the following tasks:
     - Click **Download**.
     - If there are no diagnostic packages in the **Available Diagnostic package** list, the **Download** option is disabled.
     - In the **Save As** dialog box, type the location where you want the diagnostic package saved, and then click **Save**.
Generating diagnostic packages and transferring them to a remote location

When you generate a diagnostic package, Symantec Messaging Gateway creates the package on the host for which you generate the package. After the package is created, you can transfer it to a remote location. You can only generate one diagnostic package at a time. To create diagnostic packages, you must have Full Administration rights or rights to manage status.

If you remain on the Diagnostics page after you generate a package, you receive feedback about whether the generation is successful. It is recommended that you remain on the Diagnostics page until you receive this confirmation.

If you navigate from the Diagnostics page after you generate a package, you receive no feedback about whether the generation is finished or if it was successful. If the package generation is still in progress and you try to regenerate a package, an error message appears that indicates a generation is already in progress.

If the generation is unsuccessful for any reason, an error is logged to the BrightmailLog.log.

See “About troubleshooting issues with Symantec Messaging Gateway with diagnostics” on page 723.

Generating diagnostic packages and transferring them to a remote location

1. Specify what you want to include in a diagnostic package and the host.
   See “Specifying what to include in diagnostic packages” on page 725.

2. Click the Protocol type drop-down list and select one of the following options:
   - Download to desktop
   - FTP
   - SCP

   The default setting is Download to desktop.

   If you select FTP or SCP, you must also specify protocol parameters and credentials.

   If you selected Download to desktop, proceed to step 7.

3. In the Host box, type the host name or IP address for the computer where you want to send the package.

4. In the Port box, type the port number for the computer where you want to send the package.

   The default port for FTP is 21 and for SCP is 22.
5 In the Path field, type the path.

If file path ends with a forward slash, then the directory is assumed, and the default file name is appended to it. If it does not end with a forward slash, it assumes a full file path name.

6 If the Protocol type is FTP and authentication is required, check the Requires authentication option. Otherwise, anonymous logon is attempted. If the Requires authentication option is selected:

- In the Username box, type the user name.
  Special characters (such as $ # %) are unsupported.
- In the Password box, type the password.

Or

If the Protocol type is SCP:

- In the Username box, type the user name.
  Special characters (such as $ # %) are unsupported.
- In the Password box, type the password.

7 Click Generate.

Deleting diagnostic packages

When you create a diagnostic package and select the Download to desktop option, the package appears in Available Diagnostic package list. (Only one package can appear in the Available Diagnostic package list at a time.) When you no longer need this package, you can delete it. When you delete the package from the Available Diagnostic package list, you delete the file that is stored on Control Center.

To delete a diagnostic package, you must have Full Administration rights or rights to manage status.

See “Generating diagnostic packages and transferring them to a remote location” on page 728.

See "Generating and downloading diagnostic packages" on page 726.

See “About troubleshooting issues with Symantec Messaging Gateway with diagnostics” on page 723.

To deleting diagnostic packages

1 In the Control Center, click Administration > Hosts > Utilities.

2 Click the Diagnostics tab.

3 Under Available Diagnostic package, click Delete.
Administering Symantec Messaging Gateway through the command line

This chapter includes the following topics:
- Administering Symantec Messaging Gateway through the command line
- Command line interface access methods

Administering Symantec Messaging Gateway through the command line

Each appliance (physical or virtual) has a set of commands that you can use to configure, optimize, and administer your product. You can execute these commands from an SSH session or from the system console. The help for these commands is presented in Linux man page format.

See “Command line interface access methods” on page 733.

These help pages use the following Linux man page conventions:
- Square brackets ([ ]) indicate that a statement is optional
- The pipe character (|) indicates that one of two statements can be specified
- Text in *italics* indicates that the text should be replaced with the text that you specify

The Symantec Messaging Gateway man pages contain the following sections:
- Synopsis
  - A description of the options and arguments available for the command.
■ Description
General information about the command.

■ Options
Options that you can use to control the behavior of a command. Options always begin with one or two dashes, such as \texttt{-s} or \texttt{--status}. Use two dashes for the full term; one dash for the abbreviated term.
Some options have arguments. For example, \texttt{--log level}. Square brackets mean that element of the command is optional.
Not all commands have options.

■ Arguments
Some commands require arguments. Arguments are names of files, host names, IP addresses, and so on that you specify to control the behavior of the command. Not all commands have arguments. Unlike options, you do not precede arguments with dashes.

■ Examples
This section provides sample command usage. Not all commands have examples.

■ See Also
This section lists related commands. Not all commands have see also references.

Use the following commands to navigate through the man pages:

■ \texttt{f} or \texttt{SPACE}
Forward one window

■ \texttt{b}
Backward one window

■ \texttt{/pattern}
Search for a word or pattern

■ \texttt{<}
Go to the beginning of the document

■ \texttt{>}
Go to the end of the document

■ \texttt{q}
Quit

■ \texttt{h}
Display more help with man pages

Type \texttt{help command_name} to get information about a specific command. Type \texttt{help} to get general information about command-line man pages.

The following commands are available:

■ \texttt{agent-config}
- cat
- cc-config
- clear
- db-backup
- db-restore
- delete
- diagnostics
- dns-control
- fipsmode
- grep
- help
- ifconfig
- iostat
- ip
- ldapsearch
- list
- mallog
- malquery
- monitor
- more
- mta-control
- netstat
- nslookup
- password
- patch
- ping
- ping6
- reboot
- route
- rpmdb
You can log into the command line interface on each Symantec Messaging Gateway appliance. Some of the commands duplicate functions in the Control Center. Some of the commands provide functions that are not available in the Control Center.

See "Administering Symantec Messaging Gateway through the command line" on page 730.

Table 24-1 and Table 24-2 describe the methods that you can use to access the command line interface. After connecting to the command line interface, type admin at the login as: prompt and type the administrator password at the password: prompt.

Table 24-1 Command line interface access methods for physical appliances

<table>
<thead>
<tr>
<th>Access method</th>
<th>How to connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>System console using directly attached keyboard and VGA monitor</td>
<td>You must have physical access to the appliance to access the command line interface with a keyboard and VGA monitor. Connect a keyboard to the keyboard port on the appliance. Connect a VGA-compatible monitor to the D-sub 15 VGA port on the appliance. You can also connect the keyboard and VGA ports on the appliance to a KVM switch.</td>
</tr>
</tbody>
</table>
### Table 24-1  Command line interface access methods for physical appliances (continued)

<table>
<thead>
<tr>
<th>Access method</th>
<th>How to connect</th>
</tr>
</thead>
</table>
| System console using a serial cable    | You must have physical access to the appliance to access the command line interface with serial cable. Connect a null modem cable from the DB9 serial port on the appliance to the serial port on another computer. Use a terminal emulation software on the computer to access the appliance through the serial port. On a Windows computer, ensure that the terminal emulation software is set to use the correct COM port. Configure the terminal emulation software on the computer to the following settings:  
  - 9600 bps  
  - 8 data bits  
  - No parity bit  
  - 1 stop bit                                                                                                                                          |
| Remote access using an SSH client      | Using an SSH client lets you access the command line interface from any computer on your network, unless firewall rules prohibit access.  
  For a Windows computer, use an SSH client such as PuTTY. On a UNIX computer you can use the `ssh` command that is typically included in the operating system.  
  The host name or IP address to connect to using the SSH client is the name you specified when you initially configured the appliance. For a Control Center appliance, the host name is also the name in the URL that you use to access the Control Center. |

### Table 24-2  Command line interface access methods for virtual appliances

<table>
<thead>
<tr>
<th>Access method</th>
<th>How to connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Virtual Machine Console</td>
<td>You can use the VMware Virtual Machine Console to log into the virtual appliance. Refer to the VMware Virtual Machine Console documentation for more information.</td>
</tr>
</tbody>
</table>
| Remote access using an SSH client      | If you configured the virtual appliance with a host name or IP address that resolves on your network, you can use an SSH client to access the command line interface. You can access the virtual appliance from any computer on your network, unless firewall rules prohibit access.  
  For a Windows computer, use an SSH client such as PuTTY. On a UNIX computer you can use the `ssh` command that is typically included in the operating system. |
This appendix includes the following topics:

- agent-config
- cat
- cc-config
- clear
- db-backup
- db-restore
- delete
- diagnostics
- dns-control
- fipsmode
- grep
- help
- ifconfig
- iostat
- ip
- ldapsearch
- list
- mallog
- malquery
- monitor
- more
- mta-control
- netstat
- nslookup
- password
- patch
- ping
- ping6
- reboot
- route
- rpmdb
- rsa-key
- service
- show
- shutdown
- sshd-config
- symdiag
- tail
- telnet
- traceroute
- traceroute6
- update
agent-config

agent-config -- configures the agent that connects hosts to the Control Center

SYNOPSIS

agent-config [--norestart] [--force] --add | --delete ip
agent-config --help | --status
agent-config [--norestart] --log level

DESCRIPTION

The agent-config command lets you edit the allowed IP configuration for the Scanner. Use this command when you change the IP address of the Control Center. You must run this command on every host to re-allow the new Control Center IP to connect to the hosts. The Agent restarts when you add or delete an IP address to or from the allowed IP list, unless you include --norestart in the command.

OPTIONS

--add, -a ip
Add an IP address to the agent-allowed IP address list. Specify an IP address in dotted quad format. For example, 192.168.2.1.

--delete, -d ip
Delete an IP address from the agent-allowed IP address list. Specify an IP address in dotted quad format. For example, 192.168.2.1.

--log, -l level
Set the log level. The log levels are listed below from least verbose to most verbose and each level includes the previous level. For example, if you specify the errors level, only the most urgent log messages are stored. If you specify the notices level, errors, warnings, and notices level log messages are stored.

Specify one of the following log levels:

- errors
- warnings
- notices
- information
- debug
--force, -f
    Used with --delete option to bypass the deletion warning.

--help, -h
    Display this message.

--norestart, -n
    Do not restart the agent after modifying the IP address list or log level.

--status, -s
    Display the allowed IP address list and current log level.
cat

**cat** – standard Linux command to view a file

**DESCRIPTION**

The `cat` command displays the contents of plain text files. The `more` command can be more useful than `cat` for listing long files or multiple files.

Type `help cat` on the command line for more information about the options available for `cat`. The information that appears may contain references to commands that are not available on Symantec Messaging Gateway.

The `cat` command is a standard Linux command that has been modified to only display the files that the `list` command shows.

**SEE ALSO**

See `list` on page 777.

See `more` on page 793.
cc-config

cc-config – configures the logging and network access to the Control Center

SYNOPSIS

cc-config ( --help | --status )
cc-config cclog --level level
cc-config compliancelog --days days
cc-config database ( --status | --check [tableName] | --repair [tableName] | --optimize [tableName] )
cc-config http ( --on | --off )
cc-config port-443 ( --on | --off )
cc-config set-min-tls-level (--tls1 | --tls11 | --tls12)

DESCRIPTION

The cc-config command lets you modify the selected settings that the Control Center uses. These settings include Content Filtering Audit logs, port 443 access, and more.

ARGUMENTS

cclog

Change the log level of the main Control Center log, BrightmailLog.log.

When you apply this to the Control Center log, cc-config writes the command-line parameters to the log4j properties file. It then restarts the Control Center.

compliancelog

Change the rollover frequency of the Content Filtering log.

database

List, optimize, validate, or repair the database tables that the Control Center uses.

Ensure that you validate the database using the cc-config database --check command before updating your Symantec Messaging Gateway. If there are any errors in the tables, repair the erroneous tables using cc-config database --repair [tableName] command and then update your Symantec Messaging Gateway.

http

Turn on or off access to the Control Center using HTTP and port 41080.
If http access is off, you cannot access the Control Center with a URL that starts with http://. If http access is on, you can access the Control Center with a URL that starts with http://. To access the Control Center using http, append :41080 to the URL. Regardless of the http setting, you can always access the Control Center with a URL that starts with https://. Unlike HTTPS, HTTP is not a secure protocol, so the communication between your Web browser and the Control Center could be monitored by a third party.

**port-443**

Turn on or off access to the Control Center using HTTPS and port 443 (the standard, SSL-secured port for Web servers).

When port 443 access is off, you must append :41443 to the URL when you use an https:// URL to access the Control Center. When port 443 access is enabled, you do not need to append the port number for an https:// URL to access the Control Center.

**set_tls_min_level**

Set the minimum TLS level.

**OPTIONS**

**--check, -c**

Check the given database table. If no table name is specified, then check all tables.

**--days, -d**

Set the number of days to keep logs before they roll over.

**--help, -h**

Display this message.

**--level, -l**

Set the log level. The log levels are listed below from least verbose to most verbose and each level includes the previous level. For example, if you specify the `errors` level, only the most urgent log messages are stored. If you specify the `debug` level, `errors`, `warnings`, `information` and `debug` level log messages are stored.

Specify one of the following log levels:

- `errors`
- `warnings`
- `information`
- `debug`

**--off**

Disable a feature.
--on
  Enable a feature.

--optimize, -o
  Optimize the table so it takes less space on disk. If no table name is specified, then optimize all tables.

--repair, -r
  Repair the given database table. If no table name is specified, then attempt a repair operation on all damaged tables.

--status, -s
  Display the current log settings and port statuses.

--tls1 --tls11 --tls12
  TLS versions: --tls1 = TLSv1; --tls11 = TLSv1.1; --tls12 = TLSv1.2
clear

clear – standard Linux command to clear the screen

SYNOPSIS

clear

DESCRIPTION

The clear command erases all of the text on the screen and displays the command prompt at the top of the screen.

This command is a standard Linux command that has not been modified.
db-backup

db-backup – back up the Control Center database

SYNOPSIS

db-backup [options]

DESCRIPTION

The db-backup command backs up the Brightmail databases, such as policies configuration settings, report data, log data, and incidents. You can store backups on the appliance or on a remote server. Only run this command on the appliance that contains the Control Center. This command does not function on a Scanner-only appliance. Only one instance of db-backup can run at a time.

By default, backup files are compressed before they are written to disk to minimize the size of backup files. The db-backup command calculates the amount of disk space the backup file requires. The command does not run unless at least twice this amount is available on the /data partition.

Use db-restore or the Control Center restore feature to restore a backup on the appliance or a backup on a remote computer. If you specify --file path for a backup to the appliance, you can only restore the backup using the db-restore command, not the Control Center restore feature.

You can also create backups using the Control Center. In the Control Center, click Administration > Hosts > Version > Backup.

See “Performing an on-demand backup” on page 709.

OPTIONS

--backup, -b number

The number of backups to store on the appliance. If you have more backups stored than number, then older backups are deleted. Each unique combination of type and schedule is retained separately. If you do not specify --backup number, the default is 5 for each type and schedule combination. See examples 4 and 6.

--file, -f path

The name and, optionally, location to save the backup. Use the --file option to specify an alternate file name for the backup file or to save the backup file to a remote computer. If you do not specify --file path, the backup is saved to the appliance as
You can save the backup to a remote computer using either FTP (file transfer protocol) or SCP (secure copy protocol). If the path ends with / the backup is saved in that directory using the default file name. If the path ends with a file name the backup is saved with that name in the specified path. When you save the backup to a remote computer, db-backup temporarily stores the backup file on the appliance, checks the file for data integrity, copies the file to the remote computer, and checks to ensure that the file was successfully copied.

Use one of the following two path formats to save the backup to a remote server:

FTP

Use the following format: ftp://'user':'password'@host[:port]/path. If special characters are included in the password, you must enclose the password in single quotes ('). If the special characters in a password include a single quote, you can use the double quote instead ("). Passwords containing single and double quotes are not valid. If no user name and password are specified, an anonymous login is used.

SCP

Use the following format: scp://'user'@host/path. You must specify a user name.
The db-backup command prompts you for the password.

--gzip, -g

Use the gzip compression algorithm instead of the default bzip2 compression algorithm. The gzip algorithm performs less efficient compression than bzip2.

--list, -l

List existing backups on the appliance.

--help, -h

Display this message.

--incidents, -i

Includes content incident messages in a configuration backup. Valid only when used with --type config.

--logs, -o

Includes log data in a configuration backup. Valid only when used with --type config.

--nocompress, -n

Do not compress the backup file. Use this option if you want to visually scan the file contents.

--purge, -p

Purge backups. Use the --purge option to delete old backup files that match the parameters that you specify. To delete all but the number most recent backups of a type and schedule combination, specify --purge --backup number along with the type and
schedule. Specify `--purge --backup 0` to delete all backups of a type and schedule combination. To delete a specific file, specify `--file file` along with `--purge`. See examples 5 and 6.

`--reports`, `-r`  
Includes report data in a configuration backup. Valid only when used with `--type config`.

`--schedule`, `-s schedule`  
The schedule name to include in the backup file name. If you specify a schedule name, `db-backup` does not create automatic backups at that interval. The schedule that you specify only names the backup file with that name. The schedule names differentiate backups. See `--backup` and `--purge` for more information. Use the backup feature in the Control Center to create automatic scheduled backups. The following schedules are available:

- **manual**  
  Label this backup a manual backup. This option is the default.

- **daily**  
  Label the backup a daily, manual backup.

- **weekly**  
  Label the backup a weekly, manual backup.

- **monthly**  
  Label the backup a monthly, manual backup.

`--type`, `-t type`  
The type of backup to create. Each backup type has two aliases that are alternate short versions of the backup type. See example 4. The following types are available:

- **full**  
  Perform a full backup (aliases: `f`, `1`). This is the default option.

- **config-incidents**  
  Back up configuration and content filtering incident data (aliases: `ci`, `2`).

- **config-incidents-reports-logs**  
  Back up configuration, content filtering incident, report and log data (aliases: `cirl`, `3`).

- **config**  
  Back up all configuration including policies (aliases: `c`, `4`). Use `--log` to include log data in this backup. Use `--reports` to include report data in this backup. Use `--incidents` to include content incident messages in this backup. This option is the default.
policy
Back up spam, malware, reputation, and content filtering policies and policy groups and policy resources (aliases: p, 5).

EXAMPLES

Example 1
Save a full backup on the appliance with the default schedule of manual and the default type of full. The newest five backups with a schedule of manual and type of full are kept (including the backup just created) and the rest of the backups matching that combination are deleted.

db-backup

Example 2
Save a full backup on a remote server with SCP. The database backup file in the format db-backup.<product version>.brightmail.date-time.full.manual.tar.bz2 is copied to 192.168.2.42 in the /tmp directory through SCP. Log on to the SCP server with the support user account. The db-backup command prompts for the password for the support user account.

db-backup --file scp://support@192.168.2.42/tmp/

Example 3
Save a full backup on a remote server with FTP. The database backup file db-backup.<product version>.brightmail.date-time.full.manual.tar.bz2 is copied to host.symantecexample.org in the /user/jmuir directory. Log on to the FTP server with the jmuir user account and secret password.

db-backup -f ftp://jmuir:secret@host.symantecexample.org/user/jmuir/

Example 4
Backup configuration and content filtering incident data to the appliance and include the word weekly in the backup file name. In addition to the newly created backup, keep one additional existing backup with config-incidents and weekly in the file name.

db-backup --backup 2 --schedule weekly --type ci

Example 5
Delete a single backup file.

db-backup --purge --file db-backup.10.0.0-1.brightmail.Feb-25-12-19-26.config-incidents.weekly.tar.bz2

Example 6
Delete all but the one most recent backup file of type config-incidents and schedule manual.
db-backup --purge --backup 1 --type config-incidents --schedule manual

SEE ALSO

See db-restore on page 749.
db-restore

**db-restore** – restores the Brightmail databases to an appliance from previously created backups on the appliance or from remote locations with FTP and SCP

**SYNOPSIS**

db-restore [--force --list --help] file

**DESCRIPTION**

The `db-restore` command restores Brightmail databases to an appliance from a single, previously created backup. These are the backups that you have previously generated and saved on the appliance or from remote locations with FTP and SCP. If you attempt to run more than one instance of `db-restore` at a time, an error results. If any part of the operation fails, `db-restore` fails, and an explanatory message appears on the command line. You must be on the Control Center host to use the `db-restore` command.

---

**Note:** Restoring an appliance immediately after resetting the appliance to its factory default might leave the appliance in an unusable state. Therefore, you must complete the site setup before restoring an appliance that is reset to its factory default.

---

When you restore a database backup on a different appliance than it was created, keep in mind the following considerations:

- When the backup is taken from one network configuration and restored on another network configuration, the restore will not be successful, unless the IP addresses of BCC/AIO and additional scanners match the IP addresses taken in the backup.

- If you restore the appliance from a backup that was taken on a different appliance, the restored appliance does not affect the configuration settings on the new host. However, the virtual IP addresses are not created during the configuration. Virtual IPs defined in the old Control Center host are mapped by default to an interface on the new Control Center host. You can avoid the mapping of virtual IPs from the old Control Center host to the interface on the new Control Center host by completing the site setup. Alternatively, you can create the virtual IPs on the new Control Center host after the restore.

- If you attempt to restore a backup to an appliance other than the one on which it was created, you must restart the appliance.

Stop the Control Center while this operation runs. Restart it when the restore has completed.
OPTIONS

--force, -f
Force a restore even when the version of appliance software in the backup file differs from the software that is currently on the appliance.

--list, -l
List the backup files that are stored on the appliance.

--help, -h
Display this message.

ARGUMENTS

Specify file with one of the following formats. If the file is stored on a remote computer, specify the directory path to the file.

file
Type the file name without the FTP or SCP prefix to specify a backup that is stored locally.

ftp://user:password@[::port] /path
Copy files from their remote location with FTP.

Logon is attempted with the user name and password credentials that you provide on the command line. If special characters are included in the password, enclose the password in single quotes ('). If the special characters in a password include a single quote, you can use the double quote instead ("'). If no credentials are specified, anonymous logon is used. Error checking ensures that the copies are complete.

scp://username@host/path
Copy the backup file from its remote location with SCP. A complete path, file name, and user name are required when you specify a backup file through SCP. You are prompted for a password for the user name that you specify. Return codes are checked to ensure that the entire backup file is copied from the remote host. The script exits with non-zero status on failure. If the script fails, an error message appears. Error checking ensures that the copies are complete.

SEE ALSO

See db-backup on page 744.
See diagnostics on page 757.
See “Provisioning the submitter ID for customer-specific spam submissions” on page 270.
See “Working with the Submitters Email Address list” on page 275.
See “Restoring an appliance from backups” on page 711.
See "Restarting an appliance" on page 699.

See "Stopping and starting Scanners" on page 68.
delete

delete – clear logs, configuration information, and data

SYNOPSIS

define [--purge num] component component ...
define file file

DESCRIPTION

Use the delete command to delete logs, configuration information, and other data. You may want to delete data if disk space is low or to clear configuration data to correct or diagnose a problem. The delete command restarts the Brightmail Engine if necessary after you run the delete command.

OPTIONS

--purge, -p num

Delete all database backup files except for the num most recent files. This option is only valid with the database component.

ARGUMENTS

You can delete individual files or you can specify one or more components to delete logical groups of files.

file file

Delete the file that you specify. You can only delete the files that you can view with the list command. Specify the entire path to the file as shown by the list command.

Symantec recommends that you delete items by specifying a component instead of deleting individual files. If you delete individual files, you may change the effectiveness or performance of Symantec Messaging Gateway. If you delete log files or temporary files with the delete file file command, some log data may be lost. To delete log files, specify one of the components in the log components group.

If you do delete individual log files with the delete file file command, restart the service that applies to the log file that you deleted. For example, if you delete the Control Center log file Brightmaillog.log, restart the Control Center service. Use the service command or the Control Center to restart a service.

The following components are available and are listed in groups of similar behavior.
Log components:

- **alllogs**
  Delete all logs in the log component group.

- **bcclogs**
  Delete all Control Center logs.

- **ddslogs**
  Delete all directory data service logs.

- **mallogs**
  Delete all Message Audit Logs.

- **oslogs**
  Delete all operating system logs.

- **scannerlogs**
  Delete all Scanner logs.

Configuration components:

- **allconfig**
  Delete all configuration data in the configuration component group.

- **bccconfig**
  Delete all Control Center configuration files.

- **clearsockets**
  Delete all socket files in the /var/tmp directory.

- **scannerconfig**
  Delete all of the Scanner configuration files for a given Scanner (including support sieve scripts). It does not affect the Scanner configuration information that is stored in the Control Center.

  When you run delete scannerconfig, it restarts the appliance on which the command is run. After you run delete scannerconfig, you must recommit Scanner configuration information from the Control Center to disk and relicense your Scanner.

  You can recommit the Scanner information to disk unchanged or edit the information to correct potential problems before you save this information to disk. To do either of these tasks, access Administration > Hosts > Configuration in the Control Center, select the Scanner, and click Edit. To recommit the information unchanged, click Save. Alternatively, edit any settings for this Scanner as necessary to correct a problem in the configuration and click Save.

  You can delete the Scanner configuration if you change the Scanner configuration of an independent Scanner appliance. Then you can re-add it with the Add Scanner Wizard. This option is not available for an appliance that hosts both a Control Center and Scanner.
Symantec recommends that you do not use `delete scannerconfig`.

Data components:

- **alldata**
  - Delete all data in the data component group.

- **bccdata**
  - Delete all Control Center data including any license files. Afterwards, your configuration is the same as an out-of-the-box the Control Center configuration.

- **ddedata**
  - Delete all directory data service data.

- **keystore**
  - Delete Control Center HTTPS certificates from the keystore.

- **scannerdata**
  - Delete mail from MTA queues and the following file:

```plaintext
/data/scanner/rules/matchEngine/tmp/data_match_engine_jce_keystore
```

- **spcdata**
  - Delete all Symantec Protection Center (SPC) data, and de-register any Symantec Messaging Gateway SPC instance. After using **spcdata**, you must re-register the Control Center with the SPC server in order to continue using the Control Center with SPC.

- **statsdata**
  - Delete stats files from scanner.

- **sudata**
  - Delete all of the files that are related to software updates.

Quarantine components:

- **allquarantine**
  - Delete all messages from all quarantines.

- **contentquarantine**
  - Delete all content quarantine and informational messages.

- **spamquarantine**
  - Delete all messages from Spam Quarantine.

- **virusquarantine**
  - Delete all messages from Suspect Virus Quarantine.

Rule components:

- **allrules**
  - Delete all rules and replace them with the factory default rules.
avrules
   Delete all antivirus rules and replace them with the factory default rules.

bodyhashrules
   Delete bodyhash rules and replace them with the factory default rules.

dayzerorules
   Delete all day zero rules and replace them with the factory default rules.

fastpassrules
   Delete all Fastpass rules.

gatekeeperrules
   Delete gatekeeper antispam rules and replace with factory default rules.

intsigrules
   Delete all intsig rules and replace them with the factory default rules.

ipfreqrules
   Delete IP frequency rules.

permitrules
   Delete permit rules and replace them with the factory default rules.

regexrules
   Delete regex filter rules.

spamhunterrules
   Delete all spam hunter rules and replace them with the factory default rules.

spamsigrules
   Delete spamsig rules and replace them with the factory default rules.

statsigrules
   Delete statsig rules and replace them with the factory default rules.

---

**Note:** The `delete` command may take half a minute to delete rules. Wait for the command prompt to return before you run additional commands. Do not press Ctrl+C to stop the `delete` command while it is running.

---

Miscellaneous components:

all
   Delete all logs, configuration data, passwords, support sieve scripts, Scanner data, cores, diagnostic packages, rules, queue data, SPC data, and backup files to restore your appliance to the original factory configuration.
bcchostacl
    Delete the Scanner access controls made on the Administration > Settings > Control Center page to permit access from all Scanners.

cores
    Delete all core directories.

database
    Delete all backups of the Control Center database that were created with db-backup.

diagnostics
    Delete all diagnostic packages.

fips
    Delete fips setting and replace it with factory default setting of non-FIPS mode.

help
    Display a summary of components that you can delete.

monitor
    Delete the files made by the monitor command.

EXAMPLES

Example 1
Delete the BrightmailLog.log file.

delete file /data/logs/bcc/BrightmailLog.log

Example 2
Delete all messages in the Spam Quarantine.

delete spamquarantine

Example 3
Delete all Control Center database backup files that are stored on the appliance except for the three most recent backup files.

delete --purge 3 database

SEE ALSO

See cat on page 739.

See list on page 777.

See more on page 793.

See “Clear disk space checklist” on page 625.
diagnostics


diagnostics – generate diagnostics package

SYNOPSIS

diagnostics [options] url

DESCRIPTION

The diagnostics command generates a diagnostic package that Symantec Support can use to analyze problems with the product.

You should specify a valid URL unless you use the --find-other-cores option. If you specify a valid URL but do not specify the data collection options, diagnostics uses the following parameters by default:

--config --crash-info 5 --logs 100000

These parameters generate a diagnostic package with the following contents:

- Configuration data
- Five latest core directories for each job under /data/scanner/jobs (without the core files in those directories)
- Log data (up to 100,000 lines per file)

If you specify any options, these parameters are not included unless you explicitly add them to the command.

When the user name or password are part of the URL, write them in quotes if they have any special shell characters in them. The password can be specified in the URL or at the password prompt. An example of the URL syntax is as follows:

scp://'user':'password'@host[:port]/path

If you specify a path that ends with a forward slash, the diagnostics file is written to the path that you specify with the default file name. If you specify a path that does not end with a forward slash, the backup file is written with the file name specified in the path.

The default diagnostics file name is in the following format:

diagnostics.yy-mmm-dd-hh-mm.hostname.tar.gz

For example: diagnostics.09-Sep-15-42.host9902.symantecexample.com.tar.gz

An option cannot be specified more than once whether it is in its long form or short form. For the --cores option, a component cannot be specified more than once either with the component
name or convenient string all. If you attempt to specify duplicate options, an error message appears along with the appropriate usage text.

OPTIONS

--bad-messages, -b
   Collect MTA bad messages.

--config, -c
   Collect only the configuration data. The configuration data includes Symantec Protection Center (SPC) registration details, if available.

--cores, -o component n
   Collect the latest n core directories, including core files for a component. The valid range for n is 1 through 9,999.
   The list of components include the following:
   - --cores mta n collects MTA core packages
   - --cores bmagent n collects Brightmail Agent core packages
   - --cores bmsserver n collects Brightmail Server core packages
   - --cores conduit n collects Conduit core packages
   - --cores jlu-controller n collects Java LiveUpdate core packages
   - --cores dds n collects Directory Data Service core packages
   - --cores other n collects the other core files that are not collected with other options.
   - --cores all n
     all is a convenient identifier that means all components.

--crash-info n, -a
   Collect the latest n core directories (excluding the core files in those directories) for the following processes:
   - mta
   - bmagent
   - bmsserver
   - conduit
   - jlu-controller
   - dds
   The valid range for n is 1 through 9,999.
--edm, -e
Collect the exact data match (EDM) record sets.

--find-other-cores, -d
Discover any core file outside of /data/scanner/jobs and move them to /data/scanner/jobs/other.

If Symantec Messaging Gateway discovers and moves any core files, an email notification is sent to the administrators that are specified to receive alerts. If not, no email notification is sent.

You can use this option with the delete cores command to clean up core files on your product. Run this command first to move the core files that are not in the jobs directory to the jobs directory. Then use delete cores to delete the core files.

If --find-other-cores is the only data collection option specified, a URL is not required. No diagnostics package is generated.

--force, -f
Force diagnostics to run even if a diagnostics collection that is started from the user interface is still in progress. If a package creation is in progress, the existing diagnostics collection fails.

--gcore, -g component
Generate a core image of the specified component and download it. You can use this option to capture necessary data regarding a hung or spinning component, before restarting the component. This option does not stop or restart a process, but it may cause the process to pause briefly. The available components are:

- bmagent
- bmserver
- conduit
- mta
- jlu-controller

--help, -h
Display this message.

--include-old-queues, -i
Collect queue data from old postfix queues.

This command is only useful on configurations in which Symantec Messaging Gateway is migrated from version 7.7 or earlier. This command is not applicable for Symantec Messaging Gateway version 8 or higher.
--ldap, -p
    Collect legacy ldapsync data.
    This command is only useful on configurations in which Symantec Messaging Gateway is migrated from version 8 or earlier. This command is not applicable for Symantec Messaging Gateway version 9 or higher.

--logs all, -l
    Collect all logs of all log files.

--logs n, -l
    Collect log data that is limited to n lines per log file.
    The valid range for n is 1 through 2,147,483,647.

--monitor, -m
    Collect a snapshot output of the following monitor command: monitor -c 6 --proc bmserver --proc mta system database disk mta p_all and existing monitor logs under /data/monitor.

--rules, -r
    Collect all rules that are present on the Scanner, except exact data match data.

--tracking, -t
    Collect Message Audit Log files.

--verbose, -v
    Show the command process in verbose mode.

ARGUMENTS

The syntax for the URL paths referenced by this command is as follows:

- scp://user:password@host[:port]/path
  Copies the diagnostics package remotely through SCP.

- ftp://user:password@host[:port]/path
  Copies the diagnostics package remotely through FTP.
  If no user name and password are specified, an anonymous login is used.

Logon is attempted with the user name and password credentials that are provided on the command line. If special characters are included in the password, you must enclose the password in single quotes ('). If the special characters in a password include a single quote, you can use the double quote instead ("'). If no credentials are specified, anonymous logon is used.
EXAMPLES

Create a diagnostics file and transfer it with the SCP protocol. The diagnostics file (in the format: diagnostics.yy-mmm-dd-hh-mm.hostname.tar.gz) is transferred to the SCP destination.

```
diagnostics scp://'support'@10.160.248.128/tmp/
```

**Note:** The month is expressed in the three-letter format, not two-digit format.
dns-control

dns-control – control the local DNS cache

SYNOPSIS

dns-control command

DESCRIPTION

The dns-control command manages local caching for the name server.

All dns-control command outputs end with either a completion message or a failure message. Examples are: "Command cmdname completed successfully" and "Command cmdname failed."

Some commands require the DNS cache to be running before they can be executed. In these cases, the only output is: "The DNS Cache is currently stopped." Start the cache with the dns-control start command before you run those commands.

ARGUMENTS

The command components are as follows:

start
  Start the local caching name server.
stop
  Stop the local caching name server.
restart
  Restart the local caching name server.
status
  Display the status of the local caching name server.
flush
  Flush the cache.
list
  List the locally configured name servers for the resolver.
trace
  Increment the tracing (debug) level by +1.
notrace
  Disable tracing (debug).
reconfig

Forces a reload of the name server configuration information.

help

Display this page.
fipsmode

fipsmode -- enable, disable, or check FIPS mode

SYNOPSIS

fipsmode --help
fipsmode(on|off|status)

DESCRIPTION

Enable, disable, or check the status of FIPS mode (whether an appliance is in FIPS mode or
not) on an appliance. Changing the status of FIPS mode will prompt a reboot.

fipsmode logs its actions to syslog /data/logs/messages.

OPTIONS

--help, -h
  Displays usage info.

ARGUMENTS

on
  Turn FIPS mode on. You will be prompted to allow a reboot.
  If the fipsmode on command is called when the system is already in FIPS mode, then
  the script will report “FIPS mode not being changed.”

off
  Turn FIPS mode off. You will be prompted to allow a reboot.
  If the fipsmode off command is used while the system is not in FIPS mode, the script
  will report “FIPS mode not being changed.”

status
  Display whether host is in “FIPS mode” or in “Non-FIPS mode”.

grep

grep – search in files for text or a regular expression

DESCRIPTION

The `grep` command searches in the files that you specify for text or regular expressions.

Type `grep --help` on the command line for more information about the options available for `grep`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that is limited in Symantec Messaging Gateway. Administrators can only use `grep`:

- On filenames obtainable through the `list` command.
- By piping the output of other commands to the `grep` command.
help

help – display help for individual commands or display all available commands

SYNOPSIS

help [ --list | command ]

DESCRIPTION

The help command displays a list of available commands on the product. If you specify a command name, the help command displays help for that command.

The help for commands is presented in Linux man page format. These help pages use the following Linux man page conventions. Do not type the brackets, parenthesis, or pipe symbol when you run a command.

Brackets [ ]
The options and the arguments that are listed within square brackets are optional. The options and the arguments that are not listed within square brackets are required.

Parenthesis ( )
The options and the arguments that are listed within parenthesis are required but are mutually exclusive. A pipe symbol separates the mutually exclusive options or arguments.

Pipe |
The pipe symbol indicates the options or arguments that are mutually exclusive. For example [ -e pattern | -f file ] means that you can specify -e pattern or -f file, but not both.

Colored, italic, or underlined text
Text that is italic, colored, or underlined indicates that you should substitute that text with specific text. When you type help command, the terminal or terminal software that you use to access the command line determines how this text appears. When you view help pages in a PDF or in the online help, this type of text is italic.

--option, -o
Some command options are available in long and short versions. The long version and short version produce the same behavior. Use whichever version is most convenient for you. In the OPTIONS section, these options are displayed with the long version first, followed by a comma, and then the short version. The long version is preceded with two dashes and the short version is preceded with one dash. Some options have required parameters that you specify after the option, like a log level or IP address.

The help pages contain the following sections:
SYNOPSIS
A description of the options and arguments available for the command.

DESCRIPTION
General information about the command.

OPTIONS
Options that you can use to control the behavior of a command. Options always begin with one or two dashes, such as \texttt{-s} or \texttt{--status}. If an option is listed in square brackets in the synopsis, the options are optional. If not, the option is required.

Some options have arguments. For example, \texttt{--log level}. Square brackets indicate optional arguments.

Not all commands have options.

ARGUMENTS
Some commands require arguments. Arguments are names of files, host names, IP addresses, and so on that you specify to control the behavior of the command. Not all commands have arguments.

EXAMPLES
The EXAMPLES section provides sample command usage. Not all commands have examples.

SEE ALSO
The SEE ALSO section lists related commands. Not all commands have see also references.

Use the following commands to navigate through the help pages:

\texttt{f} or \texttt{SPACE}
Forward one screen

\texttt{b}
Backward one screen

\texttt{/pattern}
Search for a word or pattern

\texttt{<}
Go to the beginning of the document

\texttt{>}
Go to the end of the document

\texttt{q}
Exit from the document and display the command prompt
Display additional information about navigating the help pages

OPTIONS

--list, -l
Display a list of all the available commands.

ARGUMENTS

cmd
Display help for the specified command.
If you do not specify a command, help for the help command is displayed (this page).
Specify one of the following commands:

agent-config
Configures the agent that connects hosts to the Control Center

cat
Standard Linux command to view a file

cc-config
Configure the logging and network access to the Control Center

clear
A standard Linux command to clear the screen

db-backup
Back up the Control Center database

db-restore
Restores the Brightmail databases to an appliance from previously created backups on the appliance or from remote locations with FTP, SCP, and HTTP

delete
Clear logs, configuration information, and data

diagnostics
Generate diagnostics package

dns-control
Control the local DNS cache

fipsmode
Enable, disable, or check FIPS mode
grep
A standard Linux command to search in files for text or a regular expression

help
Display help for individual commands or display all available commands

ifconfig
A standard Linux command to configure network interfaces

iostat
A standard Linux command to display CPU and device load

ip
Retrieve information about addresses in use by Symantec Messaging Gateway

ldapsearch
A standard Linux command to query an LDAP directory

list
Display the file names of all files that certain commands can act on

mallog
List, backup, or restore Message Audit Logs

malquery
Query Message Audit Logs

monitor
View and record information about Brightmail-specific processes

more
A standard Linux command to page through a text file

mta-control
Control the MTA processes and backup and restore mail queues

netstat
A standard Linux command to view network connections

nslookup
A standard Linux command to query DNS servers

password
Change your administrative password

ping
A standard Linux command to test for a response from a remote computer
ping6
   Test the transfer of data between the issuing machine and the given IPv6 host name or IP address
   A standard Linux command

patch
   Handles all necessary functions related to patches

reboot
   Reboot the appliance

route
   A standard Linux command to show and manipulate the IP routing table

rpmdb
   Manage and repair the RPM database

service
   A standard Linux command to start or stop services

show
   Display system information

shutdown
   Shut down the appliance without rebooting

sshd-config
   Configure which addresses can SSH to the appliance

tail
   A standard Linux command to view the end of a file

telnet
   A standard Linux command to connect to a remote computer

traceroute
   A standard Linux command to view the path that network packets take

traceroute6
   Trace the network route to the given host name or IPv6 address

update
   Update the appliance software
HISTORY

In Symantec Brightmail Gateway version 9.0, some commands that existed in version 8.0 and previous versions were renamed, incorporated into other commands, or removed. The following commands were changed in version 9.0:

agentconfig
   Replaced with agent-config.

clear
   Replaced with delete. In version 9.0, the clear command clears the screen.
crawler
   Part of diagnostics.
date
   Replaced with show --date.
delete
   Replaced with delete cores.
dn-normalize
   The functionality of the dn-normalize command is not available in version 9.0.
eula
   Replaced with show --eula.
http
   Replaced with cc-config http.
install
   Replaced with update install.
ls
   Replaced with list.
mta-stats
   Replaced with monitor mta.
passwd
   Replaced with password.
pause-mode
   Replaced with mta-control pause-mode.
rebuildrpmdb
   Replaced with rpmdb --repair.
rm
  Replaced with delete files.

set-control-center-port-443
  Replaced with cc-config port-443.

sshdctl
  Replaced with sshd-config.

sshdver
  Replaced with sshd-config --version.

sys-info
  Replaced with show --info.

system-stats
  Replaced with monitor system.

tls-ca-cert-control
  The functionality of the tls-ca-cert-control command is not available in version 9.0.
ifconfig

ifconfig – a standard Linux command to configure network interfaces

DESCRIPTION

The ifconfig command displays the status and configuration of network interfaces and can make temporary changes to interface configurations.

Type help ifconfig on the command line for more information about the options available for ifconfig. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
iostat

iostat – a standard Linux command to display CPU and device load

DESCRIPTION

The `iostat` command monitors system input/output device loading by observing the time devices are active in relation to their average transfer rates.

Type `help iostat` on the command line for more information about the options available for `iostat`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
ip

ip – standard Linux command to retrieve information about an IP address

DESCRIPTION

The ip command lets you view and modify information about an IP address.

Type help ip on the command line for more information about the options available for ip. The information that appears may contain references to commands that are not available on Symantec Messaging Gateway.
ldapsearch – a standard Linux command to query an LDAP directory

DESCRIPTION

The `ldapsearch` command searches in the LDAP source that you specify and displays matching records.

Type `help ldapsearch` on the command line for more information about the options available for `ldapsearch`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
list

list – display the file names of all files that certain commands can act on

SYNOPSIS

list --help

DESCRIPTION

The list command displays the file names of all of the files that can be acted upon by certain commands. The following commands can act upon the files that are listed with list:

cat
Display the contents of one or more files.
delete
Delete one or more files.
more
Display the contents of one or more files and pause at the end of each screen.
tail
Show the last 50 lines of the named log file.

OPTIONS

If list does not list any files when you specify an option, there are no files in that category.

--all, -a
List all files.
--cores, -c
List all core files.
--diagnostics, -d
List all diagnostic packages.
--help, -h
Display this message.
--logs, -l
List all log files.
--monitor, -m
List all monitor files.

--temp, -p
List all temporary files.

--top, -t
List the largest files that the administrator can delete and their sizes.

EXAMPLES

Example 1
List all the files that can be viewed with cat (except core files and diagnostic files) or deleted with delete.
list --all

Example 2
List the largest files that you can delete. You can use the delete command to delete large files if you do not need them.
list --top

SEE ALSO

See cat on page 739.
See delete on page 752.
See more on page 793.
mallog

mallog – list, backup, or restore Message Audit Logs

SYNOPSIS

mallog [ --list ]
mallog [ --backup | --restore ] url

DESCRIPTION

The mallog command backs up and restores Message Audit Log data that resides on the Scanner. The mallog command also lists the Message Audit Log files on the Scanner. To view message activity in the Message Audit Logs, use the Control Center or the malquery command.

Available log files include the following:

- /data/logs/scanner/audit_bmengine_log*
- /data/logs/scanner/audit_mte_log*
- /data/logs/scanner/audit_mta_log*

Note: When you run mallog --backup or mallog --restore, email processing stops while these commands run. No inbound email or outbound email is delivered during this time. If your organization’s email availability policies are strict, it may be appropriate to only run these commands during off hours.

OPTIONS

--backup url

Create a backup of all of the message tracking logs that are in tar.gz format, and upload the resulting file to the specified URL.

Note: This option suspends mail processing while the command is executed.

--list

List individual message tracking logs on the file system and their timestamps and sizes.

--restore url

Restore message tracking logs from the specified URL. Existing logs are overwritten.
**Note:** This option suspends mail processing while the command is executed.

URLs may have a scheme of either FTP, SCP, or, HTTP (for restore only).

If you specify a path that ends with a forward slash, the diagnostics file is written to the path that you specify with the default file name. If you specify a path that does not end with a forward slash, the backup file is written with the file name specified in the path. The `--restore` option requires a full path name which includes a file name. The entire URL should be taken in double quotes. If any part of the URL contains special characters, such as full or double quotes, escape the special characters with a backslash. When the password is part of the URL, it should be written in quotes if it has any special shell characters in it.

**url**

Transmit the package to the `url` location by SCP or FTP.

The entire URL should be taken in double quotes. If any part of the URL contains special characters, such as full or double quotes, escape the special characters with a backslash. When the password is part of the URL, it should be written in quotes if it has any special shell characters in it.

**SEE ALSO**

See `malquery` on page 781.
malquery

malquery – query Message Audit Logs

SYNOPSIS

malquery (-l start,end | -g start,end | -s start [ -n end] | -p range)
(-u uid [-u uid ...] | -e event[,arg_num]<=|*>string [-e ...] | -q event[,arg_num]<=|*>quoted-printable-string [-q ...])
[-m max_results] [-I index_max] [-o url] [-v]

DESCRIPTION

You can track messages in the Control Center by querying the Message Audit Logs. Alternatively, you can use the malquery command-line command to track messages. Use malquery instead of the Control Center for complex queries or queries where you expect voluminous data. The malquery command only returns data for the Scanner that you are logged into.

Enabling Message Audit Logging results in approximately 800 bytes of audit logs per message. Message Audit Logging can cause performance and storage problems if your site receives more than 1,000,000 messages per day.

Audit logs older than the current day are rolled over to a filename appended with the local date in the form yyyy-mm-dd. Audit logs older than the default retention period of two days are deleted.

The results that the malquery command line generates do not reflect events that the Control Center generates, nor does it reflect those events generated on other Scanners.

The output from malquery is in .xml format, for example:

<malResults count="message result count">
  <message AID="aid">
    <events>
      <event time="utc" name="event id">parameters</event>
      <event time="utc" name="event id">parameters</event>
      <event time="utc" name="event id">parameters</event>
      <event time="utc" name="event id">parameters</event>
    </events>
  </message>
</malResults>
OPTIONS

-a, --audit audit_id
Find the email message with the specified audit ID (aid).

-e ..., --event
Find email messages that contain the events that match the specified criterion.

Examples:
-e RCPTS=dale@company.com
RCPTS is recipient. In this example, the recipient is dale@company.com.
-e "SUBJECT*my flowers"
SUBJECT is the subject of the email message. In this example, the subject contains the words 'my flowers'.

Use the equals character (=) for an exact match. Use the asterisk (*) for contains. Searches are case-insensitive.

A list of the more common elements that you can search are as follows:

■ ACCEPT
  Connection IP
■ ATTACH
  Attachment file name
■ MSGID
  Message ID
■ RCPTS
  Recipient address
■ SENDER
  Sender address
■ SUBJECT
  Message subject

-g, --gmt start,end
Find messages by the GMT date range to search in UNIX time (the number of time units that have elapsed since the epoch time 1/1/1970). For example,


Separate the start date and end date by a comma with no space.
-i, --index index_max_n
Use the index (.idx file) if the number of matching results is less than or equal to
index_max_n. Otherwise, the index is ignored. This option searches a flat file, which saves
time when you want to look up large numbers of events.

The default for index_max_n is 1000.

-l, --date start,end
Date range to search. Dates in the form YYYYMMDDhhmm. For example:

Separate the start date and end date by a comma with no space.

-m, --max max_results
Return the max_results number of messages. The default is 1000.

-n, --end
End of date range to search. Date should be in the following form: YYYYMMDDhhmm.
For example:

-o, --output file
Output data the matches the results to the specified URL.
Use a SCP or FTP URL that contains the following syntax:
scp://user':'password'@host[:port]/path

If you specify a path that ends with a forward slash (/), the file is written to the path that
you specify with the default file name. If you specify a path that does not end with a forward
slash, the file is written with the file name that is specified in the path. When the user name
or password are part of the URL, write them in quotes if they have any special shell
characters in them. You can specify the password in the URL or at the password prompt.

For example:
malquery -p 1h -e RCPTS=dale@company.com -e "SUBJECT*check this out" \ -m
500 -o ftp://evan@ftp.company.com/home/evan/audit.info.txt

-p, --previous
Search the last range time.
The format of the range time is <integer><type> where type is m (minutes), h (hours), d
(days), or w (weeks).
For example: 5h searches the last 5 hours.

-q ..., --qevent
Find email messages that contain the events that match the specified criterion in
quoted-printable encoding. For example:
-q "SUBJECT*red =3D rose" -- subject contains 'red = rose'

Use the equals character (=) for an exact match. Use the asterisk (*) for contains. Searches are case-insensitive.

A list of the more common elements that you can search are as follows:

- ACCEPT
  Connection IP
- ATTACH
  Attachment file name
- MSGID
  Message ID
- RCPTS
  Recipient address
- SENDER
  Sender address
- SUBJECT
  Message subject

-s, --start
Beginning of date range to search. Date should be in the following form: YYYYMMDDhhmm. For example:

-v, --verbose
Show the command process in verbose mode (debug logging).

EXAMPLES

Example 1
Search for an email based on the following criteria:

- Start date is between July 4, 2008, 2:00 P.M. and date of July 4, 2008, 11:59 P.M. in GMT time
- Recipient is "dale@company.com"
- Subject contains the words "check this out"
- Maximum output is 500 results
- Send the output to 'user' on 'host.domain.com' through FTP
Example 2
Search for an email based on the following criteria:
- Start date is between July 4, 2009, 11:00 P.M. and date of July 4, 2009, 11:59 P.M.
- Audit ID: 0aa0f22b-b7c99ae000005dd7-47-4e6e7b0468ad
- Maximum output is 500 results

Example 3
Search for an email based on the following criteria:
- Start date is between July 4, 2009, 11:00 P.M. and the current time
- Recipient is "dale@company.com" using a quoted-printable encoded string
- Subject contains the words "Barney's Grill", using the quoted-printable encoded string "Barney=27s Grill"
- Maximum output is 500 results

Example 4
Search for an email based on the following criteria:
- Date is within the last 2 days
- Recipient is "dale@company.com"
- Subject contains the words "check this out"
- Number of matching results for this command is the default index_max of 1000
- Send the output to 'user' on 'host.domain.com' through SCP

Example 5
Search audit logs for messages rejected due to reputation verdicts:
- Date is within the last 3 hours
SEE ALSO

See mallog on page 779.
monitor

monitor – view and record information about Symantec Messaging Gateway-specific processes

SYNOPSIS

monitor options [--proc name] [identifier ...]
monitor list
monitor stop ( pid | all )

DESCRIPTION

The monitor command lets you view and record detailed information about Symantec Messaging Gateway and its processes.

OPTIONS

--count, -c num
  Produce num samples.
  The default is 1. The upper limit is 2^31-1 (roughly, 2.1 billion).

--help, -h
  Display this message.

--interval, -i num
  Take a sample at the num interval (measured in seconds).
  The default is 10 seconds. For any long-running monitor jobs that are written to disk, you should increase this interval (to 60 or more). If the disk space fills up, the monitor process stops. Increase the interval time to avoid this issue.

--output, -o file
  Save the output to a file instead of printing it to the console. The file is saved as /data/monitor/file.
  When you use this option, monitor runs in the background and returns the process ID (PID) of the monitor process. Use cat, more, or tail to view the file. The file name can contain ASCII characters.

--proc, -p name
  Collect data for one of the following Symantec Messaging Gateway processes and its children. The valid process names and the programs that they represent are as follows:
**bmagent**

The Brightmail Agent facilitates communicating configuration information between the Control Center and each Scanner.

**bmserver**

The *bmserver* process filters email messages.

**conduit**

The Conduit retrieves updated email filters and manages statistics.

**controlcenter**

The Control Center provides centralized Web administration, collects statistics, and hosts quarantines.

**liveupdate**

LiveUpdate downloads virus definitions from Symantec Security Response to the Scanner.

**lsisnmpd**

The *lsisnmpd* process provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

All currently-supported hardware should have the *lsisnmpd* process running. No currently-supported virtual environments should have this process running.

**monitor**

The *monitor* process displays or saves information about Symantec Messaging Gateway processes.

**mta**

The mail transfer agent routes inbound and outbound messages to the Brightmail Engine for processing and delivers filtered messages.

**mysql**

The MySQL database on the Control Center stores settings and message information.

**snmpd**

The *snmpd* process waits for requests from SNMP management software.

---

**--quiet, -q**

Suppress any warnings from the monitor program.

**--tab, -t**

Produce data in a tabular format. Use the **--tab** option with the **--output** option to create output to import into a spreadsheet. The **--tab** does not format text correctly for the screen. For example, on the screen the column headings are not aligned with the column data.
When you format data for tabular output --tab, the column headings for each identifier are prefaced with the process name. For example, `controlcenter_p_%user`.

ARGUMENTS

**list**

Produce a list of all monitor processes, their PIDs, and the options that were used at runtime. The `monitor list` command always shows the `monitor list` command as one of the monitor processes that is running. This behavior is normal.

**stop ( pid | all )**

Stop the specified monitor processes. Type a PID to stop a single process. Type the word `all` to stop all monitor processes.

**identifiers**

The information that is displayed or saved depends on the identifiers that you specify. If you do not specify one or more identifiers, then the default of `system` is used. Some identifiers represent multiple identifiers and are provided for convenience. Five groups of identifiers are available: system, database, disk, MTA, and process.

System identifiers are as follows:

- `%user` - Percent of the available CPU time that is spent in user mode.
- `%nice` - Percent of the available CPU time that is spent running as nice.
- `%sys` - Percent of the available CPU time that is spent in system mode.
- `%wait` - Percent of the available CPU time that is spent in IO wait.
- `%idle` - Percent of the available CPU time that is spent idling.
- `memt` - Total memory (k)
- `memu` - Memory in use (k).
- `pageout` - The number of memory pages that are swapped out to disk.
- `system` - A convenience identifier that includes the following system identifiers: `%user %sys %wait memt memu memf`.

Database Identifiers - These identifiers denote the size of the Control Center database, the size of its various quarantines, and how many messages they contain. The identifiers are as follows:

- `db_size` - The total size of the Control Center database in kilobytes.
- `db_qsize` - The size of the Spam Quarantine directory kilobytes.
- `db_qqty` - The number of messages in the Spam Quarantine.
- `db_vsize` - The size of the Suspect Virus Quarantine directory, in kilobytes.
- `dv_vqty` - The number of messages in the Suspect Virus Quarantine.
- `db_csize` - The size of the content incident directories.
- `db_cqty` - The number of messages in the content incident quarantine.
- `database` - A convenience identifier that includes all the database identifiers.

Disk identifiers - The disk identifiers provide information on disk utilization on the partitions that the administrator controls. The identifiers are as follows:
- `data_used` - The amount of the `/data` partition that is being used, in kilobytes.
- `data_free` - The amount of free space in the `/data` partition, in kilobytes.
- `opt_used` - The amount of the `/opt` partition that is being used, in kilobytes.
- `opt_free` - The amount of free space in the `/opt` partition, in kilobytes.
- `other_used` - The amount of the `/` partition that is being used, in kilobytes.
- `other_free` - The amount of free space in the `/` partition, in kilobytes.
- `disk` - A convenience identifier that includes all the above disk data.

MTA identifiers - These identifiers report MTA statistics. The identifiers are as follows:
- `i_conn` - Number of inbound connections.
- `i_qmsgs` - Number of queued inbound messages.
- `i_dmsgs` - Number of deferred inbound messages.
- `i_qsize` - Size of the inbound queue (MBs).
- `i_drate` - Inbound listener data rate (kbps).
- `i_mrate` - Inbound listener message rate.
- `mta_in` - All of the inbound statistics (the identifiers that begin with `i_`).
- `o_conn` - Number of outbound connections.
- `o_qmsgs` - Number of queued outbound messages.
- `o_dmsgs` - Number of deferred outbound messages.
- `o_qsize` - Size of the outbound queue (MBs).
- `o_drate` - Outbound listener data rate (kbps).
- `o_mrate` - Outbound listener message rate.
- `mta_out` - All of the outbound statistics (the identifiers that begin with `o_`).
- `d_conn` - Number of delivery connections.
- `d_qmsgs` - Number of queued delivery messages.
- `d_dmsgs` - Number of deferred delivery messages.
- `d_qsize` - Size of the delivery queue (MBs).
- `d_drate` - Delivery listener data rate (kbps).
- `d_mrate` - Delivery listener message rate.
- `mta_del` - All of the delivery statistics (the identifiers that begin with `d_`).
- `mta` - A convenience identifier that includes all of the MTA identifiers.

The information that is collected depends on the identifiers that are provided. If none are provided, then the default is used: `system`. Some identifiers represent multiple identifiers and are provided for convenience.

This command does not give any indication about the average load or amount of work that is done between one sample and the next. Each sample is a snapshot of the MTA status at that point in time.

**Process identifiers** - The `--proc` option lets you monitor statistics for groups of Symantec Messaging Gateway processes. If the `--proc` flag is used without any `p_*` identifiers, the following default value is used: `p_%user` `p_%sys` `p_memv` `p_memr` `p_memr`. Identifiers for use with `--proc` include:

- `p_%user` - Percent of the available CPU time that is spent in user mode.
- `p_%sys` - Percent of the available CPU time that is spent in system mode.
- `p_memv` - Virtual memory that the processes use (k).
- `p_memr` - Resident memory in use by the processes (k).
- `p_mems` - Highest amount of the shared memory that any of the processes use (k).
- `p_all` - All of the proc identifiers.

**EXAMPLES**

The following examples describe some ways that you can use the `monitor` command. These examples include a mix of the long and short forms of some of the option names, such as `--o` and `--output`.

**Example 1**

Check one time the percent of available CPU time and memory that the conduit service consumes. Save the result to file `/data/monitor/conduit_mon`.

```
monitor --proc conduit --output conduit_mon
```

**Example 2**
Collect the average load of the MTA service on the system every 3 seconds 1000 times. Display the average load on the system from the MTA service in a tabbed format and written out to file /data/monitor/mta_mon.

```bash
monitor --proc mta --interval 3 --count 1000 --tab --output mta_mon
```

**Example 3**

Check one time the percent of available CPU time and the memory that the LiveUpdate service uses. Save the result to file /data/monitor/liveupdate_mon.

```bash
monitor --proc liveupdate --output liveupdate_mon
```

**Example 4**

Check one time the percent of available CPU time and the memory that the monitor service consumes. Save the result to file /data/monitor/monitor_mon in tabbed format.

```bash
monitor --proc monitor --output monitor_mon --tab
```

**SEE ALSO**

See `cat` on page 739.

See `delete` on page 752.

See `list` on page 777.

See `more` on page 793.

See `tail` on page 821.
more

more – a standard Linux command to page through a text file

DESCRIPTION

The `more` command displays the contents of plain text files one screen at a time. Press `Space` to view the next screen. Use the `list` command to list the files that `more` can display.

You can run the output of another command to `more` to view the output one screen at a time. After the command that you are running, type the pipe symbol and then `more`. See the example below.

Type `help more` on the command line for more information about the options available for `more`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

The `more` command is a standard Linux command that has been modified to only display the files that the `list` command shows.

EXAMPLES

Example 1

Display BrightmailLog.log one screen at a time.

```
more /data/logs/bcc/BrightmailLog.log
```

Example 2

Examine the output of `list --top` one screen at a time.

```
list --top | more
```

SEE ALSO

See `list` on page 777.
mta-control

mta-control – control the MTA processes and backup and restore mail queues

SYNOPSIS

mta-control queue command

mta-control pause-mode mode

DESCRIPTION

The mta-control command lets you query MTA queues, and control specific elements within MTA message processing. For example, you can flush message queues.

Note: Do not use the ~ (tilde) character when you specify output file names, paths, passwords, email addresses, and user names (for exporting). Specify the full path name.

ARGUMENTS

Specify one of the following MTA queues:

- inbound
- outbound
- resubmission
- delivery
- all

The following components are available:

- start – Start the queue.
- stop – Stop the queue.
- status – Display the current status. The status can be: running, not running, enabled, or disabled.
- restart – Restart the queue.
- flush – Reattempt delivery for all queued messages.
- delete-msgs-by-sender regexp – Delete from the queue all messages with Envelope Sender that matches the given Perl regular expression (case insensitive).
- `delete-msgs-by-rcpt regexp` – Delete from the queue all messages with an Envelope Recipient that matches the given Perl regular expression (case insensitive).

  **Note:** This deletes the entire message, not just the recipient.

- `delete-msg-by-id queue-ID` – Delete the message with the given queue-ID from the queue.
- `delete-all-msgs` – Delete all messages from the queue.
- `bypass-resubm-by-sender regexp` – Bypasses resubmission for all messages in the resubmission queue with envelope sender that matches the given Perl regular expression. (case insensitive)
- `bypass-resubm-by-rcpt regexp` – Bypasses resubmission for all messages in the resubmission queue with envelope recipient that matches the given Perl regular expression. (case insensitive)
- `bypass-resubm-by-id queue-ID` – Bypasses resubmission for the message with the given queue-ID from the resubmission queue. The ID is only unique per instance.
- `bypass-resubm-all` – Bypasses resubmission for all messages from the resubmission queue.
- `active-routes` – Print all active routes and the number of messages for each route.
- `num-messages-in-route route` – Print the number of messages for the given route.
- `num-msgs-by-rcpt route` – Print the number of messages for each recipient domain on a given route.
- `num-msgs-by-rcpt-all-routes` – Print the number of messages for each recipient domain on a given route.
- `list-msgs route` – Print the messages for the given route.
- `list-msg-details msgid` – Given a message ID, print details about that message.
- `route-info route` – Display DNS lookup information, destination, and number of messages for a route.
- `reroute src-routedst-route` – Reroute messages from `src-route` to `dst-route`.
- `delete-msgs-by-sender perl regexp` – Delete from the queue all messages with an envelope sender that matches the given Perl regular expression (case insensitive).
- `delete-msgs-by-rcpt perl regexp` – Delete from the queue all messages with an envelope recipient that matches the given Perl regular expression. Note that this deletes the entire message, not just the recipient (case insensitive).
- `delete-msg-by-id queue-ID` – Delete the message with the given queue-ID from the queue. Note that the ID is only unique per queue.
- **delete-all-msgs** – Delete all messages from the queue.

- **import-queues** `url` – Import an entire mail queue from backup. Specify `all` for the queue. Ensure that the MTA is running before importing a mail queue. To start the MTA, run `mta-control all start`. Specify the URL as described for the export-msg-by-id component.

- **export-queues** `url` – Back up the mail queue to a URL. Specify `all` for the queue. Ensure that the MTA is stopped before exporting the mail queue. To stop the MTA, run `mta-control all stop`. Specify the URL as described for the export-msg-by-id component.

- **export-msg-by-id** `queue-ID [url]` – Export the message with the given queue-ID from the queue and save it to the specified URL. If you do not specify a URL, the message data is displayed on the screen. If you do not specify the FTP password, `mta-control` prompts you for the password. If you specify a path that ends with `/`, Symantec Messaging Gateway stores the file in that location using a default file name. Otherwise, Symantec Messaging Gateway stores the file with the file name that you specified in the path. The URL syntax is as follows:
  - `scp://user\@host/path` (user is prompted for password)
  - `ftp://user:password\@host[:port]/path`
  - `ftp://user\@host[:port]/path`

  Put a double-quote character before and after the URL. If any part of the URL contains special characters, such as full or double quotes, put a backslash before each special character.

- **query-queue** – Query the message queue.
  - The following additional parameters are accepted:
    - `sender_match=perl regexp`
    - `rcpt_match=perl regexp`
    - `deferred` - selects the messages that are deferred
    - `include_subject`
    - `start=N`
    - `limit=N`
    - `format=neat|xml`

  The parameters `sender_match`, `rcpt_match`, and `deferred` are logically ANDed together if present. The intermediate result set after you apply these matches is sorted by date, and then the start and limit are applied: `$start` messages are skipped and then `$limit` messages are returned. The default is to show all messages in 'neat' format, which is meant to be human readable.
bad-msg-list – List the times and IDs of messages in the bad message queue. The queue is either inbound or outbound.

bad-msg-export queue-ID [url] – Export or display the message. See export-msg-by-id for URL format.
To display the message on the screen, type mta-control queue bad-msg-export queue-ID.
Specify the URL as described for the export-msg-by-id component.

bad-msg-delete queue-ID – Delete the message.

bad-msg-bypass queue-ID – Submit the message for delivery to the original recipients and bypass scanning.

bad-msg-forward queue-ID address – Submit a copy of the message for delivery to the given address and bypass scanning. The original bad message remains in the bad message queue.

bad-msg-retry queue-ID – Retry scanning the message as if it were new.

regen-dh-keys – Regenerate keys for Diffie Hellman ciphers used by the MTA for TLS communications.

The six pause modes affect email scanning (scan), acceptance (accept), and delivery (delivery). Each pause mode sets scanning, acceptance, and delivery to a particular state as described below, regardless of the previous state of scan, accept, and delivery. Pause modes are as follows:

status – Display the current pause mode status. If you type mta-control pause-mode, mta-control displays the pause mode status.

pause-accept – Set scan to running and set accept to paused. The delivery state is not affected by pause-accept.

pause-deliver – Set delivery to paused. The accept and scan states are not affected by pause-deliver. This is equivalent to mta-control delivery stop.

pause-scan – Set scan to paused and set accept to running. The delivery state is not affected by pause-scan.

resume-accept – Set scan to running and set accept to running. The delivery state is not affected by resume-accept.

resume-deliver – Set delivery to running. The accept and scan states are not affected by resume-deliver. This is equivalent to mta-control delivery start.

resume-scan – Set scan to running and set accept to running. The delivery state is not affected by resume-scan.
EXAMPLES

Example 1
Show the status of the MTA (inbound, outbound, and delivery queues and whether they are running or not).

mta-control pause-mode status

Example 2
Do not accept any new mail on the appliance but scan mail in the queue. This command does not affect the delivery of email.

mta-control pause-mode pause-accept

Example 3
Accept email on the appliance, but do not scan it. This command does not affect the delivery of email.

mta-control pause-mode pause-scan

Example 4
Do not deliver email on the appliance.

mta-control pause-mode pause-deliver

Example 5
Accept and scan email on the appliance. This command does not affect the delivery of email.

mta-control pause-mode resume-accept

Example 6
Accept and scan email on the appliance. This command does not affect the delivery of email.

mta-control pause-mode resume-scan

Example 7
Deliver email on the appliance.

mta-control pause-mode resume-deliver

Example 8
Display the queue-id of messages in delivery queue.

mta-control delivery query-queue

Example 9
View a raw message in the delivery queue with a message queue-id.

mta-control delivery export-msg-by-id 00/00-25597-EFD46794
Example 10

Export a specific message from the delivery queue with a message queue-id. The message queue-id is 00/00-25597-EFD46794. Export it to the 192.168.159.99 SCP server in the /tmp directory with the support account. *mta-control* queries for the password.

```bash
mta-control delivery export-msg-by-id 00/00-25597-EFD46794 "scp://support@192.168.159.99/tmp/"
```

Example 11

Export all message queues. Export the message queue file to the 192.168.159.99 FTP server in the /tmp directory with the sysadmin account. Since a password is not specified, *mta-control* queries for the password.

```bash
mta-control all export-queues "ftp://sysadmin@192.168.159.99/tmp/"
```

Example 12

Show all messages currently in the inbound queue, the outbound queue, the delivery queue and the resubmission queue.

```bash
mta-control all query-queue
```

Example 13

Bypass resubmission for all messages in the resubmission queue with envelope sender that matches the given Perl regular expression.

```bash
mta-control resubmission bypass-resubm-by-sender user@company.com
```

Example 14

Bypass resubmission for all messages in the resubmission queue with envelope recipient that matches the given Perl regular expression.

```bash
mta-control resubmission bypass-resubm-by-rcpt user@company.com
```

Example 15

Bypass resubmission for the message with the given queue-ID from the resubmission queue.

```bash
mta-control resubmission bypass-resubm-by-id AC/B7-30310-4CDE7E85
```

Example 16

Bypass resubmission for all messages from the resubmission queue.

```bash
mta-control resubmission bypass-resubm-all
```
netstat

netstat – a standard Linux command to view network connections

DESCRIPTION

The netstat command prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Type help netstat on the command line for more information about the options available for netstat. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

EXAMPLES

Example 1
Display network connections.

netstat -an

Example 2
Display routing table.

netstat -r
**nslookup**

nslookup — a standard Linux command to query DNS servers

**DESCRIPTION**

The `nslookup` command performs a DNS lookup of the given hostname or IP address.

Type `help nslookup` on the command line for more information about the options available for `nslookup`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is part of the standard Linux command set. It has been modified for use by Symantec Messaging Gateway, but this modification does not affect its functionality.

**EXAMPLES**

Look up MX records for a domain (yahoo.com, for example):

```
nslookup -querytype=mx yahoo.com
```
password

password -- change your administrative password

SYNOPSIS

password [--help] [--reset]

DESCRIPTION

The password command changes the password that you use to logon to the command line. You are prompted to type your old password, and to type your new password twice.

Note: If you are using the Control Center appliance when you change the password, the admin password for login to the Control Center is also changed.

OPTIONS

--help, -h
Display this message.

--reset, -r
Set the administrative password to the factory default.
patch

patch – handle all necessary functions that are related to SMG patches

SYNOPSIS

patch [-o | --options ]
patch -help
patch [--releaseversion | -r n] list
patch [--patchversion | -p n] notes
patch <--patchversion | -p n> check | download | install
patch remove
patch localinstall <URL-to-ISO-file>
patch localcleanup

DESCRIPTION

The patch command handles all necessary functions that are related to SMG patches.

ARGUMENTS

check

Test the patch. This runs all of the pre-update checks but does not update your appliance software.

The check command requires a patch version argument, and the provided version must match the currently installed SMG version (e.g. to install patch 10.6.4-X, the appliance must be at version 10.6.4-Y)

download

Retrieve a version of the patch

The download command requires a patch version option, and the provided version must match the currently installed SMG version (e.g. to install patch 10.6.4-X, the appliance must be at version 10.6.4-Y)

install

Install a patch, downloading it if necessary
The install command requires a patch version option, and the provided version must match the currently installed SMG version (e.g. to install patch 10.6.4-X, the appliance must be at version 10.6.4-Y).

The install command prompts for confirmation before proceeding, and forces a reboot after successful completion.

remove

Back out all installed patches (in reverse order of installation)

The remove command prompts for confirmation before proceeding, and forces a reboot after successful completion.

list

Display a list of available patches for a specific released version (defaults to currently installed release), and patch installation history is displayed, if applicable

The list command takes an optional version option, but without the restrictions on the acceptable version number(s) as with the check, download, and install commands.

notes

Display a description of the patch (defaults to currently installed patch)

The notes command takes an optional version option, but without the restrictions on the acceptable version number(s) as with the check, download, and install commands.

localinstall <URL-to-ISO-file>

Install a patch by downloading an ISO from the specified URL

The localinstall command checks versions based on the available patch in the downloaded ISO file.

localcleanup

Remove temporary files that may have been left behind from a previously failed localinstall attempt

Options

--releaseversion, -r
Specify a release version number. For example, 10.6.3.

--patchversion, -p
Specify a patch version number. For example, 10.6.3-008.

--help, -h
Get more extensive help.
**ping**

`ping` – a standard Linux command to test for a response from a remote computer

**DESCRIPTION**

The `ping` command tests, through data packet, the transfer of that data between the appliance and the hostname or IP address that you specify.

Type `help ping` on the command line for more information about the options available for `ping`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
ping6

ping6 – standard Linux command to test the transfer of data between the issuing machine and the given IPv6 hostname or IP address

DESCRIPTION

This command is part of the standard Linux command set.

Type help ping6 on the command line for more information about the options available for ping6. The information that appears may contain references to commands that are not available on Symantec Messaging Gateway.
reboot

reboot – reboot the appliance

SYNOPSIS

reboot [--force]

DESCRIPTION

The `reboot` command stops all services and then restarts the appliance.

---

**Note:** When prompted, you must type `yes` to complete shutdown. Typing `y` results in an error message.

---

**Note:** If you reboot the appliance while you run software update on Symantec Messaging Gateway, you can corrupt the appliance software.

---

OPTIONS

--force, -f

Reboot the appliance, even if software update is running (not recommended). The appliance can become corrupted and require reinstallation. Contact Symantec Technical Support for information about reinstalling the appliance software.

--help, -h

Display this message.

SEE ALSO

See `shutdown` on page 815.
route

route – a standard Linux command to show and manipulate the IP routing table

DESCRIPTION

The route command lets you view routing tables or add entries to a routing table temporarily. Its primary use is for viewing the routing tables.

Type help route on the command line for more information about the options available for route. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
**rpmdb**

**rpmdb** – manage and repair the RPM database

**SYNOPSIS**

```
rpmdb [--verify] [--repair]
```

**DESCRIPTION**

The `rpmdb` command lets you verify the current RPM database and rebuild it. This command can be useful in the event the database is corrupted and you want to repair it. Software updates for Symantec Messaging Gateway are stored as RPM packages.

**OPTIONS**

```
--repair, -r
    Rebuild the RPM database.

--verify, -v
    Verify the current RPM database.
```
rsa-key

rsa-key  – import, export, test, display or delete an RSA key

SYNOPSIS

rsa-key

DESCRIPTION

Import, export, test, display or delete an RSA key.

ARGUMENTS

rsa-key export - display key for import into remote host
rsa-key import (key) - copy key into local keyring. You will need to quote the 'key' value.
rsa-key test (user@host) - test the connection to the user on a host
rsa-key status - display local keyring
rsa-key clear (option) - delete all keys and keyrings option is one of: local_key, keyring, known_hosts, all
service

service – a standard Linux command to start or stop services

SYNOPSIS

    service name command
    service name help

DESCRIPTION

Start, stop, and check the status of Symantec Messaging Gateway services with the service command. Services are programs that run continuously to perform specific tasks. During normal operation, you do not have to stop or start services. You may need to stop or start services to diagnose or resolve a problem with Symantec Messaging Gateway.

The service command is a standard Linux command that has been modified to work with services available on Symantec Messaging Gateway.

ARGUMENTS

Specify a service name and command when you run service.

name

Specify one of the following service names:

agent
    The Brightmail Agent facilitates communicating configuration information between the Control Center and each Scanner.

connector
    The Conduit and LiveUpdate services download spam and virus definitions.

controlcenter
    The Control Center provides centralized Web administration, collects statistics, and hosts quarantines.

dds
    Directory data service interfaces with LDAP to provide authentication, email address validation, message routing, and policy groups.

If you restart the dds service, the bmclient_log and bmserver_log log files may contain many Could not connect: Connection refused errors. These errors are normal.
lsisnmpd
   The lsisnmpd service provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

mta
   The mail transfer agent processes, routes, and delivers email messages in cooperation with the Brightmail Engine.

mysql
   The MySQL database on the Control Center stores settings and message information.

osconfig
   The osconfig service manages network interfaces and related services.

smsswapfile
   The smsswapfile service manages secondary swap file space.

snmpd
   The snmpd service waits for requests from SNMP management software.

casoop
   The casoop service manages communication between the SMG and CA servers.

command
   The following commands are available. Some commands do not apply to certain commands. Type service name help to display the commands that apply to a service.

condrestart
   Restart the service only if it is currently running. This command is available only for the controlcenter, snmpd and mta services.

delete
   Delete the swap file on the appliance. This command is available only for the smsswapfile service.

help
   Display the commands available for the service that you specify.

reload
   This command is available only for the mysql service.

restart
   Stop the service and then start the service.

status
   Display the status of a service.

start
   Start the service.
stop
Stop the service.

EXAMPLES

Example 1
Display the commands that are available for the mta service.

service mta help

Example 2
Display the status of the mta service.

service mta status

Example 3
Stop the mta service.

service mta stop

Example 4
Stop the Conduit, LiveUpdate, and jlu-controller.

service connector stop
show

show – display system information

SYNOPSIS

show [--date] [--eula] [--info] [--version]

show --help

DESCRIPTION

The show command displays the following information:

- Current date and time
- End User License Agreement
- System information
- Product version number

OPTIONS

--date, -d
Show the current date and time.

--eula, -e
Show the End User License Agreement.

--help, -h
Display this message.

--info, -i
Show the system hardware information.

--version, -v
Show the product version number and installation date.
**shutdown**

**shutdown** – shut down the appliance without rebooting

**SYNOPSIS**

```
shutdown [--help | --force]
```

**DESCRIPTION**

The `shutdown` command turns off the appliance immediately. The appliance is not restarted. Shutdown occurs immediately and email messages remain in the queues. To start an appliance after you run the `shutdown` command, you must press the appliance power button, unless you have configured remote access to the appliance hardware.

**Note:** When prompted, you must type **yes** to complete shutdown. Typing **y** results in an error message.

**Note:** If you shut down the appliance during the software update process, you can corrupt the appliance software.

**OPTIONS**

```
--help, -h
  Display this message.

--force, -f
  Shut down the appliance, even if software update is running (not recommended). The appliance can become corrupted and require reinstallation. Contact Symantec Technical Support for information about reinstalling the appliance software.
```

**SEE ALSO**

See `reboot` on page 807.

See “Turning off an appliance” on page 703.
sshd-config

sshd-config – configure which addresses can SSH to the appliance

SYNOPSIS

sshd-config (--list | --help)
sshd-config --add (allow|deny) [IPv6 address] or IPv4 address
sshd-config --delete (allow|deny) rule#
sshd-config --version [1|2]
sshd-config --cbc [on|off]
sshd-config --mac [on|off]

DESCRIPTION

The sshd-config command lets you specify which addresses can access the appliance through SSH.

Note: IPv6 addresses must be enclosed in brackets.

OPTIONS

--add, -a
   Add a new rule.
--cbc, -c
   Turn support for CBC ciphers, also known as block ciphers, on or off. If set to off, the only cipher available for use is RC4, also known as arcfour.
--delete, -d
   Delete an active rule.
--help, -h
   Display this message.
--list, -l
   Display the active rules and the current protocol number.
-m, --mac
   Turn on or off the limited support for hmac algorithms.
--version, -v

Show the version number of the protocol, CBC ciphers and limited MACs, and set or change the version number of the protocol used.

- To set the version number of the protocol use (1 or 2).
- To display the settings without 1/2, for example:

```bash
crt-vwei-08> sshd-config -v
```

Requires protocol version 2

Support for CBC ciphers is ENABLED

Support for limited MACs (hmac-sha2-256, hmac-sha2-512) is ENABLED

ARGUMENTS

allow/deny

When an SSH client connects, the client address is compared to the allow list and deny list in the following order:

- If the client address matches any allow rules, then the connection is allowed.
- If the client address matches any deny rules, then the connection is rejected.

rule

Each rule is a list of one or more addresses and wildcards that are separated by commas, as follows:

- some.hostname.com
  Matches a specific host
- `some | other.hostname.com`
  Matches `some.hostname.com` and `other.hostname.com`
- 1.2.3.4
  Matches a specific IP address
- 1.2.
  Matches any IP address starting with 1.2
- 1.2.3.0/255.255.255.0
  Matches any IP address within the 1.2.3.* subnet
  The EXCEPT keyword can be used to exclude a subset of addresses. For example, `hostname.com EXCEPT forbidden.hostname.com`.
- `[[:[]]]/m

An IPv6 host address is matched to an address if the prefixlen bits of ‘net’ is equal to the prefixlen of the address. For example, the [net]/prefixlen pattern [3ffe:505:2:1::]/64 would match every address in the range 3ffe:505:2:1:: through 3ffe:505:2:1:ffff:ffff:ffff:ffff.

You can specify one of the following keywords instead of a host name or IP address for the address parameter. Use the KNOWN and UNKNOWN keywords with care since they depend on DNS service.

- **ALL**
  - Matches any address

- **LOCAL**
  - Matches any host whose name does not contain a dot character

- **KNOWN**
  - Matches any host whose name and address are known

- **UNKNOWN**
  - Matches any host whose name or address are unknown
**symdiag**

`symdiag` – collects and exports system diagnostics

**SYNOPSIS**

```
symdiag [--proactive | --healthcheck][--verbose][url]
symdiag [--help]
```

**DESCRIPTION**

The `symdiag` command collects system diagnostics and exports the diagnostic file to a location specified by the user.

If no options are specified, then 'proactive' and 'healthcheck' actions are performed. If 'proactive' and 'healthcheck' are both specified, an error message is displayed and no action is performed.

When the user name or password are part of the URL, write them in quotes if they have any special shell characters in them. The password can be specified in the URL or at the password prompt. An example of the URL syntax is as follows:

```
scp://'user':'password'@host[:port]/path/
```

The URL in the command argument must end in a '/'. You cannot specify the file name, but only the directory where the output file will be placed. The diagnostics file is written to the path that you specify with the default file name.

The output file name is in the following format:

```
<hostname>__<date>__<time>__AAAAAA.sdbz
```

where AAAAAA is a 6 digit hexadecimal number.

A zero-byte file with ‘TEST’ instead of the 6 digit hexadecimal number is also created. This file is created to validate the username, password, hostname, etc. from the URL before the command to generate the output is run.

**OPTIONS**

```
--proactive, -p
  Gathers and reports information for "Configuration Review" which is the proactive service.

--healthcheck, -c
  Checks core systems.

--verbose, -v
  Collect diagnostic information in verbose mode.
```
--help, -h

   Show this message.
tail

tail – a standard Linux command to view the end of a file

SYNOPSIS

tail [-f | --help] log_name

DESCRIPTION

The tail command is part of the standard Linux command set which shows the last 50 lines of the named log file.

However, this command is modified in the following ways:

■ Only the -f and --help options that are described here are available.

■ If a character in a log file is not printable or is not ASCII, the sequence \xAB is displayed instead of that character. AB is the hexadecimal value of the character. For example, a character with a decimal value of 128 is displayed as \x80.

■ This command is restricted to the file names that are obtainable from the list command. The list command displays the file names of all of the files that can be acted upon by certain commands. In addition to the tail command, the following commands can act upon the files that are listed with list:

  cat
    Display the contents of one or more files.

  delete
    Delete one or more files.

  more
    Display the contents of one or more files and pause at the end of each screen.

OPTIONS

-f

Follow the file as new text is added to it. The tail -f command prints the last 10 lines of the file but does not exit. As new text lines are added to the file, tail displays the new text lines. The -f option is useful for monitoring a log file as additional information is added to the log file. If you type tail -f log_name and nothing seems to happen, the file is empty, the file is not being written to, or both.

To stop monitoring a file, press Ctrl+C.
--help, -h
  Display this message.

ARGUMENTS

log_name

log_name can be any of the following:
  ■ agent_log
  ■ battery.log
  ■ bmclient_log
  ■ bmserver_log
  ■ boot.log
  ■ BrightmailLog.log
  ■ conduit_log
  ■ cron
  ■ db-migration.log
  ■ dds.log
  ■ dmesg
  ■ imlinkage_log
  ■ jlu-controller_log
  ■ liveupdt.log
  ■ maillog
  ■ messages
  ■ named.run
  ■ secure
  ■ update.log

EXAMPLES

Example 1
Display the last 50 lines of the BrightmailLog.log log file.

tail BrightmailLog.log
Example 2

During an update, monitor the `update.log` log file. If you see information being written to `update.log` periodically, it usually means that the update is proceeding normally.

`tail -f update.log`

SEE ALSO

See list on page 777.
**telnet**

*telnet – a standard Linux command to connect to a remote computer*

**DESCRIPTION**

The `telnet` command lets you log into the command line of another computer on your network from the appliance.

Type `help telnet` on the command line for more information about the options available for `telnet`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
traceroute

traceroute – a standard Linux command to view the path taken by network packets

DESCRIPTION

The traceroute command displays the network route to the given hostname or IP address.

Type help traceroute on the command line for more information about the options available for traceroute. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.
traceroute6

traceroute6 — standard Linux command to trace the network route to the given host name or IPv6 address

DESCRIPTION

This command is part of the standard Linux command set.

Type traceroute6 --help on the command line for more information about the options available for traceroute6. The information that appears may contain references to commands that are not available on Symantec Messaging Gateway.
update

update – update the appliance software

SYNOPSIS

update list

update [--version | -v number] ( check | download | install | notes )

update localinstall URL to ISO file

update localcleanup

update --help

DESCRIPTION

You can perform the following tasks with the update command:

- Check for new software updates
- Download software updates
- Install software updates from the Internet or locally
- List the available software updates for download or installation

Before you update the software, ensure that your appliance is not performing any tasks that, if disrupted, could cause problems after you reset the appliance. Also ensure that you perform a backup of your database.

See db-backup on page 744.

OPTIONS

--help, -h

Display this message.

[--version | -v n] check | notes | download | install

Specify a software update version number for the check, download, install, or notes arguments.

ARGUMENTS

check

Perform a test update.
The test update demonstrates what happens if you choose to perform a software update. Running `update check` does not update your appliance software. If you do not specify a version, the test update uses the latest software version. For example, if you run `update check` without specifying the version, and your appliance is currently running a version that must be updated to an interim version before it can be updated to the latest version, the test fails. You can check the Release Notes to find information on approved update paths.

**download**

Download but do not install a software update. Defaults to the latest released version.

After you download a software update, you can install it by typing `update install`. If you do not specify a version, the latest software update is downloaded.

**install**

Download and install a software update. If you do not specify a version, the latest software update is installed on your appliance.

Defaults to the latest released version.

**list**

Display the available software updates.

**localinstall URL to ISO file**

where `URL to ISO file` is the HTTP location from which Symantec Messaging Gateway can retrieve an OSRestore ISO.

Updates the software version without an Internet connection.

You first download an ISO image from Symantec and place it on an HTTP server that is accessible from the appliance.

**localcleanup**

Remove temporary files that may have been left behind from a previously failed `localinstall` attempt.

**notes**

Display the software update notes. If you do not specify a version, the latest software update notes appear.

**EXAMPLES**

`update download`

Download but do not install a software update. After you download a software update, you can install it by typing `update install`. 
SEE ALSO

See "Updating Symantec Messaging Gateway software " on page 717.
Message filtering options

This appendix includes the following topics:

- Action combinations from multiple verdicts
- Verdicts by verdict category
- Verdict combinations
- Positive and negative content filtering rule condition examples

Action combinations from multiple verdicts

Each time a message triggers a verdict, SMG adds the actions of the corresponding policy to an actions list. After all filtering is complete, SMG removes exact duplicates from the list and then evaluates the remaining actions. The actions can combine, or one action can override another action.

Action groups

Table B-1, Table B-2, and Table B-3 describe how SMG combines or overrides actions to process a message when the message triggers multiple verdicts. These tables reference the following groups of policy actions:

Firewall actions: Defer SMTP Connection, Reject SMTP Connection, Reject messages failing bounce attack validation

Event actions: Archive the message, Create an informational incident, Forward a copy of the message, Send a delivery status notification, Send notification

Delay virus actions: Hold message in Suspect Virus Quarantine, Strip and Delay in Suspect Virus Quarantine

Delay content action: Create a quarantine incident
Delete action: Delete message

Modify actions: Add a header, Add annotation, Add BCC recipients, Clean the message, Deliver message with TLS encryption, Modify the subject line, Remove unresolved recipients, Strip attachments, Disarm attachment(s)

Modify URLs actions: Modify clickable URLs in message: Email Threat Isolation, Web Service (ProxySG), Replace URLs, Disable URLs

Route actions: Hold message in Spam Quarantine, Route the message, Deliver message with content encryption (this action exhibits both route and modify category behaviors)

No action action: Deliver message normally

Results when all action groups combine with Firewall, Event, and Delay virus actions

The following table shows how actions in these groups combine or conflict with other actions. For the full list of actions in all groups, see Action groups.

Table B-1  
Firewall, Event, and Delay virus action combinations

<table>
<thead>
<tr>
<th>Action</th>
<th>Firewall</th>
<th>Event</th>
<th>Delay virus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall:</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
</tr>
<tr>
<td>Event</td>
<td>Firewall</td>
<td>Event + event</td>
<td>Event + delay</td>
</tr>
<tr>
<td>Delay virus</td>
<td>Firewall</td>
<td>Event + delay</td>
<td>Delay only once when there are duplicate Hold message in Suspect Virus Quarantine or Strip and Delay in Suspect Virus Quarantine actions Strip and Delay in Suspect Virus Quarantine overrides Hold message in Suspect Virus Quarantine.</td>
</tr>
<tr>
<td>Delay content</td>
<td>Firewall</td>
<td>Event + delay</td>
<td>Delay Content, defer Delay Virus</td>
</tr>
<tr>
<td>Delete</td>
<td>Firewall</td>
<td>Delete + event</td>
<td>Delete</td>
</tr>
</tbody>
</table>
Table B-1  Firewall, Event, and Delay virus action combinations (continued)

<table>
<thead>
<tr>
<th>Firewall:</th>
<th>Event:</th>
<th>Delay virus:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defer SMTP Connection,</td>
<td>Archive the message, Create an informational incident, Forward a copy of the message, Send a delivery status notification, Send notification</td>
<td>Hold message in Suspect Virus Quarantine, Strip and Delay in Suspect Virus Quarantine</td>
</tr>
<tr>
<td>Reject SMTP Connection,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject messages failing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bounce attack validation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modify</th>
<th>Firewall</th>
<th>Modify + event</th>
<th>Delay, defer modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify URLs</td>
<td>Firewall</td>
<td>Modify + event</td>
<td>Delay, defer modification</td>
</tr>
<tr>
<td>Route</td>
<td>Firewall</td>
<td>Route + event</td>
<td>Delay, defer routing</td>
</tr>
<tr>
<td>No action</td>
<td>Firewall</td>
<td>Event</td>
<td>Delay</td>
</tr>
</tbody>
</table>

Results when all action groups combine with Delay content, Delete, and Modify actions

The following table shows how actions in these groups combine or conflict with other actions. For the full list of actions in all groups, see Action groups.

Table B-2  Delay content, Delete, and Modify action combinations

<table>
<thead>
<tr>
<th>Delay content:</th>
<th>Delete:</th>
<th>Modify:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a quarantine</td>
<td>Delete message</td>
<td>Add a header, Add annotation, Add BCC recipients, Clean the message, Deliver message with TLS encryption, Modify the subject line, Remove unresolved recipients, Strip attachments, Disarm attachment(s)</td>
</tr>
<tr>
<td>incident</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firewall</th>
<th>Firewall</th>
<th>Firewall</th>
<th>Firewall</th>
</tr>
</thead>
</table>
Table B-2  Delay content, Delete, and Modify action combinations (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Modify: Add a header, Add annotation, Add BCC recipients, Clean the message, Deliver message with TLS encryption, Modify the subject line, Remove unresolved recipients, Strip attachments, Disarm attachment(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay content:</td>
<td>Delete: Delete message</td>
</tr>
<tr>
<td>Create a quarantine incident</td>
<td>Modify: Add a header, Add annotation, Add BCC recipients, Clean the message, Deliver message with TLS encryption, Modify the subject line, Remove unresolved recipients, Strip attachments, Disarm attachment(s)</td>
</tr>
<tr>
<td>Event</td>
<td>Delete + event</td>
</tr>
<tr>
<td>Delay virus</td>
<td>Modify + event</td>
</tr>
<tr>
<td>Delay content</td>
<td>Delay Content, defer Delay Virus</td>
</tr>
<tr>
<td>Delay virus</td>
<td>Delete + event</td>
</tr>
<tr>
<td>Delete</td>
<td>Modify + event</td>
</tr>
</tbody>
</table>

**Delay virus**

If a Create a quarantine incident action has a folder name that is alphabetically earlier than the folder for a Create an informational incident, SMG performs the Create an informational incident action after the message is released from quarantine. The informational incident is not created if the message is deleted from quarantine.

**Delay content**

For multiple Create a quarantine incident actions, the message is put in the quarantine folder that appears first in an alphanumeric sort. If the message is released from that quarantine, it then goes to folder that is alphabetically second. The process repeats until the message is released or deleted.

**Delete**

Delay, defer deletion

Delete once

Delete
### Table B-2

<table>
<thead>
<tr>
<th>Delay content: Create a quarantine incident</th>
<th>Delete: Delete message</th>
<th>Modify: Add a header, Add annotation, Add BCC recipients, Clean the message, Deliver message with TLS encryption, Modify the subject line, Remove unresolved recipients, Strip attachments, Disarm attachment(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modify</strong></td>
<td>Delay, defer modifications</td>
<td>Delete</td>
</tr>
<tr>
<td><strong>Modify URLs</strong></td>
<td>Delay, defer Modify URLs</td>
<td>Delete</td>
</tr>
<tr>
<td><strong>Route</strong></td>
<td>Delay, defer routing</td>
<td>Modify + route</td>
</tr>
<tr>
<td><strong>No action</strong></td>
<td>Delay</td>
<td>Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modify</td>
</tr>
</tbody>
</table>

**Results when all action groups combine with Modify URL, Route, and No action groups**

The following table shows how actions in these groups combine or conflict with other actions. For the full list of actions in all groups, see [Action groups](#).
Table B-3  Modify URLs, Route, and No action combinations

<table>
<thead>
<tr>
<th>Modify URLs</th>
<th>Route:</th>
<th>No action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Threat Isolation, Web Service (ProxySG), Replace URLs, Disable URLs</td>
<td>Hold message in Spam Quarantine, Route the message, Deliver message with content encryption</td>
<td>Deliver message normally</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify URLs + event</td>
<td>Route + event</td>
<td>Event</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delay virus</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay, defer Modify URLs</td>
<td>Delay, defer routing</td>
<td>Delay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delay content</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay, defer Modify URLs</td>
<td>Delay, defer routing</td>
<td>Delay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Delete</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Delete</td>
<td>Delete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modify</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify + Modify URLs</td>
<td>Modify + route</td>
<td>Modify</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modify URLs</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Modify URLs action takes precedence, in this order: (1) Email Threat Isolation, (2) Web Service (ProxySG), (3) Replace clickable URLs in message, (4) Disable clickable URLs in message</td>
<td>Modify + route</td>
<td>Modify</td>
</tr>
<tr>
<td>Route</td>
<td>Modify URLs: Email Threat Isolation, Web Service (ProxySG), Replace URLs, Disable URLs</td>
<td>Route: Hold message in Spam Quarantine, Route the message, Deliver message with content encryption</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>No action</td>
<td>Modify URLs</td>
<td>Route</td>
</tr>
</tbody>
</table>

**Table B-3**  
Modify URLs, Route, and No action combinations (continued)

**Note:** Actions from end-user Good and Bad Senders groups override all actions except content filtering policy actions.

**Verdicts by verdict category**

The following table describes the verdicts by verdict category. The verdict categories correspond to the menus in the Control Center where you can create or edit policies for each verdict. You set up the detection conditions for each verdict when you create or edit policies from these menus. Within each policy, you also select the actions that you want SMG to take when a message meets the policy conditions and triggers a verdict.
<table>
<thead>
<tr>
<th>Verdict Category</th>
<th>Verdict</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation</td>
<td>Directory harvest attack</td>
<td>An attempt is underway to capture valid email addresses. SMG detects a directory harvest attack when the same IP address sends the specified percentage of emails to your domain from non-existent recipients.</td>
</tr>
<tr>
<td>Reputation</td>
<td>Email virus attack</td>
<td>The same IP address sends specified percentage of infected email messages to your domain.</td>
</tr>
<tr>
<td>Reputation</td>
<td>Bad Sender Groups</td>
<td>An email message, domain, or IP address is a member of one of the following groups:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Local Bad Sender Domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Local Bad Sender IPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Third Party Bad Senders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Symantec Global Bad Senders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About blocking and allowing messages using sender groups” on page 151.</td>
</tr>
<tr>
<td>Reputation</td>
<td>Good Sender Groups</td>
<td>An email message, domain, or IP address is a member of one of the following groups:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Local Good Sender Domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Local Good Sender IPs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Third Party Good Senders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Symantec Global Good Senders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About blocking and allowing messages using sender groups” on page 151.</td>
</tr>
<tr>
<td>Reputation</td>
<td>Fastpass</td>
<td>Allows most of the email messages from verified Good Senders to bypass spam filtering. You cannot specify any actions for the Fastpass verdict.</td>
</tr>
<tr>
<td>Malware</td>
<td>Virus</td>
<td>An email contains a virus, based on current Symantec virus filters.</td>
</tr>
<tr>
<td>Malware</td>
<td>Mass-mailing worm</td>
<td>An email contains a mass-mailing worm, based on current Symantec virus filters.</td>
</tr>
<tr>
<td>Malware</td>
<td>Unscannable for malware or content filtering for any reason</td>
<td>An email cannot be scanned for any of the four reasons that correspond to granular verdicts. These reasons are: attachment limits exceeded, or other. “Other” includes any reasons that do not apply to the attachment limits exceeded verdict.</td>
</tr>
<tr>
<td>Malware</td>
<td>Unscannable for malware or content filtering due to limits exceeded</td>
<td>A message’s attachment exceeds the container limits that you set. You set container limits on the Protocols &gt; SMTP &gt; Settings &gt; Content Scanning tab.</td>
</tr>
<tr>
<td>Verdict Category</td>
<td>Verdict</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malware</td>
<td>Unscannable for malware or content filtering for other reasons</td>
<td>A message or attachment is unscannable for reasons other than the ones for the other unscannable verdicts. For example, a message can contain attachments that are split among multiple instances of an otherwise supported attachment type.</td>
</tr>
<tr>
<td>Malware</td>
<td>Unscannable for Disarm</td>
<td>An email contains an attachment that is unscannable for Disarm. For example, an attachment cannot be Disarmed if it is encrypted.</td>
</tr>
<tr>
<td>Malware</td>
<td>Encrypted attachment</td>
<td>An email contains an attachment that is encrypted or password-protected, and therefore, cannot be scanned.</td>
</tr>
<tr>
<td>Malware</td>
<td>Spyware or adware</td>
<td>An email contains any of the following types of security risks: spyware, adware, hacking tools, dialers, joke programs, or remote access programs. See “Spyware or adware verdict details” on page 214.</td>
</tr>
<tr>
<td>Malware</td>
<td>Suspicious attachment</td>
<td>An email either shows virus-like signs or because suspicious new patterns of message flow involving this attachment have been detected.</td>
</tr>
<tr>
<td>Malware</td>
<td>Disarm</td>
<td>An email contains an attachment in which potentially malicious content has been detected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About Disarm” on page 207.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Spam</td>
<td>An email message is spam, based on current spam filters from Symantec.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Suspected spam</td>
<td>An email message is suspected spam, based on a suspected spam threshold that you can adjust on the Spam &gt; Settings &gt; Scan Settings page.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Failed bounce attack validation</td>
<td>An email message is part of a bounce attack based on bounce attack validation filtering.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About defending against bounce attacks” on page 160.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Marketing mail</td>
<td>An email message is a marketing email based on the unwanted email filters from Symantec.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Newsletter</td>
<td>An email message is a newsletter based on the unwanted email filters from Symantec.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Redirect URL</td>
<td>An email message contains one or more redirect URLs based on the unwanted email filters from Symantec.</td>
</tr>
<tr>
<td>Spam and Unwanted email</td>
<td>Customer-specific spam</td>
<td>An email message is spam based on the rules that are created from customer-specific spam submissions. You can enable customer-specific spam submission from the Spam &gt; Settings &gt; Submission Settings &gt; Customer-specific Spam submissions page.</td>
</tr>
</tbody>
</table>
### Table B-4 Verdicts by verdict category (continued)

<table>
<thead>
<tr>
<th>Verdict Category</th>
<th>Verdict</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam and Unwanted email</td>
<td>Sender authentication</td>
<td>An email message failed either SPF or Sender ID authentication. See “How sender authentication works” on page 112.</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>Contains advanced threats</td>
<td>An email message contains advanced malware based on threat defense detection by Symantec Content Analysis.</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>Does not contain advanced threats</td>
<td>An email message does not contain advanced malware based on threat defense detection by Symantec Content Analysis.</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>Unscannable for advanced threats</td>
<td>Symantec Content Analysis cannot scan the email message.</td>
</tr>
<tr>
<td>Threat Defense</td>
<td>Inspection time exceeds &lt;x&gt; seconds</td>
<td>Threat defense scanning did not evaluate an email message within the specified Scan timeout limit.</td>
</tr>
<tr>
<td>Content</td>
<td>Text in the subject, body, or attachments</td>
<td>An email message:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Contains or does not contain keywords in your configurable dictionary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Matches or does not match a regular expression</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Matches or does not match a pattern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Matches data in a record</td>
</tr>
<tr>
<td>Content</td>
<td>Text in this specific part of the message</td>
<td>In any of the specified message parts, an email message:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Contains or does not contain specific text</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Starts with or ends with, does not start or does not end with, matches exactly or does not match specific text</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Matches the regular expression or does not match the regular expression you specify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Matches the pattern or does not match the pattern that you specify</td>
</tr>
<tr>
<td>Content</td>
<td>Text in this specific part of the message</td>
<td>Text in the envelope recipient or envelope sender contains or does not contain an email address, domain, or country code from a specific dictionary.</td>
</tr>
<tr>
<td>Content</td>
<td>Contains the message part/Does not contain the message part</td>
<td>The message does or does not contain the message part that you specify.</td>
</tr>
</tbody>
</table>
Table B-4  Verdicts by verdict category (continued)

<table>
<thead>
<tr>
<th>Verdict Category</th>
<th>Verdict</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Message size/Attachment size</td>
<td>The message size or attachment size is equal to/greater than/less than a specific number of bytes, KB, or MB.</td>
</tr>
</tbody>
</table>
| Content          | Attachment or body part | An attachment is or is not in an attachment list, has a specific file name or MIME type, or has a specific file name or MIME type which is not from a specific dictionary.  
**Note:** SMG evaluates attachments and any objects that are embedded in message bodies for true file type, true file class, file name, file extension, and MIME. For the condition **Is not in attachment list**, SMG evaluates attachments and the objects that are embedded in message bodies for true file type and true file class.  
SMG does not test for the file name, the extension, or the MIME type because senders can easily forge them. Therefore, these items are not secure conditions to use in a policy. |
| Content          | For all messages | You can create a content filtering rule that applies to all messages. For example, you can create a policy that attaches an annotation to all inbound email messages or outbound email messages.  
All email is flagged. |

See “Positive and negative content filtering rule condition examples” on page 842.

**Verdict combinations**

In general, messages from senders in Good Sender groups bypass spam filtering but do not bypass virus filtering or content filtering. This section provides a more detailed explanation of how this process works.

Messages arriving at the gateway first undergo connection-time processing.

Messages from certain domains or IP addresses can be deferred, rejected, or accepted, based on the following:

- Locally (within your system) collected reputation information
- Globally collected reputation information
- Local Good Sender Groups and Bad Sender Groups
- Global Good Sender Groups and Bad Sender Groups

These actions occur before the Brightmail Engine processes the messages.
See “How Symantec Messaging Gateway works” on page 27.

Table B-5 shows the steps that can be skipped during connection processing.

### Table B-5  
Connection-time good sender processing

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>SMG does not check for any of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Good Sender IPs</td>
<td>Third Party Bad Senders</td>
</tr>
<tr>
<td>Third Party Good Senders</td>
<td></td>
</tr>
<tr>
<td>Symantec Global Good Senders</td>
<td></td>
</tr>
<tr>
<td>Local Good Sender IPs</td>
<td>Symantec Global Bad Senders</td>
</tr>
<tr>
<td>Symantec Global Good Senders</td>
<td></td>
</tr>
<tr>
<td>Local Good Sender IPs</td>
<td>Local Bad Sender IPs</td>
</tr>
</tbody>
</table>

See “About blocking and allowing messages using sender groups” on page 151.

See “Verdicts by verdict category” on page 836.

Table B-6 describes the steps that the Brightmail Engine message processing may skip.

### Table B-6  
Brightmail Engine inbound message processing

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>SMG does not check for any of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Good Sender Domains</td>
<td>Spam</td>
</tr>
<tr>
<td>Local Good Sender IPs</td>
<td>Suspected spam</td>
</tr>
<tr>
<td>Content filtering policy with a Bypass spam scanning action</td>
<td>Newsletter</td>
</tr>
<tr>
<td>Content filtering policy with a Treat as good sender action</td>
<td>Marketing email</td>
</tr>
<tr>
<td>Symantec Global Good Senders</td>
<td>Redirect URL</td>
</tr>
<tr>
<td>End user Good Senders List</td>
<td>Sender authentication failure</td>
</tr>
<tr>
<td>Third Party Good Senders</td>
<td></td>
</tr>
<tr>
<td>Content filtering policy with a Treat as a good sender action</td>
<td>Local Bad Sender Domains</td>
</tr>
<tr>
<td>Local Good Sender Domains</td>
<td></td>
</tr>
<tr>
<td>Local Good Sender Domains</td>
<td></td>
</tr>
</tbody>
</table>
Table B-6  Brightmail Engine inbound message processing (continued)

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>SMG does not check for any of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Suspected spam</td>
</tr>
<tr>
<td></td>
<td>Newsletter</td>
</tr>
<tr>
<td></td>
<td>Marketing email</td>
</tr>
<tr>
<td></td>
<td>Redirect URL</td>
</tr>
</tbody>
</table>

When the associated policy specifies a Bypass content filtering policy action:

- Local Good Sender Domains
- Local Good Sender IPs
- Third Party Good Senders
- Local Bad Sender Domains
- Local Bad Sender IPs
- Third Party Bad Senders
- Symantec Global Good Senders
- Symantec Global Bad Senders
- Spam
- Suspected spam
- Unwanted email
- Sender authentication failure

All content filtering policies or those content filtering policies specified in the policy

Positive and negative content filtering rule condition examples

You can create more effective policies when you understand how positive rule conditions and negative rule conditions are evaluated.

Positive rules are rules in which a condition must be present to trigger a verdict. An example of a positive rule is: **If any part of the message contains 2 or more words from dictionary "Financial Keywords."** If the message contains two or more words from the Financial Keywords dictionary, a verdict is triggered.

Negative rules are rules in which a condition must not be present to trigger a verdict. An example of a negative rule is: **does not contain Subject.**

Table B-7 lists conditions that have positive and negative rules, and gives examples of when messages trigger verdicts and when they do not.
<table>
<thead>
<tr>
<th>Condition</th>
<th>Example 1: The message has no attachments. Only content within the body matches the condition. No other parts of the message match the conditions.</th>
<th>Example 2: The message has one attachment. No other parts of the message match the conditions.</th>
<th>Example 3: The message has multiple attachments. Only one attachment matches the conditions. No other parts of the message match the conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text in the subject, body or attachments: Contains n or more words from dictionary</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Text in the subject, body or attachments: Does not contain n or more words from dictionary</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Text in the subject, body or attachments: Matches regular expression</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Text in the subject, body or attachments: Does not match regular expression</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Text in the subject, body or attachments: Matches pattern</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Text in the subject, body or attachments: Does not match pattern</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Attachment or body part: Is in the attachment list</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Condition</td>
<td>Example 1: The message has no attachments. Only content within the body matches the condition. No other parts of the message match the conditions.</td>
<td>Example 2: The message has one attachment. No other parts of the message match the conditions.</td>
<td>Example 3: The message has multiple attachments. Only one attachment matches the conditions. No other parts of the message match the conditions.</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attachment or body part: Is not in the attachment list</td>
<td>Triggers a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Attachment or body part: Has a file name which contains</td>
<td>Triggers a verdict if the message has an embedded file with a matching name If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Attachment or body part: Has a file name which does not contain</td>
<td>Triggers a verdict if the message has an embedded file with a matching name If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Attachment or body part: Has a MIME type which is</td>
<td>Triggers a verdict if the message has an embedded file with a matching name If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Attachment or body part: Has a MIME type which is not</td>
<td>Triggers a verdict if the message has an embedded file with a matching name If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Attachment or body part: Has a file name from dictionary</td>
<td>Triggers a verdict if the message has an embedded file with a matching name If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
</tbody>
</table>
**Table B-7**  
Positive and negative rule match verbs and examples *(continued)*

<table>
<thead>
<tr>
<th>Condition</th>
<th>Example 1: The message has no attachments. Only content within the body matches the condition. No other parts of the message match the conditions.</th>
<th>Example 2: The message has one attachment. No other parts of the message match the conditions.</th>
<th>Example 3: The message has multiple attachments. Only one attachment matches the conditions. No other parts of the message match the conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment or body part:</td>
<td>Triggers a verdict if the message has an embedded file with a matching name. If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Has a file name not from dictionary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment or body part:</td>
<td>Triggers a verdict if the message has an embedded file with a matching name. If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Has a file extension from dictionary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment or body part:</td>
<td>Triggers a verdict if the message has an embedded file with a matching name. If not, does not trigger a verdict</td>
<td>Does not trigger a verdict</td>
<td>Triggers a verdict</td>
</tr>
<tr>
<td>Has a file extension not from dictionary</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** For the condition **Attachment or body part: Is in attachment list**, SMG evaluates attachments and any objects that are embedded in message bodies for true file type, true file class, file name, file extension, and MIME.

For the condition **Attachment or body part: Is not in attachment list**, SMG evaluates attachments and the objects that are embedded in message bodies for true file type and true file class. SMG does not test for file name, extension, or MIME type for this condition.
This appendix includes the following topics:

- Caldicott Report policy template
- Canadian Social Insurance Number policy template
- Competitor Communications policy template
- Confidential Documents policy template
- Credit Card Numbers policy template
- Customer Data Protection policy template
- Data Protection Act 1998 policy template
- Defense Message System (DMS) GENSER Classification policy template
- Design Documents policy template
- Employee Data Protection policy template
- Encrypted Data policy template
- EU Data Protection Directives policy template
- Export Administration Regulations (EAR) policy template
- Financial Information policy template
- Gambling policy template
- Gramm-Leach-Bliley policy template
- HIPAA policy template
- Human Rights Act 1998 policy template
- Illegal Drugs policy template
- Individual Taxpayer Identification Numbers (ITIN) policy template
- International Traffic in Arms Regulations (ITAR) policy template
- Media Files policy template
- Mergers and Acquisition Data policy template
- NASD Rule 2711 and NYSE Rules 351 and 472 policy template
- NASD Rule 3010 and NYSE Rule 342 policy template
- NERC Security Guidelines for Electric Utilities policy template
- Network Diagrams policy template
- Network Security policy template
- Offensive Language policy template
- Office of Foreign Assets Control (OFAC) policy template
- Password Files policy template
- Payment Card Industry Data Security Standard policy template
- PIPEDA policy template
- Price Information policy template
- Project Data policy template
- Publishing Documents policy template
- Racist Language policy template
- Restricted Files policy template
- Restricted Recipients policy template
- Resumes policy template
- Sarbanes-Oxley policy template
- SEC Fair Disclosure Regulation policy template
- Sexually Explicit Language policy template
- Source Code policy template
- State Data Privacy policy template
The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- **UK National Insurance Number and Drug Keywords** - Looks for a keyword from UK NIN Keywords dictionary in combination with a pattern matching the UK NIN regular expression and a keyword from the Prescription Drug Names dictionary.
- **UK National Insurance Number and Disease Keywords** - Looks for a keyword from UK NIN Keywords dictionary in combination with a pattern matching the UK NIN regular expression and a keyword from the Disease Names dictionary.
- **UK National Insurance Number and Treatment Keywords** - Looks for a keyword from UK NIN Keywords dictionary in combination with a pattern matching the UK NIN regular expression and a keyword from the Medical Treatment Keywords dictionary.

The Structured Data conditions are as follows:

- **Patient Data and Drug Keywords** – Looks for any match to the following data in a Record Resource view: NIN (National Insurance Number), account number, last name, ID card number, email, phone, and UK NHS (National Health Service) number. This data must appear in combination with a keyword from the Prescription Drug Names dictionary.
- **Patient Data and Disease Keywords** – Looks for any match to the following data in a Record resource View: NIN (National Insurance Number), account number, last name, ID card number, email, phone, and UK NHS (National Health Service) number. This data must appear in combination with a keyword from the Disease Names dictionary.
- **Patient Data and Treatment Keywords** – Looks for any match to the following data in a Record resource View: NIN (National Insurance Number), account number, last name, ID card number, email, phone, and UK NHS (National Health Service) number. This data must appear in combination with a keyword from the Medical Treatment Keywords dictionary.
The included dictionaries are as follows:

- Prescription Drug Names
- Disease Names
- Medical Treatment Keywords
- UK NIN Keywords

**Canadian Social Insurance Number policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Canadian Social Insurance Numbers. This condition looks for a match to the Canadian Social Insurance Number regular expression and a keyword from the Canadian Social Ins. No. Words dictionary.

The included dictionary is Canadian Social Ins. No. Words.

**Competitor Communications policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Competitor List. This condition looks for keywords (domains) from the Competitor Domains dictionary, which is user-defined.

The included dictionary is Competitor Domains.

**Confidential Documents policy template**

The following describes the conditions and dictionaries that this policy template uses.
The Described Content conditions are as follows:

- **Confidential Documents** - A compound condition that looks for a combination of keywords from the Confidential Keywords dictionary and the following file types: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, pdf, and ppt.

- **Proprietary Documents** - A compound condition that looks for a combination of keywords from the Proprietary Keywords dictionary and the following file types: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, pdf, and ppt.

- **Internal Use Only Documents** - A compound condition that looks for a combination of keywords from the Internal Use Only Keywords dictionary and the following file types: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, pdf, and ppt.

- **Documents Not For Distribution** - A compound condition that looks for a combination of keywords from the Not For Distribution Words dictionary and the following file types: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, pdf, and ppt.

The included dictionaries are as follows:

- Confidential Keywords
- Proprietary Keywords
- Internal Use Only Keywords
- Not For Distribution Words

---

**Credit Card Numbers policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Credit Card Numbers, All. This condition looks for a match to the credit card number system pattern and a keyword from the Credit Card Number Keywords dictionary.

The included dictionary is Credit Card Number Keywords.

---

**Customer Data Protection policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- **US Social Security Number Patterns** - Looks for a match to the Social Security number regular expression and a keyword from the US SSN Keywords dictionary.

- **Credit Card Numbers, All** - Looks for a match to the credit card number system pattern and a keyword from the Credit Card Number Keywords dictionary.

- **ABA Routing Numbers** - Looks for a match to the ABA Routing number regular expression and a keyword from the ABA Routing Number Keywords dictionary.
The Structured Data conditions are as follows:

- Username/Password Combinations – Looks for user names and passwords in combination in Record resource View.
- 3 or more customer data fields – Looks for combination of data from any 3 of the following fields in Record resource View: SSN, Phone, Email, First Name, Last Name, Bank Card number, Account Number, ABA Routing Number, Canadian Social Insurance Number, and UK National Insurance Number, Date of Birth. Exceptions: combination of phone, email, and first or last names; email or phone and first and last names.
- Exact SSN or CCN – Looks for SSN or Bank Card Number in Record resource View.
- Customer Directory – Looks for Phone or Email in Record resource view

The included dictionaries are as follows:

- US SSN Keywords
- Credit Card Number Keywords
- ABA Routing Number Keywords

**Data Protection Act 1998 policy template**

The following describes the conditions and dictionaries that this policy template uses.
Described Content conditions: The Described Content conditions are as follows:

- **UK Electoral Roll Numbers** - Looks for a single compound condition with three parts: a single keyword from the UK Keywords dictionary, the pattern matching that of the UK Electoral Roll Number regular expression, and single keyword from the UK Electoral Roll Number Words dictionary.
- **UK National Insurance Numbers** - Looks for a match to the UK National Insurance number regular expression and a keyword from the UK NIN Keywords dictionary.
- **UK Tax ID Numbers** - Looks for a match to the UK Tax ID number regular expression and a keyword from the UK Tax ID Number Keywords dictionary.
- **UK Drivers License Number** - Looks for a single compound condition with three parts: a single keyword from the UK Keywords dictionary, a pattern matching that of the UK driver’s license regular expression, and different combinations of the phrase driver’s license using a regular expression.
- **UK Passport Numbers (Old Type)** - Looks for a keyword from the UK Passport Keywords dictionary and a pattern matching the regular expression for UK Passport Numbers (Old Type).
- **UK Passport Numbers (New Type)** - Looks for a keyword from the UK Passport Keywords dictionary and a pattern matching the regular expression for UK Passport Numbers (New Type).

Structured Data conditions: **UK Data Protection Act, Personal Data** – Looks for three of the following columns of data in a Record resource View: NIN (National Insurance Number), account number, pin, bank card number, first name, last name, drivers license, password, tax payer ID, UK NHS number, date of birth, mother’s maiden name, email address, and phone number. Combinations of first and last names with pin, password, email, phone, or mother’s maiden name are excepted.

Included dictionary: The included dictionaries are as follows:

- **UK Keywords**
- **UK Electoral Roll Number Words**
- **UK NIN Keywords**
- **UK Tax ID Number Keywords**
- **UK Passport Keywords**

Defense Message System (DMS) GENESER Classification policy template

The following describes the conditions and dictionaries that this policy template uses.
Looks for any keywords in the Secret, Top Secret, Classified or Restricted, or Other Sensitive Information dictionaries. Keywords and phrases other than those indicated in the titles of the Secret, Top Secret, and Classified or Restricted dictionaries are user-defined. The Other Sensitive Information dictionary includes phrases used to categorize sensitive but unclassified information.

The included dictionaries are as follows:
- Secret
- Top Secret
- Classified or Restricted
- Other Sensitive Information

**Design Documents policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:
- Design Document Extensions - Looks for specified file name extensions are found in the Design Document Extensions dictionary.
- Design Documents - Looks for specified file types: cad‚draw and dwg.

**Employee Data Protection policy template**

The Described Content conditions are as follows:
- US Social Security Number Patterns - Looks for a match to the Social Security number regular expression and a keyword from the US SSN Keywords dictionary.
- Credit Card Numbers, All - Looks for a match to the credit card number system pattern and a keyword from the Credit Card Number Keywords dictionary.
- ABA Routing Numbers - Looks for a match to the ABA Routing number regular expression and a keyword from the ABA Routing Number Keywords dictionary.
The Structured Data conditions are as follows:

- Username/Password Combinations – Looks for user names and passwords in combination in Record resource View.
- 3 or more employee data fields – Looks for combination of data from any 3 of the following fields in Record resource View: SSN, Phone, Email, First Name, Last Name, Bank Card Number, Account Number, ABA Routing Number, Canadian Social Insurance Number, and UK National Insurance Number, employee number, medical insurance number, salary, direct deposit account, and Date of Birth.
- Employee Directory: Looks for Phone or Email in Record resource view

The included dictionaries are as follows:

- US SSN Keywords
- Credit Card Number Keywords
- ABA Routing Number Keywords

### Encrypted Data policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- Password Protected Files - Looks for the following file type extensions in the Password Protected Files attachment list resource: encrypted_zip, encrypted_doc, encrypted_xls, or encrypted_ppt.
- PGP Files - Looks for the following file type: pgp
- GPG Files - Looks for a keyword from the GPG Encryption Keywords dictionary.
- S/MIME - Looks for a match with the S/MIME regular expression.
- PGP8 Header Keywords – Looks for characteristic keywords in PGP8 files headers.
- PGP8 Keywords – Looks for characteristic strings in PGP8 encrypted files.
- PGP Encrypted Documents – Looks for .pgp and .aex.message or file-attachment extensions in the PGP file extension dictionary.

The included dictionaries are as follows:

- GPG Encryption Keywords
- PGP file extensions
- PGP8 Keywords

### EU Data Protection Directives policy template

The Structured Content conditions are as follows:

- EU Data Protection Directives
Searches EU Country Codes dictionary for country codes that do not match recipient part of the message header and looks for any two of the following data columns in a record resource view: last name, bank card number, driver's license, account number, pin, medical account number, and ID card number, username, password, ABA routing number, email, phone, and mother's maiden name. Combinations of last name with email, phone, account number, and username data are excepted.

- EU Data Protection, Contact Info
  Searches EU Country Codes dictionary for country codes that do not match recipient part of the message header and looks for any two of the following data columns: last name, phone, account number, username, and email.

**Export Administration Regulations (EAR) policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is EAR Commerce Control List and Recipients. This condition is a compound rule that looks for both a country code in the recipient from the EAR Country Codes dictionary and a keyword from the EAR CCL Keywords dictionary.

The Structured Data condition is Indexed EAR Commerce Control List Items and Recipients. This compound condition looks for both a country code in the recipient from the "EAR Country Codes" dictionary and for a specific "SKU" from a Record resource View.

The included dictionaries are as follows:

- EAR Country Codes
- EAR CCL Keywords

**Financial Information policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is as follows:

Financial Information - Looks for the combination of specified file types, keywords from the Financial Keywords dictionary, and keywords from the Confidential/Proprietary Words dictionary. The specified file types are: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, and 123.

The included dictionaries are as follows:

- Financial Keywords
- Confidential/Proprietary Words
Gambling policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- Suspicious Gambling Keywords - Looks for five instances of keywords from the Gambling Keywords, Confirmed dictionary.
- Less Suspicious Gambling Keywords - Looks for ten instances of keywords from the Gambling Keywords, Suspect dictionary.

The included dictionaries are as follows:

- Gambling Keywords, Confirmed
- Gambling Keywords, Suspect

Gramm-Leach-Bliley policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- US Social Security Numbers – Looks for social security numbers. For this rule to match, there must be both a number that fits the Valid Social Security Number premium pattern, and a keyword or phrase that indicates the presence of a US SSN with a keyword from the US SSN Keywords dictionary. The keyword condition is included to reduce false positives with numbers that may match the SSN format.
- ABA Routing Numbers – Looks for a match to the ABA Routing number regex rule and a keyword from the dictionary "ABA Routing Number Keywords.
- Credit Card Numbers, All - Looks for credit card numbers. Similar to the first rule, this rule requires that there be both a number that fits a credit card system pattern ccn and a keyword or phrase that indicates the presence of a credit card number from the Credit Card Number Keywords dictionary. The keyword condition is included to reduce false positives with numbers that may match the credit card format.

The Structured Data conditions are as follows:

- Username/Password Combinations – Looks for user names and passwords in combination from a Record resource View.
- 3 or more critical customer fields – Looks for any three fields that can identify a customer uniquely from a Record resource View, except for combinations of phone, email, and first or last name.
- Exact SSN or CCN – Looks for SSN or Bank Card Number from a Record resource View.
- Customer Directory – Looks for Phone or Email from a Record resource View.
The included dictionaries are as follows:

- US SSN Keywords
- Credit Card Number Keywords
- ABA Routing Number Keywords

**HIPAA policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- **SSN and Drug Keywords** – Looks for the Social Security number (SSN) with the Valid Social Security Number premium pattern, in combination with a keyword from US SSN Keywords dictionary and a keyword from the Prescription Drug Names dictionary.
- **SSN and Treatment Keywords** – Looks for the Social Security number (SSN) with the Valid Social Security Number premium pattern, in combination with a keyword from US SSN Keywords dictionary and a keyword from the Medical Treatment Keywords dictionary.
- **SSN and Disease Keywords** – Looks for the Social Security number (SSN) with the Valid Social Security Number premium pattern, in combination with a keyword from US SSN Keywords dictionary and a keyword from the Disease Names dictionary.
- **SSN and Drug Codes** – Looks for the Social Security number (SSN) with the Valid Social Security Number premium pattern, in combination with a keyword from US SSN Keywords dictionary and a drug code using the Drug Code regular expression.

The Structured Data conditions are as follows:

- **Patient Data and Drug Codes** – Any part of the message matches the NDC Drug Code regular expression and any part of the message matches text in a Record resource View.
- **Patient Data and Drug Keywords** – Any part of the message matches a Prescription Drug Names dictionary entry and any part of the message matches an entry in a Record resource View.
- **Patient Data and Treatment Keywords** – Any part of the message matches an entry in the Medical Treatment Keywords dictionary and any part of the message matches text in a Record resource View.
- **Patient Data and Disease Keywords** – Any part of the message matches an entry in the Disease Names dictionary and any part of the message matches text in a Record resource View.

Exception conditions:

- **TPO Exception** – Looks for a recipient email address matching one from the TPO Email Addresses dictionary. If a match is found, the policy is not triggered even if the other conditions are met.

**Note**: TPOs (Treatment, Payment, or health care Operations)—companies that partner with the health care organization—have a specific carve-out for the HIPAA information restrictions. This exception in the rules does not trigger the policy if the protected information is sent to one of these allowed companies. The template requires that the customer enter the allowed email addresses of these companies.
The included dictionaries are as follows:

- US SSN Keywords
- Prescription Drug Names
- Medical Treatment Keywords
- Disease Names
- TPO Email Addresses

### Human Rights Act 1998 policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is UK Electoral Roll Numbers. This condition looks for a single compound condition with four parts: a single keyword from the UK Keywords dictionary, the pattern matching that of the UK Electoral Roll Number regular expression, a single keyword from the UK Electoral Roll Number Words dictionary, and a single keyword from the UK Personal Data Keywords dictionary.

The Structured Data condition is UK Data Protection Act, Personal Data. This condition is a compound rule that looks for last name and electoral roll number in a Record resource View in combination with a keyword from the UK Personal Data Keywords dictionary.

The included dictionaries are as follows:

- UK Personal Data Keywords
- UK Keywords
- UK Electoral Roll Number Words

### Illegal Drugs policy template

The Described Content conditions are as follows:

- Street Drugs - Looks for five instances of keywords from the Street Drug Names dictionary.
- Mass Produced Controlled Substances - Looks for five instances of keywords from the Manufd. Controlled Substances dictionary.

The included dictionaries are as follows:

- Street Drug Names
- Manufd. Controlled Substances
Individual Taxpayer Identification Numbers (ITIN) policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is US ITI. This condition looks for a match to the US ITIN regular expression and a keyword from the US ITIN Keywords dictionary.

The included dictionary is US ITIN Keywords.

International Traffic in Arms Regulations (ITAR) policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is ITAR Munitions List and Recipients. This compound rule looks for both a recipient country code from the ITAR Country Codes dictionary and a keyword from the ITAR Munition Names dictionary.

The Structured Data condition is Indexed ITAR Munition Items and Recipients. This compound rule looks for a recipient country code from the ITAR Country Codes dictionary and for a specific Stock Keeping Unit (SKU) number from a Record resource View.

The included dictionaries are as follows:
- ITAR Country Codes
- ITAR Munition Names

Media Files policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:
- Media Files - Looks for the following files types: qt, riff, macromedia_dir, midi, mp3, mpeg_movie, quickdraw, realaudio, wav, video_win, and vrml.
- Media Files Extensions - Looks for file name extensions from the Media Files Extensions dictionary.

The included dictionary is Media Files Extensions.
Mergers and Acquisition Data policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is M & A Activity. This condition looks for any keywords from the M & A Project Code Names dictionary, which is user-defined. Merger and acquisition activity is extremely customer- and project-specific. There are no general terms across all customers and users that suffice.

The included dictionary is M & A Project Code Names

NASD Rule 2711 and NYSE Rules 351 and 472 policy template

The following describes the conditions and dictionaries that this policy template uses.

Described Content condition

The Described Content condition is NASD Rule 2711 and NYSE Rules 351 and 472. This compound rule contains a sender condition and a keyword condition. The sender condition requires editing by the user and is a list of email addresses of research analysts at the user’s company (Analysts' Email Addresses dictionary). The keyword condition works for any upcoming stock offering, internal project names for the offering, and the stock ticker symbols for the offering companies (NASD 2711 Keywords dictionary). Like the sender condition, it requires editing by the user.

Included dictionaries

The included dictionaries are as follows:

- Analysts' Email Addresses
- NASD 2711 Keywords

NASD Rule 3010 and NYSE Rule 342 policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- Stock Recommendation - Compound rule that looks for both a keyword in the NASD 3010 Stock Keywords dictionary and the NASD 3010 Buy/Sell Keywords keyword dictionary. This rule requires that there is evidence of both a stock recommendation of some sort in combination with a recommendation for a specific buy or sell action.
- NASD Rule 3010 and NYSE Rule 342 Keywords - Looks for keywords in the NASD 3010 General Keywords dictionary. These keywords look for any general stock broker activity.
The included dictionaries are as follows:

- NASD 3010 Stock Keywords
- NASD 3010 Buy/Sell Keywords
- NASD 3010 General Keywords

**NERC Security Guidelines for Electric Utilities policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is a compound rule that looks for any keyword matches from the Sensitive Keywords dictionary and the Vulnerability Keywords dictionary.

The included dictionaries are as follows:

- Sensitive Keywords
- Vulnerability Keywords

**Network Diagrams policy template**

The Described Content conditions are as follows:

- Network Diagrams with IP Addresses - Looks for a Visio file type in combination with an IP address regular expression.
- Network Diagrams with IP Address Keyword - Looks for a Visio file type in combination with phrase variations of IP address with a regular expression.

**Network Security policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- GoToMyPC Activity - Looks for a GoToMyPC command format with a regular expression.
- Hacker Keywords - Looks for a keyword from the Hacker Keywords dictionary.
- KeyLoggers - Looks for a keyword from the Keylogger Keywords dictionary.

The included dictionaries are as follows:

- Hacker Keywords
- Keylogger Keywords
Offensive Language policy template

The Described Content conditions are as follows:


The included dictionaries are as follows:

- Offensive Language, Explicit
- Offensive Language, General

Office of Foreign Assets Control (OFAC) policy template

The following describes the conditions and dictionaries that this policy template uses.

There are two primary conditions in the OFAC policy template. The first deals with the Specially Designated Nationals (SDN) list, and the second deals with general OFAC policy restrictions.

The Described Content conditions are as follows:

- OFAC Special Designated Nationals List and Recipients - Looks for a recipient with a country code matching entries from the OFAC SDN Country Codes dictionary in combination with a match of a keyword from the SDN List dictionary.
  
  The SDN list refers to specific people or organizations that are subject to trade restrictions. The U.S. Treasury Department provides text files with specific names, last known addresses, and known aliases for these individuals and entities. However, the Treasury Department stipulates that the addresses may not be correct or current, and different locations do not change the restrictions against these people and organizations.

- Communications to OFAC countries - Looks for a recipient with a country code matching entries from the OFAC Country Codes dictionary.
  
  This condition provides guidance around the restrictions the U.S. Treasury Department has placed on general trade with specific countries. This is distinct from the SDN list, since individuals and organizations are not specified. The template looks for recipients that have the listed countries as the designated country code.

The included dictionaries are as follows:

- SDN List
- OFAC SDN Country Codes
- OFAC Country Codes
Password Files policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:
- Password Filenames - Looks for the file names passwd or shadow.
- /etc/passwd Format - Looks for a pattern with /etc/passwd format regular expression.
- /etc/shadow Format - Looks for a pattern with /etc/shadow format regular expression.
- SAM Passwords - Looks for a pattern with SAM format regular expression.

The included dictionary is Password Filenames.

Payment Card Industry Data Security Standard policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Credit Card Numbers, All. This condition looks for a match to the Valid Credit Card pattern and a keyword from the Credit Card Number Keywords dictionary.

The Structured Data condition searches record resource view for a match.

The included dictionary is Credit Card Number Keywords.

PIPEDA policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:
- Canadian Social Insurance Numbers - Looks for a match to the Canadian Social Insurance Number regular expression and a keyword from the dictionary Canadian Social Ins. No. Words.
- ABA Routing Numbers - Looks for a word from the ABA Routing Number Keywords dictionary and a match from the ABA Routing Number regular expression.
- Credit Card Numbers, All - Looks for a word from Credit Card Number Keywords dictionary and a match from the credit card number system pattern.

UK Electoral Roll Numbers - Looks for a single compound condition with four parts: a single keyword from the UK Keywords dictionary, the pattern matching that of the UK Electoral Roll Number regular expression, a single keyword from the UK Electoral Roll Number Words dictionary, and a single keyword from the UK Personal Data Keywords dictionary.
The Structured Data conditions are as follows:

- PIPEDA – Looks in a Record resource View for any two of the following data columns: last name, bank card, medical account number, medical record, agency number, account number, PIN, username, password, SIN, ABA routing number, email, phone, mother's maiden name. Combinations of last names with email, phone, account number, or username are excepted.
- PIPEDA, Contact Info – Looks for in Record resource View any two of the following data columns: last name, phone, account number, username, email

The included dictionaries are as follows:

- Canadian Social Ins. No. Words
- ABA Routing Number Keywords
- Credit Card Number Keywords

Price Information policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition looks for the combination of user-specified Stock Keeping Unit (SKU) numbers and the price for that SKU number in a Record resource View.

Project Data policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Project Activity. This condition looks for any keywords in the Sensitive Project Code Names dictionary, which is user-defined.

The included dictionary is Sensitive Project Code Names

Publishing Documents policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- Publishing Documents - Looks for the specified file types: qxpress, frame, aldus_pagemaker, and publ (Microsoft Publisher).

The included dictionary is Publishing Document Extensions
Racist Language policy template

The Described Content condition is Racist Language. This condition looks for any single keyword in the Racist Language dictionary.

The included dictionary is Racist Language.

Restricted Files policy template

The Described Content condition is MSAccess Files and Executables. This condition looks for files of the specified types: access, exe, and exe_unix.

Restricted Recipients policy template

The Described Content condition is Restricted Recipients. This condition looks for messages to recipients with email addresses in the Restricted Recipients dictionary.

The included dictionary is Restricted Recipients.

Resumes policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Resumes, All. This condition looks for files of a specified type (.doc) that are less than 50 kB and match at least one keyword from each of the following dictionaries: Job Search Keywords, Education, Job Search Keywords, Work, and Job Search Keywords, General.

The Structured Data condition is Resumes, Employee. This condition matches files that are less than 50 KB of a specified type (for example, .doc) in the Resumes, Employee attachment list resource and that fulfill the following conditions: (1) matches at least one keyword from each of the following dictionaries: Job Search Keywords, Education; Job Search Keywords, Work; and Job Search Keywords, General; and (2) matches first and last names of employees in Record resource View.

The included dictionaries are as follows:

- Job Search Keywords, Education
- Job Search Keywords, Work
- Job Search Keywords, General
Sarbanes-Oxley policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- SEC Fair Disclosure Regulation – Mirrors the rule in the SEC Fair Disclosure policy; looks for three different conditions, and all must be satisfied: any keywords in the SEC Fair Disclosure Keywords dictionary, any keywords in the Company Name Keywords dictionary and any commonly used documents in the spreadsheet or document writing file types.
  The SEC Fair Disclosure keywords indicate possible disclosure of advance financial information.
  The company name keywords require editing by the user. This can include any name, alternate name, or abbreviation that might indicate a reference to the company. Specifically, the file type groups detected are: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, and pdf.

- Financial Information – Three different conditions that must be satisfied, including: a word from the Financial Keywords dictionary, a word from the Confidential/Proprietary Words dictionary, and a spreadsheet file type. The spreadsheet file types required are excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, and 123.

The included dictionaries are as follows:

- SEC Fair Disclosure Keywords
- Company Name Keywords
- Financial Keywords
- Confidential/Proprietary Words

SEC Fair Disclosure Regulation policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- SEC Fair Disclosure Regulation - Mirrors the rule in the SEC Fair Disclosure policy; looks for three different conditions, and all must be satisfied: any keywords in the SEC Fair Disclosure Keywords dictionary, any keywords in the Company Name Keywords dictionary and any commonly used documents in the spreadsheet or document writing file types.
  The SEC Fair Disclosure keywords indicate possible disclosure of advance financial information.
  The company name keywords require editing by the user. This can include any name, alternate name, or abbreviation that might indicate a reference to the company. Specifically, the file type groups detected are: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, and pdf.
The included dictionaries are as follows:

- SEC Fair Disclosure Keywords
- Company Name Keywords

### Sexually Explicit Language policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- Sexually Explicit Keywords, Confirmed - Looks for any single keyword in the Sex. Explicit Keywords, Confirmed dictionary.
- Sexually Explicit Keywords, Suspected - Looks for any three instances of keywords in the Sex. Explicit Words, Suspect dictionary.
- Sexually Explicit Keywords, Possible - Looks for any three instances of keywords in the Sex. Explicit Words, Possible dictionary.

The included dictionaries are as follows:

- Sex. Explicit Words, Confirmed
- Sex. Explicit Words, Suspect
- Sex. Explicit Words, Possible

### Source Code policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- Java Source Code - Looks for the Java Import Statements or Java Class Files regular expression.
- PERL Source Code - Looks for the three different PERL-related system patterns and regular expressions.

The included dictionary is Source Code Extensions
State Data Privacy policy template

The Described Content conditions are as follows:

- US Social Security Numbers - Looks for a word from the US SSN Keywords dictionary and a hit from the Valid Social Security Number premium pattern.
- ABA Routing Numbers - Looks for a word from the ABA Routing Number Keywords dictionary and a hit from the ABA Routing Number regular expression.
- Credit Card Numbers, All - Looks for a word from Credit Card Number Keywords and the credit card number system pattern.
- CA Drivers License Numbers - Looks for a match for the CA driver’s license number pattern, a match for a regular expression for terms relating to driver’s license, and a keyword from the California Keywords dictionary.
- NY Drivers License Numbers - Looks for a match for the NY driver’s license number pattern, a match for a regular expression for terms relating to driver’s license, and a keyword from the New York Keywords dictionary.
- Letter + 12 Digits Drivers License Numbers - Looks for a match for the stated driver’s license number pattern, a match for a regular expression for terms relating to driver’s license, and a keyword from the Letter/12 Num. DLN State Words dictionary (namely, Florida, Minnesota, and Michigan).
- IL Drivers License Numbers - Looks for a match for the IL driver’s license number pattern, a match for a regular expression for terms relating to driver’s license, and a keyword from the Illinois Keywords dictionary.
- NJ Drivers License Numbers - Looks for a match for the NJ driver’s license number pattern, a match for a regular expression for terms relating to driver’s license, and a keyword from the New Jersey Keywords dictionary.

Exception condition:

- Email to Affiliates - An exception for email messages to affiliates who are legitimately allowed to receive information covered under the State Data Privacy regulations. The Affiliate Domains dictionary requires editing by the user.

State Data Privacy, Consumer Data – Searches Record resource View for any three matches with the exception of First name, last name, pin and First name, last name, password.

Exception condition:

- Email to Affiliates - An exception for email messages to affiliates who are legitimately allowed to receive information covered under the State Data Privacy regulations. The Affiliate Domains dictionary requires editing by the user.
The included dictionaries are as follows:

- US SSN Keywords
- ABA Routing Number Keywords
- Credit Card Number Keywords
- California Keywords
- New York Keywords
- Letter/12 Num. DLN State Words
- Illinois Keywords
- New Jersey Keywords
- Affiliate Domains

**SWIFT Codes policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is SWIFT Code Regex. This condition looks for a match to the SWIFT code regular expression and a keyword from the SWIFT Code Keywords dictionary.

The included dictionary is SWIFT Code Keywords.

**UK Drivers License Numbers policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is a single compound condition with three parts: a single keyword from the UK Keywords dictionary, a pattern that matches the UK driver’s license regular expression, and different combinations of the phrase driver’s license using a regular expression.

The included dictionary is UK Keywords.

**UK Electoral Roll Numbers policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is a single compound condition with three parts: a single keyword from the UK Keywords dictionary, a pattern matching the UK Electoral Roll Number regular expression, and a single keyword from the UK Electoral Roll Number Words dictionary.
The included dictionaries are as follows:

- UK Keywords
- UK Electoral Roll Number Words

**UK National Insurance Number policy template**

The Described Content condition is UK National Insurance Numbers. This condition looks for a match to the UK National Insurance number regular expression and a keyword from the UK NIN Keywords dictionary.

The included dictionary is UK NIN Keywords.

**UK Passport Numbers policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content conditions are as follows:

- UK Passport Numbers (Old Type) - Looks for a keyword from the UK Passport Keywords dictionary and a pattern matching the regular expression for UK Passport Numbers (Old Type).
- UK Passport Numbers (New Type) - Looks for a keyword from the UK Passport Keywords dictionary and a pattern matching the regular expression for UK Passport Numbers (New Type).

The included dictionary is UK Passport Keywords.

**UK Tax ID Numbers policy template**

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is UK Tax ID Numbers. This condition looks for a match to the UK Tax ID number regular expression and a keyword from the UK Tax ID Number Keywords dictionary.

The included dictionary is UK Tax ID Number Keywords.

**US Intelligence Control Markings (CAPCO) and DCID 1/7 policy template**

The following describes the conditions and dictionaries that this policy template uses.
The Described Content condition looks for any keywords in the Secret, Top Secret, or Classified or Restricted dictionaries. Keywords and phrases other than those indicated in the dictionary titles are user-defined.

The included dictionaries are as follows:
- Secret
- Top Secret
- Classified or Restricted

### US Social Security Numbers policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is US Social Security Number Patterns. This condition looks for a match to the social security number regular expression and a keyword from the US SSN Keywords dictionary.

The included dictionary is US SSN Keywords.

### Violence and Weapons policy template

The following describes the conditions and dictionaries that this policy template uses.

The Described Content condition is Violence & Weapons. This compound condition looks for a keyword from the Violence Keywords dictionary and a keyword from the Weapons Keywords dictionary.

The included dictionaries are as follows:
- Violence Keywords
- Weapons Keywords
Using the Dell Remote Access Controller

This appendix includes the following topics:

- About the Dell Remote Access Controller (DRAC) card
- Restarting the Symantec Messaging Gateway appliance with DRAC forcefully
- Restarting the Symantec Messaging Gateway appliance from DRAC gracefully
- Installing and configuring Symantec Messaging Gateway appliance with DRAC remotely
- Installing Symantec Messaging Gateway image with DRAC from virtual media
- Viewing Dell server diagnostics with DRAC
- Deleting logs, configuration information, and data of Symantec Messaging Gateway appliance with DRAC
- Restoring Symantec Messaging Gateway appliance to the original factory configuration with DRAC

About the Dell Remote Access Controller (DRAC) card

Note: SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

The DRAC card is a hardware controller that is included with a Symantec Messaging Gateway appliance. Table D-1 lists the DRAC support information for Symantec appliances.
Table D-1 DRAC support for Symantec appliances

<table>
<thead>
<tr>
<th>Appliance</th>
<th>DRAC Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Mail Security 8380</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec Brightmail 8380</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec 8380</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec Brightmail 8360</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec 8360</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec Mail Security 8360</td>
<td>No</td>
</tr>
<tr>
<td>Symantec Mail Security 8340</td>
<td>No</td>
</tr>
<tr>
<td>Symantec Mail Security 8320</td>
<td>No</td>
</tr>
</tbody>
</table>

This card is integrated into a Symantec Messaging Gateway appliance as a daughtercard that connects to the system motherboard.

DRAC cards can be used to do any of the following tasks:

- Access a server after a server failure.
- Remotely view server internal event logs for diagnostic purposes.
- Manage a server by redirecting the console output (graphics and text) to a remote console.
- Perform an orderly shutdown of a server for maintenance task.
- Diagnose a server failure and restart the servers.
- Receive alerts through email or Simple Network Management Protocol (SNMP) traps when the server detects an error.

Symantec recommends you to use a separate network subnet for DRAC management.

After you enable DRAC feature on the appliance, Symantec recommends you to change the default DRAC root password. For more information on changing DRAC password, see the Dell support Web site.

See “Restarting the Symantec Messaging Gateway appliance with DRAC forcefully” on page 874.

See “Restarting the Symantec Messaging Gateway appliance from DRAC gracefully” on page 874.

See “Installing and configuring Symantec Messaging Gateway appliance with DRAC remotely” on page 875.

See “Installing Symantec Messaging Gateway image with DRAC from virtual media” on page 876.

See “Viewing Dell server diagnostics with DRAC ” on page 877.
See “Deleting logs, configuration information, and data of Symantec Messaging Gateway appliance with DRAC” on page 877.

See “Restoring Symantec Messaging Gateway appliance to the original factory configuration with DRAC” on page 878.

Restarting the Symantec Messaging Gateway appliance with DRAC forcefully

**Note:** SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

If you have access to DRAC with no access to the operating system on the Symantec Messaging Gateway appliance, DRAC enables you to remotely restart the appliance forcefully without accessing the operating system.

**To restart the Symantec Messaging Gateway appliance with DRAC forcefully**

1. In your browser, type the IP address of the DRAC card in the address field and press **Enter**.
2. Logon using DRAC root credentials and press **OK**.
3. Click **Power Management**.
4. Select **Power Cycle System**.
5. Click **Apply**.

   See “About the Dell Remote Access Controller (DRAC) card” on page 872.

Restarting the Symantec Messaging Gateway appliance from DRAC gracefully

**Note:** SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

You can restart an appliance when needed. Restarting an appliance entails the appliance turning itself off and then restarting itself. The DRAC enables remote access of the appliance through the supported Web browsers.
Restarting Symantec Messaging Gateway appliance gracefully stops all services and then restarts the appliance.

**Note:** If you reboot the appliance while you run a software update on Symantec Messaging Gateway, you can corrupt the appliance software.

To restart the Symantec Messaging Gateway appliance from DRAC gracefully

1. In your browser, type the IP address of the DRAC card in the address field and press **Enter**.
2. Logon using DRAC root credentials and press **OK**.
3. Click **Console**.
4. Ensure that the pop-up blocker is disabled and click **Connect**.
5. Logon with your Symantec Messaging Gateway appliance administrator credentials.
6. Execute **reboot** command.

See **reboot** on page 807.

See “About the Dell Remote Access Controller (DRAC) card” on page 872.

---

**Installing and configuring Symantec Messaging Gateway appliance with DRAC remotely**

**Note:** SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

You may want to install and configure Symantec Messaging Gateway appliance from a remote location. The DRAC enables remote access of the appliance through the supported Web browsers.

To install and configure a Symantec Messaging Gateway appliance with DRAC remotely

1. In your browser, type the IP address of the DRAC card in the address field and press **Enter**.
2. Logon using DRAC root credentials and press **OK**.
3. Click **Console**.
4 Ensure that the pop-up blocker is disabled and click Connect.

5 Install Symantec Messaging Gateway product.

For more information, see the Symantec Messaging Gateway Installation Guide.

See “About the Dell Remote Access Controller (DRAC) card” on page 872.

Installing Symantec Messaging Gateway image with DRAC from virtual media

Note: SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

You may want to install Symantec Messaging Gateway from a remote location. Install Symantec Messaging Gateway on an appliance by using the virtual media that is mapped to the local ISO file or your local CD/DVD-ROM drive.

To install Symantec Messaging Gateway image with DRAC from virtual media

1 Copy the Symantec Messaging Gateway ISO image to your local drive or insert the CD/DVD into your local CD/DVD-ROM drive.

2 In your browser, type the IP address of the DRAC card in the address field and press Enter.

3 Logon using DRAC root credentials and click OK.

4 Click Media.

5 Select the Symantec Messaging Gateway ISO image file by browsing to the appropriate location.

   If you have mapped the virtual media to the local CD/DVD-ROM drive, select the local CD/DVD-ROM drive.

6 Click Connect.

7 Restart the appliance.

8 When the system restarts, type the appropriate function key to choose the boot media.

   For more information about choosing a function key, see the Dell support Web site.

9 Select Virtual CDROM.

See “About the Dell Remote Access Controller (DRAC) card” on page 872.
Viewing Dell server diagnostics with DRAC

Note: SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

When the Dell server fails, you can connect to the system remotely and view the Dell diagnostic report from DRAC.

To view Dell server diagnostics with DRAC

1. Restart Symantec Messaging Gateway remotely.
   See “Restarting the Symantec Messaging Gateway appliance with DRAC forcefully” on page 874.

2. While the system restarts, type the appropriate function key to initiate the diagnostics.
   For more information on choosing the function key to initiate diagnostics, see the Dell support website.

   See “About the Dell Remote Access Controller (DRAC) card” on page 872.

Deleting logs, configuration information, and data of Symantec Messaging Gateway appliance with DRAC

Note: SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

You may want to delete logs, configuration information, and data remotely. The DRAC enables remote access of the appliance through the supported Web browsers.

To delete logs, configuration information, and data of Symantec Messaging Gateway appliance with DRAC

1. In your browser, type the IP address of the DRAC card in the address field and press Enter.

2. Logon using DRAC root credentials and press OK.

3. Click Console.

4. Ensure that the pop-up blocker is disabled and click Connect.
5 Logon with your Symantec Messaging Gateway appliance administrator credentials.

6 Execute `delete` command.

   See `delete` on page 752.

   See "About the Dell Remote Access Controller (DRAC) card" on page 872.

---

**Restoring Symantec Messaging Gateway appliance to the original factory configuration with DRAC**

**Note:** SMG 10.7.0 runs on two different hardware platforms: the Dell 83xx and the Symantec 8380-S450. The Dell 83xx platform supports DRAC/iDRAC, but the Symantec 8380-S450 platform does not.

You may want to restore your appliance to the original factory configuration remotely. The DRAC enables remote access of the appliance through the supported Web browsers.

To restore Symantec Messaging Gateway appliance to the original factory configuration with DRAC

1 In your browser, type the IP address of the DRAC card in the address field and press **Enter**.

2 Logon using DRAC root credentials and press **OK**.

3 Click **Console**.

4 Ensure that the pop-up blocker is disabled and click **Connect**.

5 Logon with your Symantec Messaging Gateway appliance administrator credentials.

6 Execute the `delete all` command.

   See `delete` on page 752.

   See "About the Dell Remote Access Controller (DRAC) card" on page 872.
Federal Information Processing Standard (FIPS) compliance

This appendix includes the following topics:

- About Symantec Messaging Gateway FIPS 140-2 level 1 standard compliance
- About installing or upgrading if you use FIPS mode
- About certificate trust for the Control Center
- FIPS mode best practices and considerations
- About the limitations of some Symantec Messaging Gateway features with FIPS
- Turning FIPS mode on or off

About Symantec Messaging Gateway FIPS 140-2 level 1 standard compliance

FIPS 140-2 is a National Institute of Standards and Technology (NIST) standard that outlines requirements for secure design and implementation of cryptographic modules. Many organizations use this standard when they consider the use of hardware and software components.

The cryptographic modules that this release uses comply with FIPS 140-2 level 1 requirements. These modules have already been submitted to the Cryptographic Module Validation Program for validation against the FIPS 140-2 level 1 standard. Symantec expects the Symantec Cryptographic Modules to receive official validation from the National Institute of Standards and Technology sometime before the next major release of Symantec Messaging Gateway.
The following validated cryptographic modules are included as part of Symantec Messaging Gateway:

- Symantec Scanner Cryptographic Module
- Symantec Control Center Cryptographic Module

The cryptographic modules that this release uses are based on the modules that NIST has previously validated. They modules are considered to conform to the FIPS 140-2 level 1 standard.

The following cryptography conforms to the FIPS 140-2 level 1 standard and is currently under test for validation:

- Web server HTTPS connections from the Web browser to the Control Center
- HTTPS connections from the Control Center to the Scanner (agent) hosts
- Control Center administrator credential creation and storage
- Symantec Messaging Gateway to Symantec Global Intelligence Network communications
- SMTP TLS communications
- Software update communications
- Remote Secure Shell access
- SNMPv3 encryption
- DomainKeys Identified Mail (DKIM) keys
- Data directory server secure communications (LDAPS)

Some limitations apply to certain Symantec Messaging Gateway features.

See "About the limitations of some Symantec Messaging Gateway features with FIPS" on page 883.

For information about the validation, on the Internet, go to the following URL:

http://www.symantec.com/docs/TECH167725

For more information about the current state of FIPS 140-2 level 1 testing and validation, you can also contact your Symantec account representative.

For general information about the FIPS 140-2 standard and validation program, on the Internet, go to the following URL:

National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program
About installing or upgrading if you use FIPS mode

You install or upgrade to this release of Symantec Messaging Gateway in the same way as you installed or upgraded to previous releases.

The following information is important to note about new installations or upgrades:

- Symantec Messaging Gateway product architecture is identical regardless of whether you have FIPS mode turned on or turned off. The difference is that when FIPS mode is on, the product enforces a strict list of cryptographic ciphers that are associated with the FIPS 140-2 standard. The larger list of ciphers that Symantec Messaging Gateway uses when FIPS mode is turned off increases interoperability with external mail transfer agents (MTAs). See “Turning FIPS mode on or off” on page 884.

- A new installation of Symantec Messaging Gateway defaults to FIPS mode off.

- If you used FIPS mode in version 9.5.2 or later, the state of FIPS mode is preserved upon upgrade.

- FIPS mode state is not saved as part of a backup. If you restore a host to an image or appliance that does not have FIPS mode already on, you must turn it back on manually after the restore. When you do a restore, it is a best practice to check the status of FIPS mode and then change it as needed. See “Restoring an appliance from backups” on page 711.

- After you turn FIPS mode on, the following actions change the FIPS mode to its default setting (off):
  - A clean install of the Symantec Messaging Gateway software
  - A clean restore of the operating system
  - A transfer to a new host

Before you install or upgrade Symantec Messaging Gateway, ensure that you read the Release Notes that accompanied this release.

For specific details about how to install this release for the first time or how to upgrade from an earlier release, see the Symantec Messaging Gateway Installation Guide.

The following information is important to note:

- As of this release, the Control Center no longer accepts SSLv2 or SSLv3 HTTPS connections. It accepts only TLS 1.0 connections.

- In this release, the following actions take significantly longer with FIPS mode turned on than they do with FIPS mode turned off:
  - Restarting the Message Transfer Agent (MTA) service
Any configuration change that implicitly restarts the MTA service
The host may appear to be hung for several minutes, but it is not.
As a best practice, enable FIPS mode as the final step in your setup process before you deploy the host in a production environment.

About certificate trust for the Control Center

The signature algorithm that is used for the Control Center’s self-signed certificates is not FIPS-compliant. For FIPS 140-2 level 1 compliance, you must request a FIPS-compliant certificate from a certificate authority vendor and then import it into the Control Center. The file that contains the certificate must be in PEM format.

See “About certificates” on page 169.

See “Importing a Certificate Authority signed certificate” on page 177.

FIPS mode best practices and considerations

The following describes best practices and considerations for working with FIPS mode:

Key lengths and FIPS compliance
Symantec Messaging Gateway currently lets you import TLS keys and HTTPS keys that are shorter than the minimum key length permitted by FIPS 140-2 level 1 standard. When you use SNMPv3, be sure that you use a key that is long enough to conform to the FIPS 140-2 level 1 standard. To conform to the FIPS 140-2 level 1 standard, administrators must remember to create keys that are 1024 bits or greater in length.

About FIPS mode and SNMPv3
If you use SNMPv3 and want to run Symantec Messaging Gateway in FIPS mode, you must configure the Control Center to use the SHA1withRSA authentication type.

See “Configuring SNMP settings to monitor network devices” on page 673.

About SMTP authorization
You should be aware that the Require TLS encryption option for SMTP authorization does not work as you would expect when you have FIPS mode turned on. When this option is turned off, Symantec Messaging Gateway accepts both TLS and SSLv3.0 connections. However, when FIPS mode is turned on, Symantec Messaging Gateway supports and uses only TLS encryption and all earlier encryption modes fail. So, when FIPS mode is turned on, even if you have disabled the Require TLS encryption option, SSLv3.0 connections fail.

See “Assigning an MTA TLS certificate to a Scanner” on page 185.
About the limitations of some Symantec Messaging Gateway features with FIPS

The following are the Symantec Messaging Gateway features that do not operate in strict conformance to FIPS 140-2 level 1 standard:

Remote credential storage

Symantec Messaging Gateway does not use FIPS-compliant algorithms to encrypt credentials for the following entities:

- LDAP administrator passwords
- End user passwords
- Scheduled backups
  Ad hoc backups are not affected, as they do not use stored credentials.

Exact Data Matching (EDM) and record resources management

No workaround currently exists for this limitation.

Symantec Messaging Gateway does not use FIPS-compliant algorithms to store EDM or record resources.

Spam Quarantine release credentials

Symantec Messaging Gateway does not use FIPS-compliant algorithms to encrypt stored credentials in the digest emails used for access to end user Spam Quarantine. Users and administrators who enable the release of messages through Spam Quarantine notifications with FIPS mode on are not strictly FIPS-compliant.

To work around this issue, you can require that end users log directly into the quarantine to release messages.

Data directory service connections to the Domino directory servers that use LDAPS

When FIPS mode is on, the Symantec Messaging Gateway data directory service cannot connect to a Domino directory server that is configured to use LDAPS.

This limitation occurs because in FIPS mode, the data directory service uses only TLS 1.0. The versions of Domino that Symantec Messaging Gateway supports do not support TLS 1.0.
Demo certificate

The signature algorithm that is used for the demo Control Center user interface certificate is **SHA1withRSA**, which is not a FIPS-approved algorithm. To maintain compatibility with Internet Explorer browsers that run on Windows XP SP2 or earlier, the demo certificate has not been changed.

To work around this issue, you can manually import a certificate authority vendor certificate that uses a FIPS-approved algorithm into the Control Center.

See “Adding a CA or an intermediate certificate” on page 175.

See “Importing a Certificate Authority signed certificate” on page 177.

## Turning FIPS mode on or off

An administrator must log into each appliance individually to turn on FIPS mode or to turn off FIPS mode on that appliance. When you turn FIPS mode on or off on each host, the change of mode affects only the list of ciphers that are used by the Scanners. FIPS mode is configurable for Scanners because the communications protocols and versions that external mail transfer agents (MTAs) use are not under your control. Communication through some external MTAs might be disrupted if you run the Scanners with FIPS mode turned on.

Changing the FIPS mode does not affect the Control Center process. The Control Center for Symantec Messaging Gateway release always runs in FIPS mode. The Symantec Messaging Gateway product architecture remains the same, regardless of whether FIPS mode is on or off.

Each appliance (physical or virtual) has a set of configuration commands. You can execute these commands from a remote session that uses an SSH client or from the system console. FIPS mode for Symantec Messaging Gateway is implemented only from the command line. You cannot manage FIPS mode from the Control Center in this release.

---

**Note:** FIPS mode-related actions are logged to syslog and appear in `/data/logs/messages`.

See “Administering Symantec Messaging Gateway through the command line” on page 730.

---

**Note:** When you change FIPS mode, do not interrupt the command. If you accept the prompt to restart but you interrupt the command before the restart occurs, then the state of FIPS mode does not change. You are not able to change the FIPS mode in the future.
To turn on FIPS mode on a host
1. Use your preferred method to log in to the appliance's command-line interface.
2. Type the following command:
   ```
   fipsmode on
   ```

To turn off FIPS mode on a host
1. Use your preferred method to log in to the appliance's command-line interface.
2. Type the following command:
   ```
   fipsmode off
   ```

To verify that Symantec Messaging Gateway conforms to the FIPS 140-2 level 1 standard, you can check to see that FIPS mode status is on.

To check the status of FIPS mode on a host
1. Use your preferred method to log in to the appliance's command-line interface.
2. Type the following command:
   ```
   fipsmode status
   ```

   If FIPS mode is on, the status that is returned is **FIPS mode**. If FIPS mode is off, the status that is returned is **Non-FIPS mode**.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>A component that facilitates communicating configuration information between the Control Center and each Scanner.</td>
</tr>
<tr>
<td>annotation</td>
<td>A phrase or paragraph that is placed at the beginning or end of the body of an email message. Up to 1000 distinct annotations are allowed for use in specific categories of messages for specific policy groups of recipients. You can use this feature to automate email disclaimers.</td>
</tr>
<tr>
<td>archive</td>
<td>An action that can be performed on email messages in which messages are forwarded to a specific SMTP address for long-term storage.</td>
</tr>
<tr>
<td>attachment list</td>
<td>A list of attachment types for use in filtering. You can create attachment lists based on file naming (for example, based on the file extension) on the true type of each file. Or you can use a pre-filled list.</td>
</tr>
<tr>
<td>Audit ID</td>
<td>A unique identifier that is included as a message header in all processed messages.</td>
</tr>
<tr>
<td>authentication</td>
<td>The process of determining the identity of a user attempting to access a network. Authentication occurs through challenge/response, time-based code sequences, or other techniques. Authentication typically involves the use of a password, certificate, PIN, or other information that can be used to validate identity over a computer network.</td>
</tr>
<tr>
<td>Bad Sender</td>
<td>A sender from whom you do not want to accept email messages. A Bad Sender is a member of at least one of the following groups: Local Bad Sender Domains, Local Bad Sender IPs, Third Party Bad Senders, or Symantec Global Bad Senders.</td>
</tr>
<tr>
<td>bounce</td>
<td>An action that can be performed on an email message by a mail server. The action returns the message to its From: address with a custom response.</td>
</tr>
<tr>
<td>Bounce Attack</td>
<td>A feature of Symantec Messaging Gateway that eliminates the bounced messages that are a result of redirection, while still allowing legitimate bounce message notification.</td>
</tr>
<tr>
<td>Brightmail Engine</td>
<td>The Symantec Messaging Gateway component that scans email and attachments and file transfers for malware, spam, and content filtering according to polices that you configure.</td>
</tr>
<tr>
<td>broadcast address</td>
<td>A common address that is used to direct (broadcast) a message to all systems on a network. The broadcast address is based upon the network address and the subnet mask.</td>
</tr>
<tr>
<td><strong>CA (Certificate Authority)</strong></td>
<td>A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the entity granting the unique certificate is, in fact, who it claims to be. This means that the CA usually has an arrangement with the requesting entity to confirm a claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
<td>A file that is used by cryptographic systems as proof of identity. It contains a user's name and public key.</td>
</tr>
<tr>
<td><strong>Certificate Authority-signed SSL</strong></td>
<td>A type of Secure Sockets Layer (SSL) that provides authentication and data encryption through a certificate that is digitally signed by a Certificate Authority.</td>
</tr>
<tr>
<td><strong>CIDR (classless interdomain routing)</strong></td>
<td>A way of specifying a range of addresses using an arbitrary number of bits. For instance, a CIDR specification of 206.13.1.48/25 includes any address in which the first 25 bits of the address matched the first 25 bits of 206.13.1.48.</td>
</tr>
<tr>
<td><strong>clean</strong></td>
<td>An action that consists of deleting unrepairable virus infections and repairing repairable virus infections.</td>
</tr>
<tr>
<td><strong>Conduit</strong></td>
<td>A component that retrieves new and updated filters from Symantec Security Response through secure HTTPS file transfer. Once the filters are retrieved, the Conduit authenticates filters. It then alerts the Brightmail Engine that new filters are to be received and implemented. Finally, the Conduit manages statistics for use by Symantec Security Response and for generating reports.</td>
</tr>
<tr>
<td><strong>content filtering</strong></td>
<td>A set of features that enable administrators to enforce corporate email policies, reduce legal liability, and ensure compliance with regulatory requirements.</td>
</tr>
<tr>
<td><strong>Control Center</strong></td>
<td>A Web-based configuration and administration center. Each site has one Control Center. The Control Center also houses Spam Quarantine and supporting software. You can configure and monitor all of your Scanners from the Control Center.</td>
</tr>
</tbody>
</table>
| **data source** | (1) A set of configuration data that includes host connection parameters and the set of functions that are enabled for that source.  
(2) A file that your database administrator provides, which consists of columns of the company-specific, delimited data. The data source contains the customer, patient, or other data that you want to protect but that cannot be identified through regular expressions or keywords. For example, you can use a data source file to create a content filtering policy to filter outbound email for sensitive customer or employee data. |
<p>| <strong>DDS (directory data service)</strong> | A Symantec Messaging Gateway service that lets you use the information in your Lightweight Directory Access Protocol (LDAP) directories for Symantec Messaging Gateway features. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>defer</strong></td>
<td>An action that an MTA that receives an email message can take. The action consists of using a 4xx SMTP response code to tell the sending MTA to try again later.</td>
</tr>
<tr>
<td><strong>definitions</strong></td>
<td>The content that contains necessary information to detect and eliminate risks, such as malware and adware. Definitions are also used to detect unwanted email, such as spam.</td>
</tr>
<tr>
<td><strong>dictionary</strong></td>
<td>A list of words and phrases against which email messages can be checked for non-compliant content. Symantec Messaging Gateway lets you create the content filtering policies that screen email against a specific dictionary. You can use the provided dictionaries, add terms to the provided dictionaries, or add additional dictionaries.</td>
</tr>
<tr>
<td><strong>directory data source</strong></td>
<td>A set of configuration data that includes host connection parameters and the set of functions that are enabled for that source.</td>
</tr>
<tr>
<td><strong>directory data source function</strong></td>
<td>An LDAP query configuration that enables particular features in Symantec Messaging Gateway. Symantec Messaging Gateway provides four directory data source functions: authentication, address resolution, routing, and recipient validation.</td>
</tr>
<tr>
<td><strong>directory harvest attack</strong></td>
<td>A tactic that spammers use to determine valid email addresses. A directory harvest attack occurs when a spammer sends a large quantity of possible email addresses to a site. An unprotected mail server rejects the messages that are sent to invalid addresses. This behavior lets spammers know which email addresses are valid by checking the rejected messages against the original list.</td>
</tr>
<tr>
<td><strong>DKIM (Domain Key Identified Mail)</strong></td>
<td>A protocol that uses public-key cryptography that lets the sending MTA electronically sign legitimate email messages in a way that recipient MTAs can verify. See also MTA (Mail Transfer Agent).</td>
</tr>
<tr>
<td><strong>DNS (Domain Name Server) proxy</strong></td>
<td>An intermediary between a workstation user and the Internet that allows the enterprise to ensure security and administrative control.</td>
</tr>
<tr>
<td><strong>DNS (Domain Name System)</strong></td>
<td>A hierarchical system of host naming that groups TCP/IP hosts into categories. For example, in the Internet naming scheme, names with .com extensions identify hosts in commercial businesses.</td>
</tr>
<tr>
<td><strong>DNS server</strong></td>
<td>A repository of addressing information for specific Internet hosts. Name servers use the Domain Name System (DNS) to map IP addresses to Internet hosts.</td>
</tr>
<tr>
<td><strong>downstream</strong></td>
<td>At a later point in the flow of email. A downstream email server is an email server that receives messages at a later point in time than other servers. In a multiple-server system, inbound mail travels a path from upstream mail servers to downstream mail servers. Downstream can also refer to other types of networking paths or technologies.</td>
</tr>
<tr>
<td><strong>email virus attack</strong></td>
<td>A series of virus-infected emails from a specific domain. Symantec Messaging Gateway lets you choose an action to perform on these messages.</td>
</tr>
</tbody>
</table>
encrypted attachment  A message attachment that has been converted into a form that unauthorized persons cannot easily understand. Symantec Messaging Gateway does not scan encrypted attachments, but it lets you choose an action to take when an encrypted attachment is detected.

Expunger  A component of Spam Quarantine and content filtering quarantine incidents, which resides on the Control Center computer in Symantec Messaging Gateway. The Expunger can be configured to periodically remove older or unwanted messages or incidents from the Spam Quarantine or content filtering incidents folders.

false positive  A piece of legitimate email that is mistaken for spam and classified as spam by Symantec Messaging Gateway.

Fastpass  A feature of Symantec Messaging Gateway that lets most of the email messages that are from verified Good Senders bypass spam filtering. Fastpass conserves resources by providing a temporary exemption from spam scanning for senders with a demonstrated history of sending no spam messages. Fastpass reduces the processing time that is required for messages from legitimate sources.

filter  A method for analyzing email messages, used to determine what action to take on each message. Symantec Messaging Gateway uses a variety of types of filters to process messages. A filter can be provided by Symantec, created by a local administrator, created by an end user, or provided by a third party.

filter policy  In Symantec Messaging Gateway, a set of actions that apply to a category of messages. The actions that are specified in a filter policy are applied to users who are members of a policy group that includes the filter policy. Symantec Messaging Gateway uses the following types of filter policies: spam, malware, and content filtering policies. Filter policies can also make use of policy resources. See also policy group, policy resources.

FIPS (Federal Information Processing Standard)  A National Institute of Standards and Technology (NIST) standard that outlines requirements for secure design and implementation of cryptographic modules.

firewall  A program that protects the resources of one network from users from other networks. Typically, an enterprise with an intranet that lets its workers access the Internet wants a firewall to prevent outsiders from accessing its own private data resources.

gateway  A network point that acts as an entrance to another network. A gateway can also be any computer or service that passes packets from one network to another network during their trip across the Internet.

Good Sender  A sender from whom you want to accept email messages. A Good Sender is a member of at least one of the following groups: Local Good Sender Domains, Local Good Sender IPs, Third Party Good Senders, or Symantec Global Good Senders.

heuristic  Filters that pro-actively target patterns common in spam and viruses.
host 1. In a network environment, a computer that provides data and services to other computers. Services might include peripheral devices, such as printers, data storage, email, or Web access. 2. In a remote control environment, a computer to which remote users connect to access or exchange data.

incidents Messages that violate a policy's conditions. Information about incidents can help you understand, prevent, respond to, and audit potential violations. In Symantec Messaging Gateway, malware incidents are stored in the Suspect Virus Quarantine and spam incidents are stored in Spam Quarantine. Content filtering incidents are stored in Quarantine Incidents folders or Informational Incidents folders.

See also Suspect Virus Quarantine, Spam Quarantine, Quarantine Incidents, and Informational Incidents.

Informational Incidents A folder that contains the incidents that are created as a result of a content filtering policy violation in which the action is Create an informational incident.

IP (Internet Protocol) The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one address that uniquely identifies it to all other computers on the Internet.

IP address A unique number that identifies a workstation on a TCP/IP network and specifies routing information. Each workstation on a network must be assigned a unique IP address. The unique IP address consists of the network ID plus a unique host id that the network administrator assigns. This address is usually represented in dot-decimal notation, with the decimal values separated by a period (for example, 123.45.6.24).

language identification In Symantec Messaging Gateway, a feature that lets you block or allow the messages that are written in a specified language. For example, you can choose to only allow English messages, or block messages in English and Spanish and allow messages in all other languages. Administrators can set language identification for groups of users, or allow users to specify their own settings.

LDAP (Lightweight Directory Access Protocol) A software protocol that enables anyone to locate organizations, individuals, and other resources (such as files and devices). These resources can be located whether on the Internet or on a corporate intranet. LDAP is a lightweight version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.

Local Bad Sender Domains Domains of senders from whom you do not want to accept messages. Specify Local Bad Sender Domains in the Control Center.

Local Bad Sender IPs IP addresses of senders from whom you do not want to accept messages. Specify Local Bad Sender IPs in the Control Center.

Local Good Sender Domains Domain addresses of the senders that are permitted by default and bypass spam filtering. Specify Local Good Sender Domains in the Control Center.
Local Good Sender IPs | IP addresses of the senders that are permitted by default and bypass spam filtering. Specify Local Good Sender IPs in the Control Center.

malware | Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.

marketing mail | Email messages that contain the commercial or fund-raising messages that the user may have requested. These messages often do not include a functional opt-out facility.

messaging gateway | The outermost point in a network where mail servers are located. All other mail servers are downstream from the mail servers that are located at the messaging gateway.

MIME (Multipurpose Internet Mail Extensions) | A protocol used for transmitting documents with different formats via the Internet.

MTA (Mail Transfer Agent) | A generic term for programs such as Sendmail, postfix, or qmail that send and receive mail between servers using SMTP. The MTA in each Symantec Messaging Gateway Scanner routes the inbound messages and outbound messages to the Brightmail Engine for processing. Then the MTA delivers filtered messages to their internal destinations or to remote destinations.

name server | See DNS (Domain Name Server) proxy.

newsletters | Email messages that include content on specific topics, on a known periodic basis, often weekly or monthly. The user may have requested to receive these publications. A functional opt-out facility is generally available.

packet | A unit of data that is formed when a protocol breaks down messages that are sent along the Internet or other networks. Messages are broken down into standard-sized packets to avoid overloading lines of transmission with large chunks of data. Each of these packets is separately numbered and includes the Internet address of the destination. Upon arrival at the recipient computer, the protocol recombines the packets into the original message.

phishing | An attempt to illegally gather personal and financial information by sending a message that appears to be from a well known and trusted company. A phishing message typically includes at least one link to a fake Web site that is designed to mimic the site of a legitimate business. The site is designed to entice the recipient to provide the information that can be used for identity theft or online financial theft.

policy | A set of message filtering instructions that Symantec Messaging Gateway implements on a message or set of messages. See also filter policy, policy group.

policy group | In Symantec Messaging Gateway, a group of users to which you can apply a unique set of filter policies. You can specify users by email address or domain. See also filter policy.
port 1. A hardware location used for passing data into and out of a computing device. Personal computers have various types of ports, including internal ports for connecting disk drives, monitors, and keyboards, and external ports, for connecting modems, printers, mouse devices, and other peripheral devices. 2. In TCP/IP and UDP networks, the name given to an endpoint of a logical connection. Port numbers identify types of ports. For example, both TCP and UDP use port 80 for transporting HTTP data.

probe account An invalid email address that is used to attract spam. You create a probe account and add it to the Symantec Probe Network through the Control Center.

Probe network A network of email accounts that Symantec’s probe network partners provide. Used by Symantec Security Response to detect spam, the probe network has a statistical reach of over 300 million email addresses. The network includes over 2 million probe accounts.

Probe network partners ISPs or the corporations that participate in the probe network.

protocol A set of rules for encoding and decoding data so that messages can be exchanged between computers and so that each computer can fully understand the meaning of the messages. On the Internet, the exchange of information between different computers is made possible by the suite of protocols known as TCP/IP. Protocols can be stacked, meaning that one transmission can use two or more protocols. For example, an FTP session uses the FTP protocol to transfer files, the TCP protocol to manage connections, and the IP protocol to deliver data.

proxy server A server that acts on behalf of one or more other servers, usually for screening, firewall, or caching purposes, or a combination of these purposes. Also called a gateway. Typically, a proxy server is used within a company or enterprise to gather all Internet requests, forward them out to Internet servers, and then receive the responses and in turn forward them to the original requester within the company.

reject An action that an MTA receiving an email message can take. The action consists of using a 5xx SMTP response code to tell the sending MTA that the message is not accepted.

replication In Symantec Messaging Gateway, the process of duplicating configuration data from the Control Center to Scanners.

Scanner The component in Symantec Messaging Gateway that filters mail. Each site can have one or many Scanners. The configuration of each Scanner is managed through the Control Center.

sender group A category of email senders that Symantec Messaging Gateway manages using the Brightmail Adaptive Reputation Management (Brightmail ARM) feature. Sender groups can be based upon IP addresses, domains, third-party lists, or Symantec lists. You can configure the Brightmail ARM to take a variety of actions on messages from each sender group.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender ID</td>
<td>A set of standard practices to authenticate email. If the sender's domain owner participates in Sender ID, the recipient MTA can check for forged return addresses. Symantec Messaging Gateway lets you specify an action for the messages that fail Sender ID authentication.</td>
</tr>
<tr>
<td>signature</td>
<td>1. A state or pattern of activity that indicates a violation of policy, a vulnerable state, or an activity that may relate to an intrusion. 2. Logic in a product that detects a violation of policy, a vulnerable state, or an activity that may relate to an intrusion. This term is also referred to as a signature definition, an expression, a rule, a trigger, or signature logic. 3. Information about a signature including attributes and descriptive text. This term is more precisely referred to as signature data.</td>
</tr>
<tr>
<td>SMTP (Simple Mail Transfer Protocol)</td>
<td>The protocol that allows email messages to be exchanged between mail servers. Then, clients retrieve email, typically through the POP protocol or IMAP protocol.</td>
</tr>
<tr>
<td>spam</td>
<td>1. Unsolicited commercial bulk email. 2. An email message that is identified as spam by Symantec Messaging Gateway, using its filters.</td>
</tr>
<tr>
<td>Spam Quarantine</td>
<td>A file directory that stores email messages separately from the normal message flow, and allows access to those messages. In Symantec Messaging Gateway, Spam Quarantine is located on the Control Center computer and provides users with Web access to their spam messages. Users can browse, search, and delete their spam messages and can also redeliver misidentified messages to their inbox. An administrator account provides access to all quarantined messages. Spam Quarantine can also be configured for administrator-only access.</td>
</tr>
<tr>
<td>spam scoring</td>
<td>The process of scoring messages. Symantec Messaging Gateway assigns a spam score to each message that expresses the likelihood that the message is spam. See also suspected spam.</td>
</tr>
<tr>
<td>SPF (Sender Policy Framework)</td>
<td>A set of standard practices to authenticate email. If the sender's domain owner participates in SPF, the recipient MTA can check for forged return addresses. Symantec Messaging Gateway lets you specify an action for the messages that fail SPF authentication.</td>
</tr>
<tr>
<td>spyware</td>
<td>The stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay the information back to another computer.</td>
</tr>
<tr>
<td>SSH (Secure Shell)</td>
<td>A program that allows a user to log on to another computer securely over a network by using encryption. SSH prevents third parties from intercepting or otherwise gaining access to the information that is sent over the network.</td>
</tr>
<tr>
<td>SSL (Secure Sockets Layer)</td>
<td>A protocol that allows mutual authentication between a client and server. The protocol allows for the establishment of an authenticated and encrypted connection, thus ensuring the secure transmission of information over the Internet. See also TLS.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>submitter ID</td>
<td>An ID assigned to a Control Center that is required to submit messages to Symantec for custom spam rules. Custom spam rules are applied to the Scanners that any Control Center with that ID controls. See also spam.</td>
</tr>
<tr>
<td>subnet mask</td>
<td>Used to subdivide an assigned network address into additional subnetworks by using some of the unassigned bits to designate local network addresses. Subnet masking facilitates routing by identifying the network of the local host. The subnet mask is a required configuration parameter for an IP host. A local bit mask (set of flags) that specifies which bits of the IP address specify a particular IP network or a host within a subnetwork. Used to &quot;mask&quot; a portion of an IP address so that TCP/IP can determine whether any given IP address is on a local network or remote network. Each computer that is configured with TCP/IP must have a subnet mask defined.</td>
</tr>
<tr>
<td>Suspect Virus Quarantine</td>
<td>A file directory that temporarily holds the messages that are suspected to contain malware. Messages with suspicious attachments can be held in Suspect Virus Quarantine for a number of hours and then filtered again with updated filters, if available. This processing delay capability enables Symantec Messaging Gateway to more effectively deal with new virus threats as they emerge.</td>
</tr>
<tr>
<td>suspected spam</td>
<td>A message that Symantec Messaging Gateway deems can potentially be spam based on the scores that are derived from pattern matching and heuristic analysis. Through policies, you can specify different actions for the messages that are identified as suspected spam. See also spam.</td>
</tr>
<tr>
<td>suspicious attachment</td>
<td>A message attachment that Symantec Messaging Gateway has determined may contain malware. You can choose what action to take when a suspicious attachment is detected.</td>
</tr>
<tr>
<td>suspicious URL content</td>
<td>Email messages that contain URLs that are abused to deliver spam or malware payloads. Suspicious URLs include free hosting sites, URL shortening services, and URL redirecting services. Symantec Messaging Gateway can filter against the email messages that contain one or more suspicious URLs.</td>
</tr>
<tr>
<td>Symantec Global Bad Senders</td>
<td>A list of IP addresses collected by Symantec, based on global spam data from the mail servers that Symantec protects. One of the sender groups in Symantec Messaging Gateway.</td>
</tr>
<tr>
<td>Symantec Global Good Senders</td>
<td>A list of IP addresses collected by Symantec, based on global legitimate sender data from the mail servers that Symantec protects. One of the sender groups in Symantec Messaging Gateway.</td>
</tr>
<tr>
<td>Symantec Network Prevent</td>
<td>A component of Symantec Data Loss Prevention which discovers, monitors, and protects confidential data wherever it is stored or used. Symantec Messaging Gateway integrates with Symantec Network Prevent to deliver, route, hold, or block email traffic.</td>
</tr>
</tbody>
</table>
Symantec Security Response is a team of dedicated intrusion experts, security engineers, virus hunters, threat analysts. They are a global technical support team that work in tandem to provide extensive coverage for enterprise businesses and consumers. Symantec Security Response also leverages sophisticated threat and early warning systems to provide customers with comprehensive, global, 24x7 Internet security expertise. This expertise helps you proactively guard against today’s blended Internet threats and complex security risks.

Security Response covers the full range of security issues to provide complete protection for customers including the following areas:

- Viruses, malware, worms, Trojan horses, bots, and other malicious code
- Hackers
- Vulnerabilities
- Spyware, adware, and dialer programs
- Spam
- Phishing and other forms of Internet fraud

Security Response keeps Symantec and its customers ahead of attackers by forecasting the next generation of threats using its worldwide intelligence network and unmatched insight. The team delivers the bi-annual Internet security threat report that identifies critical trends, and statistics for the entire security community. It places Symantec at the forefront of the rapidly shifting landscape.

With the steadily increasing sophistication of today’s threats, a holistic approach to defending your digital assets is the key to repelling attackers. With a unified team covering the full range of security issues, Symantec Security Response helps provide its customers with fully integrated protection. It combines the collective expertise of hundreds of security specialists to bring updates and security intelligence to the full range of Symantec’s products and services. Symantec has research and response centers that are located around the world.

### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Symantec Security Response** | Symantec Security Response is a team of dedicated intrusion experts, security engineers, virus hunters, threat analysts. They are a global technical support team that work in tandem to provide extensive coverage for enterprise businesses and consumers. Symantec Security Response also leverages sophisticated threat and early warning systems to provide customers with comprehensive, global, 24x7 Internet security expertise. This expertise helps you proactively guard against today’s blended Internet threats and complex security risks. Security Response covers the full range of security issues to provide complete protection for customers including the following areas:
- Viruses, malware, worms, Trojan horses, bots, and other malicious code
- Hackers
- Vulnerabilities
- Spyware, adware, and dialer programs
- Spam
- Phishing and other forms of Internet fraud

Security Response keeps Symantec and its customers ahead of attackers by forecasting the next generation of threats using its worldwide intelligence network and unmatched insight. The team delivers the bi-annual Internet security threat report that identifies critical trends, and statistics for the entire security community. It places Symantec at the forefront of the rapidly shifting landscape.

With the steadily increasing sophistication of today’s threats, a holistic approach to defending your digital assets is the key to repelling attackers. With a unified team covering the full range of security issues, Symantec Security Response helps provide its customers with fully integrated protection. It combines the collective expertise of hundreds of security specialists to bring updates and security intelligence to the full range of Symantec’s products and services. Symantec has research and response centers that are located around the world. |
| **Third Party Bad Senders** | A sender group in Symantec Messaging Gateway that lets administrators add multiple lists of Bad Senders that third-party services compile. |
| **Third Party Good Senders** | A sender group in Symantec Messaging Gateway that lets administrators add multiple lists of Good Senders that third-party services compile. |
| **TLS (Transport Layer Security)** | A protocol that provides communications privacy over the Internet that uses symmetric cryptography with connection-specific keys and message integrity checks. TLS provides some improvements over SSL in security, reliability, interoperability, and extensibility. See also SSL. |
| **Transformation Engine** | A component of a Symantec Messaging Gateway Scanner that performs actions on messages. |
true file type recognition
A technology that identifies the actual type of a file, whether or not the file extension matches that type. In Symantec Messaging Gateway, you can specify filtering actions based on the true file type or true file class of a file. Or you can filter based on the file name or extension.

unscannable
In Symantec Messaging Gateway, a message can be unscannable for viruses for a variety of reasons. For example, unscannable files exceed the maximum file size or maximum scan depth that is specified. Compound messages such as compressed files that contain many levels may exceed the maximum scan depth. You can configure how unscannable messages are processed.

virus
A piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or present on a diskette. The source of the file you are downloading or of a diskette you have received is often unaware of the virus. The virus lies dormant until circumstances cause the computer to execute its code. Some viruses are playful in intent and effect, but some can be harmful, erasing data or causing your hard disk to require reformatting.

worm
A special type of virus. A worm does not attach itself to other programs like a traditional virus, but creates copies of itself, which create even more copies.
Symbols
7-bit MIME 677
8-bit MIME 677

A
actions
  combining, limits on
  processing limits, matrix of 830
content filtering policies 333, 347
  multiple
  content filtering policies 347
policy group precedence 203
address masquerading
  adding 93
  configuring 89
  editing 93
  ignoring text casing in addresses 95
  importing list 94
  probe accounts 93
address resolution
data source
  adding 508
  disabling 548
  editing 548
  enabling 548
  queries 527
  service communication errors 508
data source query
  creating custom 527
  modifying 548
function 512
queries
  creating 527
  editing 548
  enabling 548
administration settings
  Ethernet 41
  Scanner 54
administrator
  adding 658
  administrator-only Spam Quarantine access 284
  (continued)
  deleting 668
  LDAP 658
  local 658
  managing 652
  managing notifications 432
  modifying 667
  password
    resetting 696
    strong 681, 696
  rights 658, 661
adware 204, 214
agent-config command 737, 826
alerts
  conditions 684, 688
  low disk space 684
  setting up 683
  SMTP authentication 110
  types 684
aliases and distribution lists
  adding 91
  configuring 89–90
  details, examples 92
  editing 91
  ignoring text casing in addresses 95
  importing 92
  notification
    enabling 307
    spam 303
  spam addressed to 304
Allowed Sender Lists. See good sender groups
annotations. See content filtering
antispam filters 248
  See also spam
  about 248
  language-based 201–202
antivirus 204
  See also malware
  See also virus
  engine 206
  filters 204
appliances 703
  See also MTA, managing
  backing up 706, 709
  maintaining 698
  restarting 699
  restarting with DRAC 874
  restoring 701, 711
  returning to factory defaults 700
  turning off 701, 703
application certificate
  deleting 182
  editing 182
  exporting 181
architecture, Symantec Messaging Gateway 27
archive messages 417
artificial intelligence (static and dynamic) 206
artificial intelligence settings 206, 235
attachment
  container files 228
  encrypted 204
  suspicious 204, 214
attachment lists. See content filtering
attack
  about 141
  about detecting 204
  configuring 215
  email virus detection 147
  technologies that detect 206
Audit ID 638
authentication
  data source
    adding 502
    disabling 541
    editing 541
    enabling 541
    queries 518, 541
    service communication errors 502
  data source query
    creating custom 518
    modifying 541
  Enforce Server 453
  function 510
  queries 518
B
backup
  log data 713
  managing 705
  on demand 709
backup (continued)
  restoring 701, 711
  scheduling 706, 709
bad message
  handling 53
  queue 53
bad sender groups
  about 141
  adding members 130
  choosing actions 129
  deleting senders 131
  editing members 131
  enabling, disabling
    groups 128
    members 132
  end user lists 201
  exporting data 135
  impact of Connection Classification on 143
  import file formats 133
  importing data 132
  overview 151
  sender identification methods 136
  use case 151
best practices
  data directory services
    scalability 570
    security 569
  FIPS 882
  passwords 697
  SMTP authentication 110
  Spam Quarantine 311
blacklists. See third party sender lists
Blocked Sender Lists. See bad sender groups
Bounce Attack Prevention
  configuring 159, 162
  creating a seed value 161
  overview 160
  spam policies 163
Brightmail
  ARM (Adaptive Reputation Management) 141
  engine
    about 73
    enabling, disabling 71, 610
  IQ Services 141
C
CA (Certificate Authority) certificate. See certificate
cache. See directory data source, cache
cache persistence 563
cache settings, directory data source 566
cat command 739
cc-config command 740
certificate
  application 180, 182
  assigning 169, 185
  assigning user interface HTTPS 186
Certificate Authority signed
  about 169
  accessing the Control Center 675
  adding 173, 175
  backing up 179
  importing 177
  modifying 175
  PEM format requirements 183
  replacing 178
  requesting 176
configuring 169
Control Center 676
Data Loss Prevention 180
deleting 185
exporting 181, 184
HTTPS 169, 184–186
importing 180
MTA TLS 169, 185
PEM format 183
renaming 179
self-signed 169, 173, 179, 183, 675
SMTP/TLS 184–185
viewing 176, 184
working with 171
clear command 743
command line interface 721, 730, 733, 766, 803
commands
  agent-config 737
  cat 739
  cc-config 740
  clear 743
  db-backup 744
  db-restore 749
  delete 752
diagnostics 757
dns-control 762
fipsmode 764
grep 765
help 766
ifconfig 773
iostat 774
ip 775
commands (continued)
  ldapsearch 776
  list 777
  mallog 779
  malquery 781
  monitor 787
  more 793
  mta-control 794
  netstat 800
  nslookup 801
  password 802
  patch 803
  ping 805
  ping6 806
  reboot 807
  route 808
  rpmdb 809
  rsa-key 810
  service 811
  show 814
  shutdown 815
  sshd-config 816
  symdiag 819
  tail 721, 821
telnet 824
  traceroute 825
  traceroute6 826
  update 827
compliance. See content filtering
conditions
  based on message parts 842
  consideration 327
  creating in content filtering policies 328
  match criteria 330
  negative 842
Conduit
  about 73
  starting, stopping 71, 610
Connection Classification
  about 141
  configuring 145
  default settings 146
  disabling 145
  enabling 145
  how it works 143
  impact on sender groups 143
  learning mode 143, 145
  connection time processing 141
  container limit 204, 228
content compliance. See content filtering
content encryption
  about 449
  setting up 449
content filtering 327, 474
  See also conditions
  See also Data Loss Prevention Network Prevent integration
  about 322
  annotations
    creating 399
    deleting 399
    editing 399
  archiving
    incidents 436
    messages 417
attachment lists
  about 401
  creating 411
  deleting 414
  editing 413
  provided with product 402
  working with 400
content incident folders
  about 419
  creating 422
  deleting 425
  editing 425
  expunging 420, 426
  Hold for Review (Content Quarantine) 419
  Informational Incidents 419
  managing 418, 427
  monitoring 427
  spam option 426
  submitting spam for rules 443
  viewing contents 433
creating 325
dictionaries
  about 382
  creating 387
  deleting 390
  deleting words and phrases 389
  disabling words and phrases 386
  editing 388
  exporting words and phrases 385
  finding words and phrases 390
  importing words and phrases 388
  provided with product 391
content filtering (continued)
dictionaries (continued)
  scanning non-plaintext file attachments 385
  working with 380
filtering, language-based 202
header markup 488
incidents
  about 429
  acting on 434–435, 444
  archiving 436
  changing severity 446
  creating notifications 430
  creating using Symantec Network Prevent
    header markup 488
  deleting 442
  exporting 440
  forwarding 441
  updating status 445
  viewing 433, 447
matching text 449
multiple policies 347
notifications
  about 377
  creating 377
  deleting 380
  editing 379
  incidents 430
  variables 377, 423
  working with 376
patterns
  about 395
  creating 397
  deleting 398
  editing 398
  managing 395
Perl-compatible regular expressions 414, 416
policies
  actions 332–333
  applying to policy groups 346
  assigning to policy groups 200
  conditions 327, 330, 842
  considerations 328
  copying 323
  enabling or disabling 323
  fine-tuning 351
  order of evaluation 323
  setting up content encryption 449
  troubleshooting 351
content filtering (continued)
records
  about 354
  data source file 355
  deleting 369
  mapping data source file fields 360–361
  modifying 368
  replicating 367
  structured data 354
  system patterns 360–361
  uploading data source files 366
  using in policies 354
  views 369, 373–375
reports 582
scanning non-plain text file attachments 385
setting up content encryption 449
views. See content filtering, records
content incident folders. See content filtering
Content Quarantine. See content filtering
Control Center
  Bounce Attack Prevention 161
certificate for 169, 675–676
configuring 668
DNS 672
error log 618
host access 672
IP address 70
IPv6 host access 672
licensing 714–715
listener port 675
logging on and off 681
logs 614
preferences 679
relicensing 716
security warning 675
simultaneous access 671
user logon help 680
customer-specific spam rules. See spam: custom rules

D
Dashboard
  contents 603
  threat categories 605
data directory services
  creating a data source 496
  limiting server access 569
  security 569

Data Loss Prevention
  about 470
  integrating with Symantec Messaging Gateway 470
  Network Prevent. See Data Loss Prevention Network Prevent integration
Data Loss Prevention Network Prevent integration 474
  See also content filtering
  about 474
  blocking messages 477
  bypass mode 478, 481
  configuring 481, 486
  forwarding 478
  maintenance 489
  message queues 478
  multiple Scanners 476
  performance 483
  ports 475–476, 486
  preference 484
  redirecting messages 477
  reflecting 478
tagging, message 477
TLS encryption 486
troubleshooting 478, 483, 485
data sources and functions 499
  See also directory data source
date format 677–678
day-zero protection 206
db-backup command 744
db-restore command 749
DBCS 676
defaults
  Connection Classification 146
  email virus policy actions 197
  features 29
  internal hosts list 66
  malware policy actions 196
  policies 29
definitions
  disabling automatic updates 233
  on demand 234
  platinum 234
  scheduling 232
  source
    LAN host 234
    Symantec 234
  status 232
  updating 206, 231
delete command 752
delivery
  Spam Quarantine
    misidentified messages 299
    undeliverable messages 309
  starting, stopping 71
  Suspect Virus Quarantine 237
Dell Remote Access Controller (DRAC) 877–878. See DRAC
denial-of-service attack
  Bounce Attack Prevention 160
  container limits 228
deployment
  advantages at gateway 65
  non-gateway 65
  sender group policies 66, 151
diagnostics 722–723, 725–726, 728–729, 877
diagnostics command 757
dialers 214
dictionary. See content filtering
directory data cache
  about 562
  preloader 564
  setting the cache 562
directory data service
  about 492
  about distribution list expansion 532
  about preserving recipient addresses 532
  about sources and functions 499
  address resolution 512
  authentication 510
  cache preloader 564
  recipient validation 513
  routing 511
  scalability 570
directory data source
  about modifying 535
  adding 496
  address resolution 508, 548
  address resolution queries 527
  advanced settings 558
  authentication 502, 541
  authentication queries 518
  cache
    about 562
    best practices for scalability 570
    configuring advanced settings 566
    deleting 538
    disabling 538
directory data source (continued)
  editing 539
  editing LDAP server configuration 539
  enabling 538
  modifying 534
  modifying address resolution queries 548
  modifying authentication queries 541
  modifying recipient validation queries 556
  modifying routing queries 553
  preserving recipient addresses 534
  recipient validation 500, 556
  recipient validation queries 517
  routing 506, 553
  routing queries 524
  service communication errors 496
directory data source functions
  adding 498
  address resolution 512
  authentication 510
  recipient validation 513
  routing 511
directory data source queries
  about 514
  query syntax 514
directory data sources
  about 499
  features that rely on 492
directory harvest attacks
  about 141
  configuring recognition 149
Disarm 206
disk space
  clearing 625
  managing 703
distribution list expansion
  enabling and disabling for data sources 533
  expanding and preserving recipient addresses 531
distribution lists. See aliases and distribution lists
DKIM
  adding domain key 126
  enabling DKIM signing 123
  importing domain key 127
dns-control command 762
documentation, product 30
domain key
  adding 126
  importing 127
  PEM format 183
domain key  \textit{(continued)}
renaming 179
Domain Name System (DNS) servers 36
domains
about 80
configuring 79
deleting 87
enabling DKIM signing 123
for outbound mail acceptance 51
importing 85
local 82
See also local domains
non-local 82
reverse DNS 79
specifying for sender groups 136
specifying which to accept 80
double-byte character sets 676
DRAC 872
configuring 875
deleting 877
installing 875
installing an image 876
restarting
forcefully 874
gracefully 874
restoring 878
viewing diagnostics 877
duplicate messages, Spam Quarantine 309

E
early release 461
email. See content filtering. See spam. See virus
email addresses, identifying for groups 136
email aliases. See aliases and distribution lists
email authentication
  DKIM
    enabling signing 123
  SMTP authentication 106
e-mail domains 79
email filtering 204, 248, 322
  See also content filtering
  See also spam
  See also virus
inbound diagram 101
overview 100
phases 101
email message flow
inbound diagram 101
overview 100
email message flow \textit{(continued)}
phases 101
email settings, Scanner 42
email traffic. See gateway
e-mail virus attack
about 141
  configuring recognition 147
encoding 676
encrypted attachment 204
encryption 80
  See also TLS encryptionende-mail virus attack
end user settings
  configuring 201
  enabling, disabling 201
  requirements for 202
Enforce Server
about 470
  configuring authentication 453
  integrating 471
  synchronizing with 453
errors, Spam Quarantine 309
Ethernet settings
addresses
IPv4 39
IPv6 40
advanced 41
Expungere
  content incidents folders 420
  logs 614, 620
  Spam Quarantine 288

F
factory defaults, restoring 700, 878
fallback encoding 676
false positive spam messages 258, 290, 299
Fastpass
about 141
  configuring 156
  enabling, disabling 156
  how it works 154
favorite reports
  deleting 580
  generating automatically 581
features
  default settings 29
  product 25
Federal Information Processing Standard (FIPS). See
  FIPS
filters 204, 248
See also spam
See also virus
dead user 201–202
improving 263–264
language-based 201–202
overview 100
policy group precedence 203
FIPS
about 879
best practices 882
certificates 882
certified cryptographic modules 879
checking the status 884
command line 764
installing or upgrading 881
limitations 883
turning on and off 884
fipsmode command 764
folders, content filtering. See content filtering
formats, time and date 677–678
G
gateway
deployment considerations 65
managing traffic 140
Global Intelligence Network 141
global reputation 151
good sender groups
about 141
adding members 130
choosing actions 129
deleting senders 131
editing members 131
enabling, disabling
  groups 128
  members 132
dead user lists 201
exporting data 135
impact of Connection Classification on 143
import file formats 133
importing data 132
overview 151
reasons to use 153
sender identification methods 136
grep command 765
groups, policy. See policy groups
H
hacking tools 214
hardware
  information about 608
  monitoring 607
  status 609
headers
  Spam Quarantine
    searching 296
    viewing 298
  Suspect Virus Quarantine 245
help
  Symantec Messaging Gateway 30
  user logon help 680
help command 766
hosts
  accessing the Control Center 672
  adding 35
  advanced configuration settings 41
  configuration settings 39–40
  disabling 68
  enabling 68
  internal mail hosts 65
  modifying 67
  services 73
  SMTP settings 694
  starting 68
  status 610
  stopping 68
  turning off 703
HTTPS
  Control Center 186
  user interface certificate 169, 186, 675–676
I
ifconfig command 773
inbound SMTP settings
  about 43
  changing 46
  delivery 48
  restricting acceptance 47
incident folders. See content filtering
incidents. See content filtering
Informational Incidents. See content filtering
internal mail hosts 65
internal mail servers 151
invalid recipient
  accepting all 99
  dropping 99
invalid recipient  (continued)
overview 98
rejecting 99
reports 582
iostat command 774
IP address
change Control Center IP address 70
configuring 39–40
IPv4 39
IPv6 33, 40
researching reputation 163
specifying for sender groups 136
ip command 775
IP connections reports 582
IPv4. See IP address
IPv6. See IP address

J
joke programs 214

L
LAN host 234
language encoding 240, 286
language identification
configuring 202
end user 201
LDAP 282
See also Spam Quarantine
postmaster mailbox 294
LDAP server configuration, editing 539
ldapsearch command 776
license 714–716
list command 777
listener port 675
lists
aliases and distribution lists
about 90
adding 91
details, examples 92
editing 91
importing 92
importing local routes/domains list 82
lists, attachment 401
See also content filtering
LiveUpdate  (continued)
service
disabling 610
enabling 610
source 234
starting, stopping 71
local domains 87
See also domains
about 80
configuring 82
importing 85
specifying which to accept 80
local reputation 151
local routes list 82
locale 676
logon
bypassing credentials 681
Spam Quarantine, troubleshooting 309
logs 634
See also message audit logging
about 614
backing up 713
Control Center 618
database size 620
directory data service 624
disk space alerts 625
local Scanners 622
logging levels 622
manually deleting 624
monitoring 612
purging 620
remote Scanners 622
remote syslog 627–628
saving 619
Scanner 624
settings 628
syslog 628–630, 632–633
system performance 622
types 615
viewing 617

M
mail flow 645
See also MTA
about 27
inbound diagram 101
managing 74
omitted verdicts 840
overview 100
mail flow (continued)
phases 101
starting, stopping 71, 74
stopping 645
mail hosts, internal 65
MAL. See message audit logging
malicious attack
denial-of-service 228
detecting 204, 206, 215
zip bomb 228
mallog command 779
malquery command 781
malware 214
See also virus
detecting 204
managing policies 222
policies
assigning to policy groups 196
copying 224
creating 217
default 218
default actions 196
deleting 224
disabling 223
enabling 223
modifying 222
reports 582
verdicts 214
marketing mail 248
masquerade list
adding, editing 93
importing 94
mass-mailer worm 204
message audit logging
working with 634
message flow
inbound diagram 101
managing 74
omitted verdicts 840
overview, email 100
phases 101
reducing volume 141
starting, stopping 71, 74
Message ID 296, 639
message queues (continued)
mail flow 645
managing 74
searching 643
starting, stopping 74
status 647
viewing 643
message reports 582
messages
archiving 417
dropping invalid recipients 99
rerouting 643
Spam Quarantine
duplicate 309
false positives, who to notify of 290
maximum allowed 309
message retention period 289
misidentified 299
navigating 282
postmaster mailbox 294
retention period 288
searching 296–297
thresholds 287
viewing 292
starting, stopping 71, 74
Suspect Virus Quarantine
navigating 238
releasing 244
retention period 241
searching 245–246
viewing 243
misidentified spam messages 290, 309
monitor command 787
more command 793
MTA
about 73
managing 74
message queue behavior 74
operations 71
starting 71, 610, 645
stopping 71, 610, 645
TLS certificate 169, 185
viewing the service status 610
mta-control command 794

N
netstat command 800
Network Time Protocol (NTP) servers 37
network utilities 724
network, sender group policy considerations 66, 151
newsletter 248
non-local domains. See domains, non-local
non-plain text file attachments 385
notification
  content filtering violations 377
  remediating actions 432
  Spam Quarantine
    choosing the format 308
    editing the template 305
    frequency of 301
nslookup 724
nslookup command 801

O
outbound SMTP settings
  about 43
  changing 50
  delivery 52
  domains to accept mail from 51

P
password
  best practices 697
  bypassing 681
  managing 695
  resetting 696
  strong 681, 696, 698
password command 802
patch command 803
patterns. See content filtering
PEM, format requirements 183
performance versus effectiveness 154
Perl-compatible regular expressions 414, 416
ping 724
ping command 805
ping6 command 806
platinum virus definitions. See definitions
policies 204, 248, 322
  See also content filtering
  See also spam
  See also virus
  assigning
    content filtering 200
    language 202
    malware 196
    spam 198
    virus 197

policies (continued)
  defaults 29
  end user 201–202
  language-based 201
  managing malware 222
  policy group precedence 203
  threat defense, about 460
  threat defense, default 461
  threat defense, secure preview 463
  virus, default 218
policy groups
  assigning policies
    content filtering 200, 346
    language 202
    malware 196
    spam 198
  creating 189
  default policies 29
  deleting 195
  editing 195
  enabling, disabling 195
  end user settings 201–202
  managing 195
members
  adding 191
  deleting 192
  exporting 193
  importing 193
outbound, inbound effects of 188, 656
overview 188, 656
precedence 188, 203, 656
user, finding 194
port 675
postmaster mailbox 294
precedence, policy group 203
probe accounts
  about 314
  address masquerades 90, 315
  alias addresses 90, 315
  creating 316
  creating from invalid recipient email
    addresses 318
  creating manually 319
  deleting 321
  enabling 320
  filtering spam 314
  guidelines for creating 315
  reports 582
  running a report 578
probe accounts (continued)
Symantec Probe Network 313
tracking data for 576
tracking in reports 316
Probe Network 141
probe participation 317
proxy
adding 38
editing 38
LAN host 234
purge 420
See also Expunger
content incidents folders 420
logs 620
Spam Quarantine 288–289
Suspect Virus Quarantine 241
Q
Quarantine Incidents. See content filtering
Quarantine, Content. See content filtering
Quarantine, Spam. See Spam Quarantine
Quarantine, Suspect Virus. See Suspect Virus Quarantine
queries, for data sources 514
queues. See message queues
R
reboot command 807
recipient address preservation 534
recipient validation
adding a directory data source 500
configuring 99
editing a data source 556
enabling an existing directory data source 556
function 513
overview 98
queries 517
recipient validation data source
adding 500
editing 556
enabling, disabling 556
queries
creating and testing 517
enabling, disabling 556
modifying 556
service communication errors 500
records. See content filtering
redirect URL 248
registration
Control Center 714–715
Scanner 714–715
regular expressions, Perl-compatible 414, 416
regulatory compliance 322
release notes 720
release, message
from Spam Quarantine 299
from Suspect Virus Quarantine 244
remote access programs 214
remote server logs 627
replication of Scanners 682
reports
configuring data retention period 577
content filtering 582
creating 578
Data Loss Prevention Network Prevent integration 483
data tracking
retention 577
what to track 576
deleting 580
emailing 578
favorites
deleting 580
generating automatically 581
generating automatically 581
generating
automatically 581
graphs 597
invalid recipient reports 582
invalid recipients 582
IP connections 582
layout 597
malware 582
message 582
overview 575
probe accounts 582
purging 577
spam 582
summary 582
tables 597
troubleshooting 595
reputation
global 151
local 151
researching 163
resources 141, 156, 840
resources, content filtering. See content filtering
restore
  factory defaults 700
  from different IP address 701
  from local backup 711
retention
  Spam Quarantine
    message retention period 288
    retention period 289
  Suspect Virus Quarantine
    retention period 241
reverse DNS 79
route command 808
routing
  data source
    adding 506
    disabling 553
    editing 553
    enabling 553
    queries 524, 553
    service communication errors 506
  data source query
    creating custom 524
    modifying 553
    function 511
    queries 524
rpmdb command 809
rsa-key
  command line 810
rsa-key command 810
rules. See spam

S
scalability, directory data service integration 570
Scanners (continued)
  logs 614
  managing mail flow 74
  modify SMTP settings for 45
  modifying 67
  NTP time servers 37
  proxy 35, 38
  relicensing 716
  replicating 682
  services
    about 73
    starting, stopping 71
  SMTP advanced settings 54
  SMTP settings
    about 43
    inbound 46
    inbound delivery 48
    outbound 50
    outbound delivery 52
    restricting acceptance 47
    starting 68
    stopping 68
    time settings 35, 37
    turning off 703
scheduled tasks
  locations in Control Center 649
  monitoring 648
  setting scheduled task failure alerts 648, 693
  viewing status of 648
search
  Spam Quarantine
    criteria and tips 297
    headers 296
    messages 296
  Suspect Virus Quarantine
    criteria and tips 246
    headers 245
    messages 245
    words or phrases in content filtering
      dictionaries 390
security for data directory integration
  best practices 569
security risks 214
self-signed certificate
  about 169
  adding 173
  renaming 179
sender groups
  about 141
sender groups (continued)
  adding members 130
  choosing actions 129
  deleting senders 131
  editing members 131
  enabling, disabling
    groups 128
    members 132
  end user lists 201
  exporting data 135
  impact of Connection Classification on 143
  import file formats 133
  importing data 132
  managing members 129
  overview 151
  sender identification methods 136
sender policies
  about 141
  choosing actions 129
senders
  adding to sender groups 130
  bad sender groups 151
  deleting from sender groups 131
  editing lists 131
  enabling, disabling 132
  exporting from senders groups 135
  importing into sender groups 132
  sender identification methods 136
service command 811
services
  about 73
  monitoring 607
  proxy 38
  Scanner 71
  status 610
settings 248
  See also spam
  Domain Name System (DNS) 36
  end user 201–202
  hosts 54
  Network Time Protocol (NTP) 37
  proxy 38
  Scanners 36, 39–41, 54
  Scanners, email
    about 43
    inbound 46
    inbound delivery 48
    outbound 50
    outbound delivery 52
settings (continued)
  Scanners, email (continued)
    outbound mail acceptance 51
    restricting acceptance 47
  SMTP
    about 43
    advanced 54
    inbound 46
    outbound 50
    static routes 39–41
    show command 814
    shutdown command 815
  SMTP
    advanced settings
      configuring 54
      delivery 61
      delivery bindings 62
      inbound 56
      outbound 58
    bad message handling 53
    host settings 694
    inbound Scanner settings
      about 43
      configuring 46
      delivery 48
      restricting acceptance 47
    message audit logging 634
    message queues 642
    outbound mail acceptance 51
    outbound Scanner settings
      about 43
      configuring 50
      delivery 52
    validation 111
  SMTP authentication
    about 102
    best practices 110
    configuring 103, 106
    creating a data source 502
    editing a data source 541
    overview 103
    queries
      creating custom 518
      modifying 541
  SNMP 673
  software
    licensing 714–715
    monitoring 607
    relicensing 716
software (continued)
update notes 720
updating 717, 720–721
version 721
spam 248
See also policies
See also policy groups
See also Spam Quarantine
about 248, 250
bypassing scanning 156
custom rules
about 265, 267
configuring 268
deleting 278
enabling and disabling 269
monitoring submissions 437
submission aggressiveness 272
submitter ID 270
submitters 273, 275
submitting messages 265, 277, 302, 426, 443
troubleshooting 267
directory harvest attacks 149
exempting senders from spam scanning 154
language-based filtering 201–202
policies
assigning to policy groups 198
Bounce Attack Prevention 163
copying 261
creating 256
deleting 262
enabling and disabling 259
modifying 260
preconfigured 250
reports 582
scanning text-based attachments 256
suspected spam threshold, configuring 262
unwanted email 259
spam filters 248
See also spam
Spam Quarantine (continued)
differences between administrator and user
pages 291
distribution lists, aliases 304
duplicate messages 309
errors 309
false positives 299
language encoding 286
logs 615
messages
deleting 300
false positives, who to notify of 290
headers, viewing 298
language encoding 286
maximum number of 309
misidentified 299
number of entries on message list page 295
postmaster mailbox 294
searching 296–297
searching tips 297
sorting 296
submitting for custom rules 302
viewing 292
misidentified messages 299
navigating 282
notification
about 303
enabling 307
false positives, who to notify of 290
message template 303
modifying the template 305
selecting the format 308
to users 301
variables 307
number of entries on message list page 295
postmaster mailbox 294
purging 288–289
retaining messages 288–289
thresholds 287–288
troubleshooting 309
undeliverable messages 309
unresolved email addresses 282
user logon help 680
viewing 282, 292
viewing messages 291
working with messages 294
spyware 204, 214
sshd-config command 816
SSL 569
static routes 39–40

status
  about 602
  Dashboard 603
  hardware information 608
  hardware status 609
  logs 614
  message queue size 647
  queued messages 642
  services 610
  SMTP 602
  spam email submissions 437
  system 602

structured data. See content filtering

summary reports 582

Suspect Virus Quarantine 237
  See also virus
  about 237
  language encoding 240
  messages
    deleting 243
    language encoding 240
    number of entries on message list page 240
    releasing 244
    searching 245–246
    searching tips 246
    sorting 243
    viewing 243
    working with 242
  navigating 238
  number of entries on message list page 240
  purging 241
  retaining messages 241
  size, maximum 241
  viewing 243

suspicious attachment 204, 214

Symantec Content Encryption. See content encryption

Symantec Mail Security. See Symantec Messaging Gateway

Symantec Messaging Gateway 24, 875
  See also best practices
  See also DRAC
  about 24
  architecture 27
  features 25
  FIPS compliance 879
  how viruses are detected 206
  information, where to get 30
  integrating with Enforce Server 471

Symantec Messaging Gateway (continued)
  keeping current 713
  licensing 714–715
  logs 614
  product documentation 30
  relicensing 716
  software
    updating 721
    version 721
  status 602
  troubleshooting 723
  updating software 717

Symantec Network Prevent integration
  bypass mode 479, 482
  configuring 486, 488
  message queues 479
  policies 482, 488
  ports 486
  troubleshooting 479

Symantec Probe Network 313

Symantec Security Response 141, 263

symdiag command 819

syslog. See logs, syslog

system
  administrator. See administrator
  locale 676

system patterns 360–362

T
  tail command 721, 821
  telnet command 824

third party sender lists
  specifying for sender groups 136
  using to block messages 151

threat categories 605

threat defense
  policies
    about 460
    default 461
    secure preview 463
  reports 582
  scan settings
    configuring 458
    excluding file types from scanning 460

threshold
  content incidents folders 420
  Spam Quarantine 287–288
  Suspect Virus Quarantine 241

time format 677–678
TLS certificate 169, 184–185
TLS encryption
  best practices, SMTP authentication 110
  enforcing on inbound 82
  inbound Scanner settings for 46
  outbound Scanner settings 50
  per domain for routing, delivery 80
  specifying per non-local domain 82
traceroute 724
traceroute command 825
troubleshoot
  reports 595
  Spam Quarantine 309

U
undeliverable spam messages 309
Uniform Resource Identifier (URI). See URI (Uniform Resource Identifier)
unresolved email addresses 309
unscannable container limit 228
untested verdict 640
unwanted email
  definition 259
  filtering 248
  reducing false positives 258
update
  command 827
  definitions 231
UPS monitoring 701
URI (Uniform Resource Identifier) 263
URL reputation filtering 264
user groups. See policy groups
user interface certificate, HTTPS 169, 675
user, finding in a policy group 194

V
variables, notification messages 307, 423
  verdicts
    by category 836
    filtering actions available
      content filtering 333
    omitted from processing 840
    policy group precedence 203
    spyware or adware verdict 214
    untested 640
views. See content filtering, records
virtual IP address (continued)
  IPv6 40
  virus 214
  See also malware
  artificial intelligence settings 206, 235
  category and default actions 197
  container limits 228
  definitions
    LiveUpdate 231
    managing 230
    on demand 234
    platinum 234
    Rapid Response 231
    source 234
    status 232
    updating 231
detecting 204, 215
exclude files from scanning, list
  creating 225
  deleting 228
  disabling 227
  enabling 227
  exporting 228
  modifying 226
  working with 224
message settings 239
techologies that detect 206
virus attack recognition
  about 141
  configuring 147, 204, 215
  disabling 147
  enabling 147
  how viruses are detected 206

Z
zip bomb. See container limit