Symantec Brightmail™ Gateway 8.0 Administration Guide
Symantec Brightmail™ Gateway 8.0 Administration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 8.0

PN: 20002719

Legal Notice

Copyright © 2009 Symantec Corporation. All rights reserved.

Symantec, the Symantec 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product feature and function. The Technical Support group also authors content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec’s Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

**Licensing and registration**

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals
Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

- **Symantec Early Warning Solutions**: These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.

- **Managed Security Services**: These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

- **Consulting Services**: Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.

- **Educational Services**: Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.
Technical Support ................................................................................................................. 4

Chapter 1  Introducing Symantec Brightmail Gateway ................... 21

About Symantec Brightmail Gateway .............................................................. 21
What's new in Symantec Brightmail Gateway ........................................ 22
Components of Symantec Brightmail Gateway ........................................ 24
  About the Symantec Brightmail Gateway software components .................. 27
  About the Symantec Brightmail Gateway hardware component ................ 28
How Symantec Brightmail Gateway works ........................................ 28
What you can do with Symantec Brightmail Gateway ...................... 31
Where to get more information ............................................................... 34

Chapter 2  Understanding message flow ............................................. 35

About email message flow ........................................................................ 35
  Email message flow phases .............................................................. 36
  Inbound SMTP connection phase processing details ....................... 39
  Inbound SMTP session phase processing details ............................ 41
  Inbound message filtering phase processing details ....................... 43
About outbound message flow .................................................................. 45
  Outbound SMTP connection phase processing details .................... 45
  Outbound SMTP session phase processing details .......................... 46
  Outbound message filtering processing details ............................... 48
Message routing phase processing details ........................................... 50
Message delivery phase processing details .......................................... 51

Chapter 3  Understanding message filtering ..................................... 53

About filtering ......................................................................................... 53
Filtering actions and verdicts for email messages .............................. 56
Filtering actions and verdicts for instant messages ............................. 60
Multiple actions per verdict ................................................................. 61
Verdict and action combinations ......................................................... 62
About multiple content compliance policies ..................................... 63
Chapter 6

Blocking and allowing messages at connection time ........................................... 131

About blocking and allowing messages at connection time ......................... 132
About managing connection load at the gateway ........................................ 134
Configuring Connection Classification ......................................................... 136
Connection class default settings ................................................................. 138
Configuring email virus attack recognition ................................................ 138
Configuring directory harvest attack recognition ....................................... 140
About blocking and allowing messages using sender groups ..................... 143
Enabling or disabling good and bad sender groups .................................... 147
Choosing actions for good and bad sender groups .................................... 147
Adding senders to administrator and third party sender groups ................. 148
Editing good and bad sender group members .......................................... 149
Deleting good and bad sender group members ......................................... 149
Enabling or disabling good and bad sender group members .................... 149
Importing good and bad sender group entries .......................................... 150
Sender group import file formats ................................................................. 151
Exporting sender group information .......................................................... 153
Supported methods for identifying senders .............................................. 154
About conserving resources using Fastpass ............................................... 155
Configuring Fastpass .................................................................................. 157
About defending against bounce attacks ................................................. 159
Configuring your Control Center for bounce attack prevention ................. 161
Configuring your groups for bounce attack prevention ............................ 161
Chapter 7  Detecting viruses and malicious attacks  

Creating email virus policies .......................................................... 179
Spyware or adware verdict details .................................................. 180
Modifying email virus policies ....................................................... 181
Enabling or disabling email virus policies ..................................... 182
Deleting email virus policies .......................................................... 183
Copying email virus policies .......................................................... 183
Excluding file types from virus scanning ....................................... 184
Modifying the file types to exclude from scanning ....................... 186
Enabling or disabling the lists of file types to exclude from scanning .................................................. 187
Deleting lists of file types to exclude from scanning ..................... 187
Exporting lists of the file types to exclude from scanning ............... 188
Modifying the heuristic level .......................................................... 189
Configuring container settings ....................................................... 189
About updating virus definitions .................................................... 191
Viewing the status of your virus definitions .................................. 193
Scheduling automatic virus definition updates ............................ 193
Disabling automatic virus definition updates ............................... 194
Initiating virus definition updates on demand .............................. 194
Specifying from where to obtain virus definitions ....................... 195
Obtaining definitions when a new, emerging threat is discovered .................................................. 196

Chapter 8  Quarantining suspected viruses  

About quarantining suspected viruses ............................................. 199
Viewing suspect virus messages in quarantine ............................... 200
Choosing the language encoding for suspect virus messages .......... 201
Specifying the number of suspect virus message entries to view per page .................................................. 201
About navigating Suspect Virus Quarantine ................................. 202
Sorting suspect virus messages in quarantine ............................... 203
Chapter 9 Filtering spam ................................................................. 209
  About filtering spam .................................................................... 209
    About the default spam policies .............................................. 210
  Creating email spam policies ..................................................... 211
  Enabling and disabling spam policies ......................................... 213
  Modifying spam policies ......................................................... 213
  Copying spam policies ............................................................. 214
  Deleting spam policies ............................................................. 215
  Identifying messages written in specific languages .................... 215
  Configuring the threshold for suspected spam identification .......... 216

Chapter 10 Quarantining spam ....................................................... 219
  About quarantining spam ........................................................ 220
  Before you use Spam Quarantine ................................................. 220
  Forwarding spam messages for non-existent addresses to quarantine ........................................ 221
  Configuring Spam Quarantine for administrator-only access .......... 222
  Viewing spam and suspected messages in quarantine ................. 223
    How Spam Quarantine differs for administrators and users ...... 224
  Viewing spam and suspected spam messages sent to the postmaster mailbox .................................. 225
  About navigating Spam Quarantine ............................................. 226
  Specifying the number of entries to appear on the Spam Quarantine Message list page ....................... 227
  Sorting spam and suspected messages in quarantine by date .......... 227
  Redelivering messages misidentified as spam .......................... 228
  Deleting spam messages in quarantine ....................................... 229
  Searching quarantined spam messages ..................................... 230
    Spam message search criteria and tips .................................... 232
  Viewing spam message headers ............................................... 233
  Choosing the language encoding for spam messages .................. 233
  Modifying Spam Quarantine thresholds .................................... 234
    Spam Quarantine threshold considerations ............................. 235
  Specifying who to notify of false positive messages .................... 236
About configuring the user and distribution list notification digests ................................................................. 237
About how spam is handled when addressed to distribution lists ........................................................................ 238
Specifying when to notify users of spam messages in their quarantine .................................................................... 239
Modifying the spam notification message digest templates .............................................................. 240
Enabling notification digests for distribution lists ................................................................. 243
Selecting the notification digest format ......................................................................................... 243
Specifying how long spam messages are retained in quarantine .......................................................... 245
Specifying when and how often Spam Quarantine is purged ........................................................................ 246

Chapter 11 Filtering IM .......................................................................................................................... 251
About IM ................................................................................................................................. 251
Enabling IM filtering .................................................................................................................. 254
About spim ...................................................................................................................................... 256
About how spim works .................................................................................................................. 256
About detecting spim ..................................................................................................................... 257
About detecting known spim .......................................................................................................... 257
About detecting suspected spim ..................................................................................................... 258
Enabling spim detection .................................................................................................................. 259
About registering IM users ............................................................................................................. 259
About the IM user registration process ........................................................................................ 260
Enabling IM user registration ........................................................................................................ 260
Editing IM user registration text ................................................................................................... 261
Registering an IM user as an administrator ....................................................................................... 265
Self-registering an IM user ............................................................................................................... 266
Editing and deleting registered IM users .......................................................................................... 267
Blocking access to an IM network .................................................................................................... 269
About default IM virus policies ......................................................................................................... 271
Creating IM virus policies ................................................................................................................ 272
Creating IM spim policies ................................................................................................................ 274

Chapter 12 Configuring email content filtering and compliance .......................................................... 279
About content filtering ...................................................................................................................... 279
About regulatory compliance ........................................................................................................... 280
About configuring compliance policies ............................................................................................ 280
Creating compliance policies .......................................................................................................... 282
Enabling and disabling compliance policies .................................................................................... 285
Determining compliance policy order .............................................................................................. 286
About compliance policy conditions ............................................... 286
Adding conditions to compliance policies ........................................ 289
About compliance policy actions ................................................... 290
About annotating messages .................................................... 291
About notifications ............................................................... 294
About archiving messages ...................................................... 298
About using compliance policy resources ........................................ 300
About compliance policy templates .......................................... 302
About dictionary resources .................................................... 305
About attachment list resources .............................................. 311
About pattern policy resources ............................................... 314
About using structured data records in policy conditions ............. 317
About creating a record resource for compliance policies ............. 318
About using regular expressions in conditions ........................... 327
About Vontu Network Prevent integration ...................................... 329
How Symantec Brightmail Gateway and Vontu Network Prevent interact ................................................................. 330
Ports used for Vontu Network Prevent integration ..................... 331
Common Vontu Network Prevent actions .................................. 331
Supported Vontu Network Prevent delivery modes ..................... 332
About performance implications for Vontu Network Prevent integration ................................................................. 333
About Vontu Network Prevent preference order ......................... 333
Configuring Vontu Network Prevent to return email to Symantec Brightmail Gateway ................................................................. 334
Configuring email connections to and from Vontu Network Prevent ................................................................................. 335
Creating an incident based on Vontu Network Prevent header markup ................................................................................. 336
About failure behavior with Vontu Network Prevent ................... 337
Correcting a delivery queue backup to Vontu Network Prevent ................................................................................. 338
Enabling or disabling bypass for Vontu Network Prevent ............. 340
Managing unscanned email if bypass is enabled for Vontu Network Prevent ................................................................................. 340
About Vontu Network Prevent reports .......................................... 341
Troubleshooting Vontu Network Prevent integration: messages bounce ................................................................................. 342
Troubleshooting Vontu Network Prevent integration: deferred messages ................................................................................. 342
Taking Vontu Network Prevent servers offline for maintenance ................................................................................. 342
Chapter 13 Monitoring and managing compliance

About monitoring compliance policies ........................................... 345
About compliance folders ............................................................. 346
  Adding compliance folders ..................................................... 348
  Editing compliance folders .................................................. 350
  Deleting compliance folders ................................................... 350
  Setting the compliance folder storage threshold ....................... 351
About incident management ........................................................ 351
  Acting upon incidents ........................................................... 352
  Forwarding and tracking incidents ......................................... 353

Chapter 14 Working with reports .................................................. 355

About working with reports ........................................................ 356
Selecting the data to track for reports .......................................... 357
Creating and configuring reports ............................................... 357
  Report types ........................................................................ 359
Saving favorite reports ............................................................ 370
Editing a favorite report's filter options ....................................... 370
Editing a favorite report's schedule ............................................. 371
Copying favorite reports ............................................................ 371
Deleting favorite reports ............................................................ 372
About generated reports layout and data ...................................... 372
Running reports on demand ....................................................... 377
Generating reports automatically ............................................... 377
Canceling scheduled reports ..................................................... 379
Emailing generated reports ........................................................ 379
  Specifying the report email notification sender and subject line ...................................................... 380
Printing generated reports .......................................................... 381
Saving generated reports ............................................................ 382
About purging report data ......................................................... 383
  Specifying how long report data is retained ................................ 383
  Specifying when and how often report data is purged ............... 384
  Deleting all report data at one time ......................................... 384
Troubleshooting report generation ............................................... 385

Chapter 15 Monitoring the status of your product ............................ 387

About monitoring the status of your product ................................ 387
About the Dashboard ............................................................... 389
  Viewing the Dashboard ......................................................... 390
Threat category components .................................................... 391
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the status of your hardware</td>
<td>392</td>
</tr>
<tr>
<td>Viewing information about your hardware</td>
<td>393</td>
</tr>
<tr>
<td>Viewing the status of software and services</td>
<td>394</td>
</tr>
<tr>
<td>About LDAP synchronization and Control Center replication</td>
<td>395</td>
</tr>
<tr>
<td>Viewing LDAP synchronization status</td>
<td>396</td>
</tr>
<tr>
<td>Synchronizing LDAP servers manually</td>
<td>398</td>
</tr>
<tr>
<td>Canceling an LDAP synchronization in progress</td>
<td>399</td>
</tr>
<tr>
<td>Troubleshooting LDAP synchronization rejection entries</td>
<td>400</td>
</tr>
<tr>
<td>Viewing Control Center replication status</td>
<td>400</td>
</tr>
<tr>
<td>Replicating the Control Center database manually</td>
<td>402</td>
</tr>
<tr>
<td>Canceling a Control Center replication in progress</td>
<td>402</td>
</tr>
<tr>
<td>About logs</td>
<td>403</td>
</tr>
<tr>
<td>Log types</td>
<td>403</td>
</tr>
<tr>
<td>Viewing log files</td>
<td>406</td>
</tr>
<tr>
<td>Saving log files</td>
<td>407</td>
</tr>
<tr>
<td>Managing the log database size</td>
<td>408</td>
</tr>
<tr>
<td>Manually deleting Scanner log files</td>
<td>410</td>
</tr>
<tr>
<td>Configuring log levels</td>
<td>410</td>
</tr>
<tr>
<td>Configuring remote logging to syslog</td>
<td>412</td>
</tr>
<tr>
<td>About message audit logging</td>
<td>418</td>
</tr>
<tr>
<td>Enabling the Message Audit Log</td>
<td>419</td>
</tr>
<tr>
<td>Searching for a message in the Message Audit Log</td>
<td>419</td>
</tr>
<tr>
<td>Exporting Message Audit Log data</td>
<td>424</td>
</tr>
<tr>
<td>About message queues</td>
<td>424</td>
</tr>
<tr>
<td>Viewing queued messages</td>
<td>425</td>
</tr>
<tr>
<td>Deleting queued messages</td>
<td>425</td>
</tr>
<tr>
<td>Flushing message queues</td>
<td>426</td>
</tr>
<tr>
<td>Stopping the mail flow</td>
<td>427</td>
</tr>
<tr>
<td>Monitoring message queue size and volume</td>
<td>428</td>
</tr>
<tr>
<td>Troubleshooting the message queue</td>
<td>428</td>
</tr>
<tr>
<td>Viewing IM users that are signed on</td>
<td>429</td>
</tr>
<tr>
<td>Viewing the connection status of your IM networks</td>
<td>432</td>
</tr>
<tr>
<td>Chapter 16 Administering your product through the Control Center</td>
<td>433</td>
</tr>
<tr>
<td>About simultaneous Control Center access</td>
<td>434</td>
</tr>
<tr>
<td>About backing up log data</td>
<td>435</td>
</tr>
<tr>
<td>Checking the Control Center error log</td>
<td>435</td>
</tr>
<tr>
<td>Running network utilities from the Control Center</td>
<td>436</td>
</tr>
<tr>
<td>Licensing your product</td>
<td>436</td>
</tr>
<tr>
<td>Viewing license statuses</td>
<td>437</td>
</tr>
<tr>
<td>Enforcing strong passwords</td>
<td>438</td>
</tr>
</tbody>
</table>
Password best practices ......................................................... 438
Strong password criteria ........................................................ 439
Adding administrators .............................................................. 439
Editing an administrator ............................................................ 441
Deleting an administrator ............................................................ 441
Administrator rights ................................................................... 442
Resetting an administrator password ............................................. 446
Configuring alert notification criteria ............................................. 447
Types of alerts ..................................................................... 447
Monitoring devices through SNMP .............................................. 450
  Downloading a Management Information Base for SNMP ............ 451
About specifying host names for Control Center access ..................... 451
  Specifying which hosts can access the Control Center ................. 452
Specifying a custom user logon help page ......................................... 453
Setting the locale encoding and fallback encoding .......................... 453
About maintaining adequate disk space ........................................ 454
Specifying SMTP host settings for product generated alerts, reports, and messages ................................................................. 454
Replicating data between the Control Center and your Scanners ......... 455
Modifying or disabling the port through which the Control Center accepts messages ................................................................. 456
About configuring certificate settings ............................................. 457
  Adding a self-signed certificate ................................................. 458
  Requesting a Certificate Authority-signed certificate .................. 459
  Adding a CA certificate .......................................................... 459
  Importing a Certificate Authority-signed certificate ...................... 461
  Changing a CA certificate name ............................................... 462
  Replacing existing CA certificates .......................................... 462
  Viewing existing CA certificates .............................................. 463
  Backing up CA certificates ..................................................... 463
  Viewing an SMTP/TLS or HTTPS certificate .............................. 463
  Deleting an SMTP/TLS or HTTPS certificate .............................. 464
  Assigning an MTA TLS certificate to a Scanner .......................... 464
  Assigning a user interface HTTPS certificate to the Control Center ................................................................. 465
  Bypassing the security warning when you access the Control Center ................................................................. 465
  Designating a Control Center certificate ................................... 466
Turning off an appliance ............................................................. 466
Gracefully turning off the appliance due to loss of power ................... 467
Restarting an appliance ............................................................. 468
Resetting an appliance to its factory defaults .................................. 468
Scheduling backups ................................................................. 469
Chapter 17 Using LDAP for Symantec Brightmail Gateway

About the supported LDAP services and directories
About the authentication service
About LDAP synchronization
  Initiating LDAP synchronization
About the LDAP routing service
About recipient validation
About Configuring LDAP settings and sources
  Configuring LDAP settings and adding source definitions
    Configuring authentication source details
    Configuring synchronization source details
    Configuring routing source details
    Configuring recipient validation source details
  Editing an LDAP source definition
  Enabling or disabling an LDAP source
  Deleting an LDAP source
About replicating data to Scanners
  Starting or stopping replication
  Troubleshooting replication
  Troubleshooting status messages

Appendix A Action and verdict combinations
  Limits on combining actions
  Action processing combinations
  User interface action combinations
  Verdict combinations

Appendix B Premium Content Compliance Resources
  Described Content Compliance policy templates
  Structured Data Compliance policy templates
  Regular expressions for context-filtering conditions
Premium attachment list resources .................................................. 529
Premium pattern resources ............................................................... 536
Premium dictionary resources ......................................................... 537
Premium regular-expression resources keyed to policy
templates ....................................................................................... 541
U.S. regulatory policy templates ...................................................... 542
    Export Administration Regulations (EAR) .................................. 544
    Gramm-Leach-Bliley ................................................................. 545
    HIPAA .................................................................................. 546
    International Traffic in Arms Regulations (ITAR) ....................... 547
    NASD Rule 2711 and NYSE Rules 351 and 472 ..................... 548
    NASD Rule 3010 and NYSE Rule 342 ................................... 548
    NERC Security Guidelines for Electric Utilities ...................... 548
    Office of Foreign Assets Control (OFAC) .................................. 549
    Payment Card Industry Data Security Standard ...................... 549
    Sarbanes-Oxley ..................................................................... 550
    SEC Fair Disclosure Regulation ............................................. 550
    State Data Privacy .................................................................. 551
Confidential data-protection policy templates .................................. 552
    Confidential Documents ......................................................... 554
    Defense Message System (DMS) GENSED Classification .......... 555
    Design Documents .................................................................. 555
    Encrypted Data ..................................................................... 555
    Financial Information ............................................................. 556
    Mergers and Acquisition Data ................................................. 556
    Price Information ................................................................... 556
    Project Data ........................................................................ 556
    Publishing Documents ............................................................ 557
    Resumes ............................................................................. 557
    Source Code ........................................................................ 557
    US Intelligence Control Markings (CAPCO) and DCID 1/7 ........ 558
Acceptable use policy templates .................................................... 558
    Competitor Communications .................................................. 559
    Gambling ........................................................................... 560
    Illegal Drugs ....................................................................... 560
    Media Files ......................................................................... 560
    Offensive Language ............................................................... 560
    Racist Language .................................................................. 561
    Restricted Files .................................................................... 561
    Restricted Recipients ............................................................ 561
    Sexually Explicit Language .................................................... 561
    Violence and Weapons ......................................................... 562
Customer and employee data-protection templates ......................... 562
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canadian Social Insurance Number</td>
<td>564</td>
</tr>
<tr>
<td>Credit Card Numbers</td>
<td>564</td>
</tr>
<tr>
<td>Customer Data Protection</td>
<td>564</td>
</tr>
<tr>
<td>Employee Data Protection</td>
<td>565</td>
</tr>
<tr>
<td>Individual Taxpayer Identification Numbers (ITIN)</td>
<td>566</td>
</tr>
<tr>
<td>SWIFT Codes</td>
<td>566</td>
</tr>
<tr>
<td>UK Drivers License Numbers</td>
<td>566</td>
</tr>
<tr>
<td>UK Electoral Roll Numbers</td>
<td>567</td>
</tr>
<tr>
<td>UK National Insurance Number</td>
<td>567</td>
</tr>
<tr>
<td>UK Passport Numbers</td>
<td>567</td>
</tr>
<tr>
<td>UK Tax ID Numbers</td>
<td>567</td>
</tr>
<tr>
<td>US Social Security Numbers</td>
<td>567</td>
</tr>
<tr>
<td>Network security policy templates</td>
<td>568</td>
</tr>
<tr>
<td>Network Diagrams</td>
<td>568</td>
</tr>
<tr>
<td>Network Security</td>
<td>569</td>
</tr>
<tr>
<td>Password Files</td>
<td>569</td>
</tr>
<tr>
<td>UK and international regulatory policy templates</td>
<td>569</td>
</tr>
<tr>
<td>Caldicott Report</td>
<td>571</td>
</tr>
<tr>
<td>Data Protection Act 1998</td>
<td>572</td>
</tr>
<tr>
<td>EU Data Protection Directives</td>
<td>573</td>
</tr>
<tr>
<td>Human Rights Act 1998</td>
<td>573</td>
</tr>
<tr>
<td>PIPEDA</td>
<td>574</td>
</tr>
<tr>
<td>Page settings for adding a compliance folder</td>
<td>574</td>
</tr>
<tr>
<td>Compliance Conditions</td>
<td>575</td>
</tr>
<tr>
<td>Attachment characteristics for attachment lists</td>
<td>579</td>
</tr>
<tr>
<td>Email notification variable attributes</td>
<td>580</td>
</tr>
<tr>
<td>Compliance condition categories</td>
<td>581</td>
</tr>
<tr>
<td>Record system patterns</td>
<td>583</td>
</tr>
<tr>
<td>Perl-compatible regular expressions</td>
<td>587</td>
</tr>
</tbody>
</table>

**Appendix C**  
Administering your product through the command line  

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>agentconfig</td>
<td>591</td>
</tr>
<tr>
<td>cat</td>
<td>593</td>
</tr>
<tr>
<td>cc-config</td>
<td>594</td>
</tr>
<tr>
<td>clear</td>
<td>594</td>
</tr>
<tr>
<td>crawler</td>
<td>595</td>
</tr>
<tr>
<td>date</td>
<td>596</td>
</tr>
<tr>
<td>db-backup</td>
<td>597</td>
</tr>
<tr>
<td>db-restore</td>
<td>597</td>
</tr>
<tr>
<td>deleter</td>
<td>600</td>
</tr>
<tr>
<td></td>
<td>602</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------</td>
<td>------</td>
</tr>
<tr>
<td>diagnostics</td>
<td>602</td>
</tr>
<tr>
<td>dn-normalize</td>
<td>604</td>
</tr>
<tr>
<td>dns-control</td>
<td>605</td>
</tr>
<tr>
<td>eula</td>
<td>605</td>
</tr>
<tr>
<td>grep</td>
<td>605</td>
</tr>
<tr>
<td>help</td>
<td>605</td>
</tr>
<tr>
<td>http</td>
<td>606</td>
</tr>
<tr>
<td>ifconfig</td>
<td>606</td>
</tr>
<tr>
<td>install</td>
<td>606</td>
</tr>
<tr>
<td>iostat</td>
<td>607</td>
</tr>
<tr>
<td>ldapsearch</td>
<td>607</td>
</tr>
<tr>
<td>ls</td>
<td>610</td>
</tr>
<tr>
<td>mallog</td>
<td>610</td>
</tr>
<tr>
<td>malquery</td>
<td>612</td>
</tr>
<tr>
<td>more</td>
<td>619</td>
</tr>
<tr>
<td>mta-control</td>
<td>619</td>
</tr>
<tr>
<td>mta-stats</td>
<td>622</td>
</tr>
<tr>
<td>netstat</td>
<td>623</td>
</tr>
<tr>
<td>nslookup</td>
<td>624</td>
</tr>
<tr>
<td>passwd</td>
<td>624</td>
</tr>
<tr>
<td>pause-mode</td>
<td>624</td>
</tr>
<tr>
<td>ping</td>
<td>625</td>
</tr>
<tr>
<td>reboot</td>
<td>625</td>
</tr>
<tr>
<td>rebuildrpdb</td>
<td>626</td>
</tr>
<tr>
<td>rm</td>
<td>626</td>
</tr>
<tr>
<td>route</td>
<td>626</td>
</tr>
<tr>
<td>service</td>
<td>626</td>
</tr>
<tr>
<td>set-control-center-port-443</td>
<td>628</td>
</tr>
<tr>
<td>shutdown</td>
<td>629</td>
</tr>
<tr>
<td>sshdctl</td>
<td>629</td>
</tr>
<tr>
<td>sshdver</td>
<td>631</td>
</tr>
<tr>
<td>sys-info</td>
<td>632</td>
</tr>
<tr>
<td>system-stats</td>
<td>633</td>
</tr>
<tr>
<td>tail</td>
<td>634</td>
</tr>
<tr>
<td>telnet</td>
<td>635</td>
</tr>
<tr>
<td>traceroute</td>
<td>635</td>
</tr>
<tr>
<td>update</td>
<td>635</td>
</tr>
<tr>
<td>version</td>
<td>636</td>
</tr>
<tr>
<td>watch</td>
<td>637</td>
</tr>
</tbody>
</table>

**Glossary** ............................................................................................................. 639

**Index** ................................................................................................................... 651
Introducing Symantec Brightmail Gateway

This chapter includes the following topics:

- About Symantec Brightmail Gateway
- What’s new in Symantec Brightmail Gateway
- Components of Symantec Brightmail Gateway
- How Symantec Brightmail Gateway works
- What you can do with Symantec Brightmail Gateway
- Where to get more information

About Symantec Brightmail Gateway

Symantec Brightmail™ Gateway (formerly branded as Symantec Mail Security) offers enterprises a comprehensive gateway-based message-security solution. Symantec Brightmail Gateway provides a solution that integrates email security, IM security, and premium data loss prevention capabilities in one appliance.

Symantec Brightmail Gateway does the following to protect your environment:

- Detects spam, denial-of-service attacks, and other inbound email threats
- Leverages a global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections
- Filters the email content to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email
- Secures and protects public instant messaging communications with the same management console as it uses to secure and protect email
Obtains visibility into messaging trends and events with minimal administrative burden

See “What's new in Symantec Brightmail Gateway” on page 22.
See “What you can do with Symantec Brightmail Gateway” on page 31.

What's new in Symantec Brightmail Gateway

Table 1-1 lists the new features and enhanced features for this release of Symantec Brightmail Gateway.

<table>
<thead>
<tr>
<th>New feature or enhancement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Connection Classification   | Connection Classification ensures that your worst senders cannot degrade the connection experience of your best senders. Connection Classification assigns every inbound IP address to one of ten classes that are based on local reputation data. Connection Classification automatically does all of the following tasks:  
  ■ Collects local reputation data to support classification and regularly re-evaluates class membership  
  ■ Places the senders that are in the best class on good IP lists and the senders that are in the worst class on bad IP lists  
  ■ Grants the best connection experience to the best class and more restrictive connection abilities to the remaining classes  
  See “About managing connection load at the gateway” on page 134. |
| Fastpass                   | The Fastpass feature conserves resources by exempting senders with the best local reputation from spam scanning. Symantec Brightmail Gateway automatically collects local sender reputation data to support Fastpass determinations and regularly re-evaluates the senders that are granted a pass. You can exclude specific senders from ever receiving a pass.  
  See “About conserving resources using Fastpass” on page 155. |
### Table 1-1: Symantec Brightmail Gateway new features and enhanced features (continued)

<table>
<thead>
<tr>
<th>New feature or enhancement</th>
<th>Description</th>
</tr>
</thead>
</table>
| Brightmail Adaptive Reputation Management | The features that perform filtering that are based on reputation data now appear together in the Control Center on a new top-level Reputation tab. These features leverage both the extensive, world-wide data collection capabilities of Brightmail IQ Services and the local sender data collection capabilities of Symantec Brightmail Gateway. Brightmail Adaptive Reputation Management includes the following features:  
  ■ Sender groups.  
    All sender groups have new names and are organized into good and bad groups. These groups correspond to the former allowed and blocked terminology.  
  ■ New reputation features: Fastpass and Connection Classification.  
  ■ Email virus attacks and directory harvest attacks, which now also appear on the new Reputation tab.  
  See “About blocking and allowing messages at connection time” on page 132. |
| Bounce Attack Prevention | Bounce Attack Prevention protects your network from bounce attacks. Bounce Attack Prevention weeds out the bounced messages that are a result of redirection and forgery while still permitting legitimate bounce message notification.  
  See “About defending against bounce attacks” on page 159. |
| Integration with Vontu Network Prevent | Vontu Network Prevent is a Symantec product that scans email for sensitive data, such as credit card numbers. Symantec Brightmail Gateway now provides an easy and secure method to route email through Vontu Network Prevent. If Vontu Network Prevent detects sensitive data, it can reject the message, redirect the message, add headers or modify subject line. You can configure additional actions in Symantec Brightmail Gateway that are based on added headers, such as creating a compliance incident.  
  See “About Vontu Network Prevent integration” on page 329. |
| Logging improvements | You can now record logs to both the Control Center and syslog on a remote computer. The log levels for the Control Center and the remote syslog can be different.  
  See “Configuring remote logging to syslog” on page 412. |
<table>
<thead>
<tr>
<th><strong>New feature or enhancement</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for multiple downstream MTAs</td>
<td>Administrators can now define up to three static routes as default relays for mail delivery. See “Adding or editing local domains” on page 81.</td>
</tr>
<tr>
<td>Delivery binding strategies</td>
<td>Delivery bindings let you specify the IP address from which mail is sent. You can configure delivery bindings separately for local and non-local email and for email to Spam Quarantine. See “Message delivery phase processing details” on page 51.</td>
</tr>
<tr>
<td>Improved queue management</td>
<td>You can define a limit for the number of messages in a queue. Symantec Brightmail Gateway issues alerts as the message count approaches, reaches, and exceeds the limit. See “About message queues” on page 424.</td>
</tr>
<tr>
<td>Reports</td>
<td>The new Connection Classification Summary report provides a summary of connection data for each connection class. The Reputation Summary and Connection Summary reports are enhanced. See “About working with reports” on page 356.</td>
</tr>
<tr>
<td>Message Audit Log</td>
<td>The Message Audit Log data is updated to include Fastpass and Connection Classification verdicts. You can now specify Fastpass or Connection Classification as an optional filter. See “About message audit logging” on page 418.</td>
</tr>
</tbody>
</table>

### Components of Symantec Brightmail Gateway

Symantec Brightmail Gateway is an all-in-one appliance that secures your gateway. Symantec Brightmail Gateway integrates the core hardware and software pieces necessary for a comprehensive, secure, and easy-to-deploy message security solution. Symantec Brightmail Gateway provides multiple layers of protection that result in infrastructure cost savings and ease of management. By managing connections and messages at each point in the SMTP conversation, Symantec Brightmail Gateway ensures that your infrastructure is used in a cost-effective manner.

The following describes the ways that Symantec Brightmail Gateway protects your environment:
A surging increase in spam volumes strains customer email infrastructures as email scanners must process more messages. When a product filters mail for spam and viruses, the process slows down email delivery and taxes CPU and mail server resources. The increased demand in resources and mail delivery delay occurs because each message needs to be opened and processed.

Symantec Brightmail Gateway can detect undesirable connections and block or defer them. It features a set of automated and configurable connection management features that go into effect as soon as an incoming connection is detected. It serves as a “gatekeeper” in front of the more CPU-intensive pieces of the filtering engine, including the antispm and antivirus layers. It can be configured to block spam attacks, directory harvest attacks, connections from the senders that are identified as spammers by Symantec, and more—automatically. The gateway is the first stage in the inbound protection process. It protects the internal infrastructure by detecting and examining the incoming IP connection before the mail server in Symantec Brightmail Gateway accepts a message. It can then take preventive action such as rejecting the SMTP connection. The gateway can also recognize and block directory harvest attacks and help defend against denial-of-service attacks.

The ability to stop potential attacks is another reason to ensure that certain mail does not breach the gateway in the first place. The best email security solutions accurately reject unwanted mail at the gateway that is based on its IP address. Such SMTP connection management features are an increasingly effective method of dealing with the side effects of increased email volume.
Accounting for over 80 percent of all email traffic, spam chokes the messaging infrastructure, saps mail server and storage resources, and clutters user inboxes. Offensive and fraudulent spam can create liability issues for organizations. Given the unbeatable economics and ineffective legislation, spammers continue to flood organizations with unsolicited mail. As always, spammers continue to adjust tactics and increase their volume to get around the defenses that IT organizations deploy.

Multi-layered spam protection is the cornerstone of the Symantec Brightmail Gateway. Driven by technologies and response capabilities originally developed by Brightmail, the Brightmail Engine harnesses a robust arsenal for filtering techniques. These techniques include spam signatures, heuristics, URL filtering, reputation-based filters, and other standard and proprietary approaches.

Viruses can wreak extreme havoc in an organization. The damage ranges from email server crashes to system downtime and the destruction of company data. From an email security perspective, the worlds of spam and viruses are intricately tied. Internet-delivered email accounts for approximately 80 percent of virus incidents. In addition, the actual payload of many viruses and email-borne worms includes the software that turns the target computer into a spam “zombie.” Spammers then access these zombies and use them to launch spam and other email-based attacks. Given the damage resulting from viruses, it is essential to employ virus protection at the earliest point of network entry: the email gateway. Symantec Brightmail Gateway scans and detects viruses by integrating award-winning Symantec AntiVirus technology.

Antivirus protection includes the following features:

- Automatic virus definition updates
- Flexible policies to handle messages with viruses
- Specific defenses against mass-mailing worms and the associated spawned email messages

Symantec Brightmail Gateway includes a Message Transfer Agent (MTA) that processes, routes, and delivers email messages in cooperation with the Brightmail Engine. You can use the facilities of the MTA to configure custom message handling for different domains or mail servers.

Data loss prevention

To conform to IT, regulatory, HR guidelines, organizations increasingly look to email security appliances to assist in managing policies for email. Symantec Brightmail Gateway includes several features to support a company’s regulatory and internal governance requirements. It also provides the tools to enable development of robust content compliance policies.
About the Symantec Brightmail Gateway software components

A hardened, preinstalled Linux-based operating system powers Symantec Brightmail Gateway. The filtering and management platform software also resides on the appliance. In addition, there is an IM relay and a mail transfer agent (MTA) that enable email communication. Software updates are easily applied, which helps to ensure minimal disruptions for updates.

Symantec Brightmail Gateway software consists of the following subcomponents:

Scanner

Scanners do the following tasks:

- Process the inbound messages and outbound messages and route messages for delivery.
- Download virus definitions, spam and spim signatures, and other security updates from Symantec Security Response.
- Run filters, render verdicts, and apply actions to messages in accordance with the appropriate policies and settings.

See “About Scanner email settings” on page 98.

Each Symantec Brightmail Gateway Scanner uses a separate mail transfer agent, or MTA, when it scans email messages.

See “MTA and message queue behavior” on page 111.

Instant messages are handled through the IM Relay proxy.

See “Working with Services” on page 107.
Control Center

The Control Center provides message-management services, such as centralized administration, reporting, and monitoring. The Control Center also houses a Web server and the databases that store system-wide information.

The Control Center collects and aggregates statistics from connected and enabled Scanners and provides information on their status and maintains system logs. The Control Center also collects statistics on types and levels of security threats. These statistics can be displayed in a variety of reports and distributed in different formats.

The Control Center also hosts Spam Quarantine and Suspect Virus Quarantine. It may also be configured to store Information that is related to messages that trigger content-compliance policies.

See “About quarantining spam” on page 220.
See “About quarantining suspected viruses” on page 199.
See “About compliance folders” on page 346.

About the Symantec Brightmail Gateway hardware component

You can deploy Symantec Brightmail Gateway on the Brightmail / Mail Security 8300 Series. The appliance is rack mountable and includes features such as redundant storage with RAID and dual power supplies and fans.

See “Viewing the status of your hardware” on page 392.
See “Viewing information about your hardware” on page 393.

How Symantec Brightmail Gateway works

Figure 1-1 shows how Symantec Brightmail Gateway processes an email message. This diagram assumes that the message passes through the Filtering Engine to the Transformation Engine without being rejected. The diagram also shows the path IM traffic takes through the system.
A description of the path that email messages and instant messages take is as follows:

---

**Figure 1-1** Symantec Brightmail Gateway Architecture

---

Introducing Symantec Brightmail Gateway

How Symantec Brightmail Gateway works
Email messages The path an email message takes through the system is as follows:

- At the gateway, Connection Classification classifies the sending IP into one of 9 classes based on local reputation. It either accepts or defers the connection based on class membership. New senders are placed in a tenth, default class. Symantec Brightmail Gateway also checks the IP address to determine if it belongs to a good sender group or bad sender group. It then blocks or permits the connection accordingly.

- 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 groups. If it does, applies the configured action to the message. If appropriate, the MTA moves the message to its inbound queue.

- The Brightmail Engine consults the LDAP SyncService directory to expand the message’s distribution list.

- The Brightmail Engine determines each recipient’s filtering policies.

- Antivirus filters determine whether the message is infected.

- Content Compliance filters scan the message for restricted attachment types or words, as defined in configurable dictionaries.

- If the sending IP is granted a pass by Fastpass, antispam filtering is bypassed. If not, the antispam filters that use the latest rules from Symantec Security Response determine whether the message is spam. The message may also be checked against user-defined Language settings.

- The Transformation Engine performs actions according to filtering results and configurable policies and applies them to each recipient’s message based on group membership.

Instant messages The path an instant message takes through the IM message flow (from an external source) is as follows:

- IM traffic enters your network and is redirected to the IM proxy by your enterprise DNS servers.

- The IM proxy filters IM traffic according to your settings and compares the traffic with current filters Symantec Security Response publishes. These filters determine whether a message is spam or contains a virus. If a message is determined to contain spam or a virus, you can choose to block this traffic.

- The IM traffic reaches the internal user's IM client.

- If you have enabled outbound IM filtering, outbound messages are routed through the IM proxy before they are sent to an external user's IM client.
**Note:** Symantec Brightmail 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. Nor does it filter the messages on different servers within a Microsoft Exchange organization.

See “About email message flow” on page 35.

### What you can do with Symantec Brightmail Gateway

Table 1-2 describes what you can do with Symantec Brightmail Gateway.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block unwanted email</td>
<td>Symantec Brightmail 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 132.</td>
</tr>
<tr>
<td>Create user groups and policies</td>
<td>You can manage users through user groups. You can specify the groups of users according to email addresses, domain names, or LDAP groups. Then you can apply filtering policies to specific groups. Symantec Brightmail Message filter installs with a Default group that consists of all of the users. See “About groups” on page 63.</td>
</tr>
<tr>
<td>Detect spam</td>
<td>Symantec Brightmail Gateway can detect spam with a high level of accuracy. You can define policies for handling the messages that are identified as spam and set thresholds for suspected spam. You can store spam messages in Spam Quarantine until they can be reviewed. If you configure user access to Spam Quarantine, recipients receive notification when they have messages in their quarantine. Users can then review these messages and take appropriate action. You can also configure Symantec Brightmail Gateway to allow messages from specified domains to bypass antispam scanning altogether. See “About filtering spam” on page 209. See “About quarantining spam” on page 220.</td>
</tr>
<tr>
<td>Tasks</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Detect viruses and other malicious attacks</td>
<td>You can create policies and configure settings to detect viruses and other malicious attacks.</td>
</tr>
<tr>
<td></td>
<td>See “About detecting viruses and malicious attacks” on page 170.</td>
</tr>
<tr>
<td>Enforce content compliance</td>
<td>Keyword dictionaries and templates help you create the compliance policies that filter the email messages. Such policies can be used to monitor user compliance with corporate and regulatory requirements and to prevent data loss.</td>
</tr>
<tr>
<td></td>
<td>See “About content filtering” on page 279.</td>
</tr>
<tr>
<td>Detect IM threats</td>
<td>Symantec Brightmail Gateway offers enterprises a gateway-based instant messaging (IM) traffic filter solution. Along with its email security solutions, Symantec Brightmail Gateway provides threat protection solutions to your enterprise for IM through the features and settings.</td>
</tr>
<tr>
<td></td>
<td>See “About IM” on page 251.</td>
</tr>
<tr>
<td>Monitor performance</td>
<td>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 compliance policies.</td>
</tr>
<tr>
<td></td>
<td>See “About monitoring the status of your product” on page 387.</td>
</tr>
<tr>
<td></td>
<td>Symantec Brightmail Gateway includes over 50 reports that provide statistics on content compliance, email messages, instant 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.</td>
</tr>
<tr>
<td></td>
<td>See “About working with reports” on page 356.</td>
</tr>
<tr>
<td>Tasks</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Obtain definition updates</td>
<td>You can use either of the following methods to obtain virus definition updates:</td>
</tr>
<tr>
<td></td>
<td>■ LiveUpdate</td>
</tr>
<tr>
<td></td>
<td>You can use LiveUpdate to automatically update your protection. When LiveUpdate runs, it downloads and installs any available definitions.</td>
</tr>
<tr>
<td></td>
<td>■ Rapid Response</td>
</tr>
<tr>
<td></td>
<td>You can use Rapid Response when you need quick responses to emerging threats. Rapid Response definitions are most useful for a perimeter defense to mitigate quickly spreading threats. Rapid Response is an alternative to LiveUpdate.</td>
</tr>
<tr>
<td></td>
<td>See “About updating virus definitions” on page 191.</td>
</tr>
<tr>
<td>Obtain notifications about outbreaks, system issues, and policy violations</td>
<td>You can configure Symantec Brightmail Gateway to automatically send alerts and notifications about a wide variety of events.</td>
</tr>
<tr>
<td></td>
<td>These events include the following:</td>
</tr>
<tr>
<td></td>
<td>■ Policy violations</td>
</tr>
<tr>
<td></td>
<td>■ Virus outbreaks</td>
</tr>
<tr>
<td></td>
<td>■ System, synchronization, and replication errors and status</td>
</tr>
<tr>
<td></td>
<td>■ Spam and virus quarantine information</td>
</tr>
<tr>
<td></td>
<td>■ License expiration and update availability</td>
</tr>
<tr>
<td></td>
<td>See “Types of alerts” on page 447.</td>
</tr>
<tr>
<td>Manage your appliance</td>
<td>Symantec Brightmail Gateway provides the features that help you do the following tasks:</td>
</tr>
<tr>
<td></td>
<td>■ Monitor devices.</td>
</tr>
<tr>
<td></td>
<td>See “Monitoring devices through SNMP” on page 450.</td>
</tr>
<tr>
<td></td>
<td>■ Configure and manage Scanners.</td>
</tr>
<tr>
<td></td>
<td>See “About Scanner email settings” on page 98.</td>
</tr>
<tr>
<td></td>
<td>■ Configure LDAP clients and schedule synchronization and replication.</td>
</tr>
<tr>
<td></td>
<td>See “About LDAP synchronization” on page 481.</td>
</tr>
<tr>
<td></td>
<td>See “About replicating data to Scanners” on page 504.</td>
</tr>
<tr>
<td></td>
<td>■ Manage system software.</td>
</tr>
<tr>
<td></td>
<td>See “Updating your software” on page 474.</td>
</tr>
</tbody>
</table>
Table 1-2  What you can do with Symantec Brightmail Gateway *(continued)*

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the command line to configure Symantec Brightmail Gateway</td>
<td>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. See “About administering your product through the command line” on page 591.</td>
</tr>
</tbody>
</table>

### Where to get more information

The following resources provide more information about your product:

**Documentation**

The Symantec Brightmail Gateway documentation set consists of the following manuals:

- Symantec Brightmail Gateway Administration Guide
- Symantec Brightmail Gateway Installation Guide
- Symantec Brightmail Gateway Getting Started Guide

**Product Help system**

Symantec Brightmail 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:

- [www.symantec.com/enterprise/support](http://www.symantec.com/enterprise/support)
  Provides you access to the technical support Knowledge Base, newsgroups, contact information, downloads, and mailing list subscriptions
  Provides you information about registration, frequently asked questions, how to respond to error messages, and how to contact Symantec License Administration
- [www.enterprisesecurity.symantec.com](http://www.enterprisesecurity.symantec.com)
  Provides you product news and updates
  Provides you access to the Virus Encyclopedia, which contains information about all known threats; information about hoaxes; and access to white papers about threats
Understanding message flow

This chapter includes the following topics:

■ About email message flow
■ About outbound message flow
■ Message routing phase processing details
■ Message delivery phase processing details

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 Brightmail Gateway lets you manage two messaging protocols: SMTP and Instant Messaging. This chapter provides an overview of the message flow for SMTP (Simple Mail Transfer Protocol). Although you can filter instant messages on the same host as email, the two protocols operate through separate IP addresses and ports.

See “About IM” on page 251.

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 compliance policies, on the other hand, address the data loss prevention and regulatory compliance issues that most often effect outbound message flow.
**Warning:** Symantec Brightmail 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 Brightmail 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 132.

See “About content filtering” on page 279.

See “Email message flow phases” on page 36.

See “About outbound message flow” on page 45.

**Note:** You can vary the number of times Symantec Brightmail Gateway scans a potentially malformed message.

See “Determining which message caused a Brightmail Engine failure” on page 475.

---

**Email message flow phases**

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

- **Phase 1, SMTP connection** – During the connection phase Symantec Brightmail 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 Brightmail 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 Brightmail Gateway rejects the SMTP connection, unless a different action is configured for the group. Based on Connection Classification limits, some connections are deferred. See “Inbound SMTP connection phase processing details” on page 39.

- **Phase 2, SMTP session** – During the SMTP session, Symantec Brightmail 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 “Inbound SMTP session phase processing details” on page 41.

- **Phase 3, Message filtering** – After the Scanner accepts a message, Symantec Brightmail Gateway evaluates the message content and renders verdicts. It evaluates the message content based on applicable policies and settings, including, if required, compliance policies. Based on the verdicts, it applies the configured actions.
See “Inbound message filtering phase processing details” on page 43.

■ Phase 4, Message routing – Symantec Brightmail 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 “Message routing phase processing details” on page 50.

■ Phase 5, Message delivery – Symantec Brightmail 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 Brightmail Gateway uses the specified IP addresses.
See “Message delivery phase processing details” on page 51.

Figure 2-1 illustrates the inbound message flow.
Figure 2-1  Inbound Message Flow
Inbound SMTP connection phase processing details

During the connection phase, Symantec Brightmail Gateway accepts, defers, or rejects connections from hosts based on their IP addresses. Table 2-1 shows the settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

**Note:** If you do not use the default action for a sender group, the action that you configure may not occur in the same phase. For example, if you change the default action for the Local Bad Sender IPs sender group to Modify the Subject line, the action takes place in the message filtering phase.

See “About blocking and allowing messages using sender groups” on page 143.

Table 2-1 Inbound SMTP connection phase setting defaults

<table>
<thead>
<tr>
<th>Setting or group of settings</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab - Inbound Mail Acceptance</td>
<td>Accept inbound mail connections from all IP addresses</td>
<td>Accept all SMTP connections. Symantec recommends this setting if your appliance is at the gateway. If the IP address or domain is listed, accept the SMTP Connection. If not, reject the SMTP connection.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab - Inbound SMTP Configuration</td>
<td>Accept inbound mail connections only from the following IP addresses and domains</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Maximum number of Connections</td>
<td>If either maximum is exceeded, defer the SMTP connection.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Maximum number of connections from a single IP address</td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Defer new connections when inbound queue is full</td>
<td>If the inbound message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when the appliance storage space is exhausted.</td>
</tr>
<tr>
<td>Setting or group of settings</td>
<td>Detail</td>
<td>Default action</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Delivery SMTP Configuration</td>
<td>Defer new connections when delivery queue is full</td>
<td>If the delivery message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when the appliance storage space is exhausted.</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders &gt; Local Bad Sender IPs</td>
<td>IP addresses added by a local administrator</td>
<td>If the IP address is listed in this group, reject the SMTP connection.</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders &gt; Third Party Bad Senders</td>
<td>Third party lists of IP addresses subscribed to by a local administrator.</td>
<td>If the IP address is listed in this group, reject the SMTP connection.</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders &gt; Symantec Global Bad Senders</td>
<td>IP addresses provided by Symantec based on combined world-wide reputation data from Brightmail IQ Services, a part of Symantec’s Global Intelligence Network.</td>
<td>If the IP address is listed in this group, reject the SMTP connection.</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders &gt; Directory Harvest Attack</td>
<td>IP addresses that have sent messages to numerous invalid recipients.</td>
<td>If the IP address is listed in this group, and the configured thresholds are exceeded, defer the SMTP connection.</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders &gt; Email Virus Attack</td>
<td>IP addresses that have sent numerous virus messages.</td>
<td>If the IP address is listed in this group, and the configured thresholds are exceeded, defer the SMTP connection.</td>
</tr>
</tbody>
</table>
### Table 2-1 Inbound SMTP connection phase setting defaults (continued)

<table>
<thead>
<tr>
<th>Setting or group of settings</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation &gt; Settings &gt; Connection Classification</td>
<td>Maximum Connections</td>
<td>If either maximum is exceeded for the class that the IP address currently belongs to, defer the SMTP connection. Defer the connection for the number of seconds specified in the Reconnect Timeout field for that class.</td>
</tr>
<tr>
<td></td>
<td>Maximum Connections per IP</td>
<td></td>
</tr>
</tbody>
</table>

### Inbound SMTP session phase processing details

During the SMTP session (or protocol) phase, Symantec Brightmail Gateway validates sender domains and message envelope details. Table 2-2 shows the settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

#### Table 2-2 Inbound SMTP session phase setting defaults

<table>
<thead>
<tr>
<th>Setting or group of settings</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Maximum message size in bytes</td>
<td>Reject the message if it exceeds the maximum size.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Maximum number of recipients per message</td>
<td>If the number of recipients for a message exceeds the maximum, reject the message for the additional recipients.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Maximum number of messages in inbound queue</td>
<td>After the maximum is reached, defer messages.</td>
</tr>
<tr>
<td>Setting or group of settings</td>
<td>Detail</td>
<td>Default action</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Inbound SMTP Configuration</td>
<td>Defer new connections when inbound queue is full</td>
<td>If the inbound message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when appliance storage space is exhausted.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Delivery SMTP Configuration</td>
<td>Defer new connections when delivery queue is full</td>
<td>If the delivery message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when appliance storage space is exhausted.</td>
</tr>
<tr>
<td>Protocols &gt; SMTP &gt; Domains/Edit/Add - Acceptance - Recipient Validation</td>
<td>Enable Recipient Validation for this domain</td>
<td>If Reject invalid recipients or Drop invalid recipients is configured at Protocols &gt; SMTP &gt; Invalid Recipients, reject or drop the message for all invalid recipients. This only works if LDAP is correctly configured.</td>
</tr>
<tr>
<td>Protocols &gt; SMTP &gt; Address Masquerading</td>
<td>Apply to Inbound messages or Inbound and outbound messages</td>
<td>Modify message envelope and header to rewrite recipient addresses.</td>
</tr>
<tr>
<td>Protocols &gt; SMTP &gt; Aliases</td>
<td>Rewrite recipient addresses on mail addressed to aliases</td>
<td>Modify message envelope</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, TLS Encryption</td>
<td>Accept TLS Encryption Request Client Certificate</td>
<td>N/A</td>
</tr>
<tr>
<td>Spam &gt; Policies &gt; Email/Editor Add</td>
<td>If a message fails bounce attack validation</td>
<td>Reject messages with no tag or invalid tags</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Connection Classification-message thresholds</td>
<td>Messages per Connection Deferred Messages (%)</td>
<td>Defer message</td>
</tr>
</tbody>
</table>
Inbound message filtering phase processing details

During the message filtering phase, Symantec Brightmail Gateway renders verdicts on messages and implements actions based on those verdicts. The message filtering phase is also when messages are scanned for spam, viruses, and compliance issues.

Table 2-3 shows the policies and settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

**Note:** If you do not use the default action for a sender group, the action that you configure may not occur in the same phase. For example, if you change the default action for the Local Bad Sender IPs sender group to Modify the Subject line, the action takes place in the message filtering phase.

### Table 2-3 Inbound message-filtering phase policy and setting defaults

<table>
<thead>
<tr>
<th>Feature, settings, policies, or resources</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation &gt; Policies &gt; Good Senders/Fastpass/Enable Fastpass</td>
<td>Most messages from legitimate senders that Fastpass granted passes for bypass spam filtering</td>
<td>If the message is free of viruses and compliance issues, deliver normally.</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Good Senders</td>
<td>Local Good Sender Domains Local Good Sender IPs Symantec Global Good Senders Third Party Good Senders</td>
<td>Deliver message normally.</td>
</tr>
<tr>
<td>Spam &gt; Settings &gt; Sender Authentication</td>
<td>Authenticate the sender IP against a published DNS record using Sender Policy Framework (SPF) or Sender ID.</td>
<td>If authentication fails, prepend subject line with [sender auth failure]</td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders</td>
<td>Local Bad Senders Domains</td>
<td>Delete message</td>
</tr>
<tr>
<td>Spam &gt; Settings &gt; Scan Settings/Email tab Spam &gt; Policies &gt; Email/Add or Edit</td>
<td>Select a Suspected Spam Threshold between 25 and 89 Conditions If a message is spam or suspected spam, If a message is spam, If a message is suspected spam</td>
<td>Modify the subject line</td>
</tr>
<tr>
<td>Feature, settings, policies, or resources</td>
<td>Detail</td>
<td>Default action</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>Virus &gt; Scan Settings Exclude Scanning Lists Email Virus Policies</td>
<td>Filter message subject, body, or attachment content for viruses and other threats</td>
<td>Virus (clean message) Mass-mailing worm (delete message) Unscannable for viruses (delete message) Encrypted attachment (prepend subject line) Spyware or adware (prepend subject line) Suspicious attachment (strip attachment and delay in Suspect Virus Quarantine) Exclude Scanning List (do not scan for viruses)</td>
</tr>
<tr>
<td>Dictionaries Regular expressions, Patterns Described content compliance policy</td>
<td>Filter message subject, body, or attachment content for keywords and regular expressions</td>
<td>If the specified content is found, take the configured action for the compliance policy.</td>
</tr>
<tr>
<td>Dictionaries Described content compliance policies</td>
<td>Filter message headers for keywords</td>
<td>If the specified content is found, take the configured action for the compliance policy.</td>
</tr>
<tr>
<td>Dictionaries, regular expressions, Patterns Described content compliance policy condition</td>
<td>Filter envelope or message headers for keywords and regular expressions</td>
<td>If the specified content is found, take the configured action for the compliance policy.</td>
</tr>
<tr>
<td>SMTP Scan Settings Virus Scan Settings - Exclude Scanning</td>
<td>Identify configured attachment file types</td>
<td>Stop processing Bypass scanning</td>
</tr>
</tbody>
</table>
### Table 2-3
Inbound message-filtering phase policy and setting defaults (continued)

<table>
<thead>
<tr>
<th>Feature, settings, policies, or resources</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content compliance policy condition</td>
<td>Filter messages that exceed size limits</td>
<td>If a message exceeds the limit, take the action configured for the compliance policy.</td>
</tr>
<tr>
<td>Attachment Lists</td>
<td>Filter message attachments for metadata (file type, file name, MIME type)</td>
<td>If the specified metadata is found, take the configured action for the compliance policy.</td>
</tr>
<tr>
<td>Compliance policy metadata condition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### About outbound message flow

Because Symantec Brightmail Gateway only accepts outbound connections from secure internal mail servers it performs fewer checks on mail addressed to non-local domains. It rejects connections from mail host IP addresses that are not allowed by SMTP Mail Acceptance settings or that exceed SMTP Configuration connection parameters. It then evaluates message content for spam, viruses, and content compliance to determine whether a message should be deleted, quarantined, held for review in a compliance folder or forwarded with or without modifications or notifications. Depending on the outcome of message filtering, Symantec Brightmail Gateway routes outbound mail for Internet delivery. Alternatively, it routes messages to the appropriate non-local or local mail host according to your Domains Delivery options and SMTP Mail Delivery, SMTP Delivery Configuration, and Delivery Bindings settings.

See “Outbound SMTP connection phase processing details” on page 45.

See “Outbound SMTP session phase processing details” on page 46.

See “Outbound message filtering processing details” on page 48.

See “Message routing phase processing details” on page 50.

See “Message delivery phase processing details” on page 51.

### Outbound SMTP connection phase processing details

Before accepting email that is addressed to a non-local domain, Symantec Brightmail Gateway validates the connecting mail host against the Scanner's Outbound Mail Acceptance settings. It only accepts connections from specified IP addresses.
Symantec Brightmail Gateway also rejects connections that exceed Outbound SMTP Configuration connection limits.

Table 2-4 shows the settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

<table>
<thead>
<tr>
<th>Setting or group of settings</th>
<th>Details</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP Outbound Mail Acceptance</td>
<td>Accept outbound mail connections from the following IP addresses and domains</td>
<td>If the IP address or domain is listed, accept the SMTP Connection. If not, reject the SMTP connection.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings Outbound SMTP Configuration</td>
<td>Maximum number of Connections Maximum number of connections from a single IP address</td>
<td>If either maximum is exceeded, defer the SMTP connection.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Outbound SMTP Configuration</td>
<td>Defer new connections when outbound queue is full</td>
<td>If the outbound message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when the appliance storage space is exhausted.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Delivery SMTP Configuration</td>
<td>Defer new connections when delivery queue is full</td>
<td>If the delivery message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when the appliance storage space is exhausted.</td>
</tr>
</tbody>
</table>

Outbound SMTP session phase processing details

Symantec Brightmail Gateway accepts outbound messages from qualified mail host IP addresses except for those that exceed SMTP Configuration message thresholds.
During the SMTP session, Symantec Brightmail Gateway checks the following SMTP Configuration settings:

- If the size of a message exceeds Outbound SMTP Configuration message size threshold, Symantec Brightmail Gateway rejects the message.
- If the number of recipients exceeds the good number of recipients per message, Symantec Brightmail Gateway rejects the recipient address and generates an error.

Table 2-5 shows the settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

**Table 2-5** Outbound SMTP session phase setting defaults

<table>
<thead>
<tr>
<th>Setting or group of settings</th>
<th>Details</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Outbound SMTP Configuration</td>
<td>Maximum message size in bytes &lt;br&gt;Maximum number of recipients per message</td>
<td>Reject the message if it exceeds the maximum size. &lt;br&gt;If the number of recipients for a message exceeds the maximum, reject the message for the additional recipients.</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab - Outbound Mail Settings</td>
<td>Accept TLS encryption</td>
<td>N/A</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Outbound SMTP Configuration</td>
<td>Defer new connections when outbound queue is full</td>
<td>If the outbound message queue is full, defer the SMTP connection. &lt;br&gt;If this box is not checked, connection deferrals begin when the appliance storage space is exhausted.</td>
</tr>
</tbody>
</table>
Table 2-5  Outbound SMTP session phase setting defaults (continued)

<table>
<thead>
<tr>
<th>Setting or group of settings</th>
<th>Details</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - Delivery SMTP Configuration</td>
<td>Defer new connections when delivery queue is full</td>
<td>If the delivery message queue is full, defer the SMTP connection. If this box is not checked, connection deferrals begin when the appliance storage space is exhausted.</td>
</tr>
<tr>
<td>Protocols &gt; SMTP &gt; Address Masquerading</td>
<td>Apply to Outbound messages or Inbound and outbound messages</td>
<td>Modify message envelope and header to rewrite sender addresses.</td>
</tr>
</tbody>
</table>

Outbound message filtering processing details

During the message filtering phase, Symantec Brightmail Gateway renders verdicts on messages and implements actions based on those verdicts. The message filtering phase is when Symantec Brightmail Gateway scans messages for spam, viruses, and compliance issues.

If you use Vontu Network Prevent to filter content, Symantec Brightmail Gateway first routes outbound messages to Vontu Network Prevent for message filtering.

See “About Vontu Network Prevent integration” on page 329.


Table 2-6 shows the policies and settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

Table 2-6  Outbound message filtering setting and policy defaults

<table>
<thead>
<tr>
<th>Setting, group of settings, policies, or resources</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan settings – Suspected Spam threshold</td>
<td>Filter message subject, body, or attachment content for spam or suspected spam</td>
<td>Modify subject line</td>
</tr>
<tr>
<td>Spam and Suspected Spam policies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-6 Outbound message filtering setting and policy defaults (continued)

<table>
<thead>
<tr>
<th>Setting, group of settings, policies, or resources</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
</table>
| LiveUpdate antivirus definitions | Filter message subject, body, or attachment content for viruses and other threats | Virus (clean message)  
Worm (delete message)  
Unscannable for virus (delete message)  
Encrypted attachment (prepend subject line)  
Spyware or adware threat (prepend subject line)  
Suspect virus (strip attachment and delay in Suspect Virus Quarantine) |
| Virus Scan settings | | |
| Virus policies | | |
| Dictionaries | Filter message subject, body, or attachment content for keywords and regular expressions | If the specified content is found, take the configured action for the compliance policy. |
| Regular expressions, Patterns | | |
| Described content compliance policy | | |
| Dictionaries | Filter message headers for keywords | If the specified content is found, take the configured action for the compliance policy. |
| Described content compliance policies | | |
| Dictionaries, regular expressions, Patterns | Filter envelope or message headers for keywords and regular expressions | If the specified content is found, take the configured action for the compliance policy. |
| Described content compliance policy condition | | |
| SMTP Scan Settings | Identify configured attachment file types | Stop processing  
Bypass scanning |
| Virus Scan Settings - Exclude Scanning | | |
| Content compliance policy condition | Filter messages that exceed size limitations | If a message exceeds the limit, take the action configured for the compliance policy. |
Table 2-6  Outbound message filtering setting and policy defaults (continued)

<table>
<thead>
<tr>
<th>Setting, group of settings, policies, or resources</th>
<th>Detail</th>
<th>Default action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment Lists</td>
<td>Filter message attachments for metadata (file type, file name, MIME type)</td>
<td>If the specified metadata is found, take the configured action for the compliance policy.</td>
</tr>
<tr>
<td>Compliance policy metadata condition</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Message routing phase processing details**

During the message routing phase, Symantec Brightmail Gateway sends inbound mail to the server that you define for delivery of mail that is addressed to a local domain. By routing messages to multiple downstream servers, you can distribute local delivery of inbound mail among internal mail hosts for load balancing and failover redundancy.

You can define up to three static routes via non-local default mail hosts for non-local delivery of outbound mail. You can use these routes to send bounce messages generated by non-deliverable spam messages back to their sender domains. You do this by changing your Outbound Non-Local Mail Delivery settings.

You can optionally define static routes on a per-domain basis using the Edit Domain/Delivery settings.

See “Adding or editing local domains” on page 81.

When you define a spam, virus, compliance, or reputation policy, you can use the Route the message action to specify a route for messages that match that policy.

If you use Vontu Network Prevent, configure Symantec Brightmail Gateway to route outbound messages to Vontu Network Prevent. Messages are then immediately re-accepted by Symantec Brightmail Gateway for further filtering and delivery.


Table 2-7 shows the settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.
### Table 2-7  
**Email message routing settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab -</td>
<td>Relay local mail to: (3 hosts maximum)</td>
</tr>
<tr>
<td><strong>Inbound Local Mail Delivery</strong></td>
<td></td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab -</td>
<td>Use MX Lookup for non-local mail</td>
</tr>
<tr>
<td><strong>Outbound Non-Local Mail Delivery</strong></td>
<td>Relay non-local mail to: (3 hosts maximum)</td>
</tr>
<tr>
<td>Protocols &gt; SMTP &gt; Domains/Add or Edit/Delivery tab/Optional Destination Routing</td>
<td>Destination host, optionally Port and MX Lookup</td>
</tr>
<tr>
<td>Spam &gt; Policies &gt; Email/Add or Edit/Actions</td>
<td>Route the message</td>
</tr>
<tr>
<td>Virus &gt; Policies &gt; Email/Add or Edit/Actions</td>
<td></td>
</tr>
<tr>
<td>Compliance &gt; Policies &gt; Email/Add or Edit/Actions</td>
<td></td>
</tr>
<tr>
<td>Reputation &gt; Policies &gt; Bad Senders or Good Senders/sender group name/Add or Edit/Actions</td>
<td></td>
</tr>
<tr>
<td>Compliance &gt; Settings &gt; Vontu DLP Connect/Route Outbound Mail to DLP Servers</td>
<td>Add</td>
</tr>
</tbody>
</table>

### Message delivery phase processing details

During the message delivery phase, Symantec Brightmail Gateway delivers messages, implements configured delivery restrictions on connections and messages, and implements configured delivery bindings.

Delivery bindings allow you to specify the IP address from which mail is sent. In systems where Symantec Brightmail Gateway is not deployed at the gateway, a firewall may prevent inbound and outbound Scanners from communicating. In such cases, you change your SMTP Delivery Bindings setting for Local messages to your outbound mail IP address. Or, you can change your setting for Non-local messages to your inbound mail IP address. You can also let Symantec Brightmail Gateway automatically decide which IP address to use.

If you use Vontu Network Prevent, Symantec Brightmail Gateway also delivers messages that were filtered by Vontu Network Prevent.

Table 2-8 shows the settings that control this phase.

Only the settings that Symantec Brightmail Gateway uses during this phase are shown. Some settings are used in more than one phase.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - SMTP Delivery Configuration</td>
<td>Maximum number of connections to all internal servers</td>
</tr>
<tr>
<td></td>
<td>Maximum number of connections per single internal mail server</td>
</tr>
<tr>
<td></td>
<td>Maximum number of external connections</td>
</tr>
<tr>
<td></td>
<td>Maximum number of external connections to a single IP address</td>
</tr>
<tr>
<td></td>
<td>Maximum number of messages in delivery queue</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - SMTP Delivery Configuration</td>
<td>Minimum retry interval</td>
</tr>
<tr>
<td></td>
<td>Sent message time-out</td>
</tr>
<tr>
<td></td>
<td>Bounce message time-out</td>
</tr>
<tr>
<td>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - SMTP Delivery Configuration</td>
<td>Message time delay time in queue before notification</td>
</tr>
<tr>
<td></td>
<td>Attempt TLS encryption for delivery of all messages</td>
</tr>
<tr>
<td></td>
<td>Offer TLS client certificate</td>
</tr>
<tr>
<td>Protocols &gt; SMTP &gt; Domains/Add or Edit/Delivery tab/TLS Encryption</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>Administration &gt; Hosts &gt; Configuration/Edit/SMTP tab, Advanced Settings - SMTP Delivery Bindings</td>
<td>Local messages</td>
</tr>
<tr>
<td></td>
<td>Non-local messages</td>
</tr>
<tr>
<td></td>
<td>Dynamically routed messages</td>
</tr>
<tr>
<td></td>
<td>Messages destined for the Control Center</td>
</tr>
</tbody>
</table>
Understanding message filtering

This chapter includes the following topics:

- About filtering
- Filtering actions and verdicts for email messages
- Filtering actions and verdicts for instant messages
- Multiple actions per verdict
- Verdict and action combinations
- About multiple content compliance policies
- About groups
- About assigning filter policies to groups
- Configuring Sender Authentication

About filtering

Although Symantec Brightmail Gateway provides default settings for dealing with spam, spim, and viruses, you can configure the actions taken on filtered messages to meet your organizational requirements. Content compliance policies offer further methods of managing mail flow into and out of your organization. You can use content compliance policies to monitor and enforce compliance with regulatory and organizational requirements.
Symantec Brightmail Gateway provides a wide variety of actions for filtering email and instant messages (IM), and allows you to either set identical options for all users, or specify different actions for distinct user groups.

You specify groups of users based on email addresses, domain names, or LDAP groups. For each group, you can specify an action or group of actions to perform when a message results in a particular verdict. You specify actions when you create or edit a spam, spim, virus, or compliance policy. Each of these policies is a filtering policy.

Verdicts are the conclusions reached on a message by the filtering process. When you create or edit a filtering policy, you specify the conditions that you are looking for in messages. Each condition or set of conditions corresponds to a type of verdict that Symantec Brightmail Gateway can assign to a message.

Symantec Brightmail Gateway performs actions on an email or IM based on the verdict applied to the message and the groups that include the message recipient or sender as a member, as follows:

- For inbound email filtering, the groups that impact message filtering are those groups that include the message recipient.
- For outbound email filtering, the groups that impact message filtering are those groups that include the message sender.

See “About groups” on page 63.

Table 3-1 describes email filtering verdicts by category.

Table 3-1 Filtering verdicts by verdict category

<table>
<thead>
<tr>
<th>Verdict Category</th>
<th>Verdict</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Sender Policies</td>
<td>Directory harvest attack</td>
<td>An attempt is underway to capture valid email addresses. A directory harvest attack is accomplished by emailing to your domain with a specified number of non-existent recipient addresses sent from the same IP address.</td>
</tr>
<tr>
<td></td>
<td>Email virus attack</td>
<td>A specified quantity of infected email messages has been received from a particular IP address.</td>
</tr>
<tr>
<td>Bad Sender Groups</td>
<td></td>
<td>An email message, domain, or IP address is a member of one of the following groups:</td>
</tr>
<tr>
<td></td>
<td>Local Bad Sender Domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Bad Sender IPs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Third Party Bad Senders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Symantec Global Bad Senders</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About blocking and allowing messages using sender groups” on page 143.</td>
</tr>
</tbody>
</table>
### Filtering verdicts by verdict category (continued)

<table>
<thead>
<tr>
<th>Verdict Category</th>
<th>Verdict</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good Sender</td>
<td>Good Sender</td>
<td>An email message, domain, or IP address is a member of one of the following groups:</td>
</tr>
</tbody>
</table>
| Policies         | Groups         | ■ Local Good Sender Domains  
|                  |                | ■ Local Good Sender IPs  
|                  |                | ■ Third Party Good Senders  
|                  |                | ■ Symantec Global Good Senders  
|                  |                | See “About blocking and allowing messages using sender groups” on page 143.                                                           |
|                  | Fastpass       | Allows most email messages from verified good senders to bypass spam filtering. You cannot specify any actions for the Fastpass verdict.          |
|                  | Sender          | An email message has failed either SPF or Sender ID authentication.                                                                         |
|                  | authentication  | See “Configuring Sender Authentication” on page 76.                                                                                         |
|                  | Virus          | An email or IM message contains a virus, based on current Symantec virus filters.                                                           |
|                  | Mass-mailing    | An email or IM message contains a mass-mailing worm, based on current Symantec virus filters.                                             |
|                  | worm           |                                                                                                                                              |
|                  | Unscannable for | An email or IM message exceeds the container limits configured on the Scanning Settings page or is unscannable for other reasons. For example, a  |
|                  | viruses        | message or an attachment that contains malformed MIME cannot be scanned for viruses.                                                        |
|                  | Encrypted       | An email or IM message contains an attachment that is encrypted or password-protected and therefore cannot be scanned.                      |
|                  | attachment     |                                                                                                                                              |
|                  | Spyware or      | An email or IM message contains any of the following types of security risks: spyware, adware, dialers, joke programs, or remote access         |
|                  | adware         | programs. See Spyware or adware verdict details for descriptions of these risks.                                                           |
|                  | Suspicious      | An email or IM message either shows virus-like signs or because suspicious new patterns of message flow involving this attachment have been detected.|
|                  | attachment     |                                                                                                                                              |
|                  | Spam           | An email message is spam, based on current spam filters from Symantec.                                                                     |
|                  | Suspected spam  | An email message is suspected spam, based on a configurable Suspected Spam Threshold.                                                      |
|                  | Failed bounce   | An email message is part of a bounce attack, based on bounce attack validation filtering.                                                 |
|                  | attack validation | See “About defending against bounce attacks” on page 159.                                                                                 |
### Table 3-1  Filtering verdicts by verdict category *(continued)*

<table>
<thead>
<tr>
<th>Verdict Category</th>
<th>Verdict</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spim</td>
<td>Spim</td>
<td>An IM message contains spim, based on current spim filters from Symantec.</td>
</tr>
<tr>
<td>Content Compliance Text in the Subject, Body, or Attachments</td>
<td>Text in this specific part of the message</td>
<td>An email message contains keywords in your configurable dictionary, matches/does not match a regular expression or pattern, or matches data in a record.</td>
</tr>
<tr>
<td></td>
<td>Text in this specific part of the message header</td>
<td>Text in any of 13 message parts contains or matches in one of several ways a specific string, or matches/does not match a regular expression or pattern.</td>
</tr>
<tr>
<td></td>
<td>Message size</td>
<td>The message size is equal to/greater than/less than a specific number of bytes, KB, or MB.</td>
</tr>
<tr>
<td></td>
<td>File metadata</td>
<td>An attachment is in an attachment list, has a specific filename or MIME type, or contains/does not contain a filename or file extension from specific dictionary.</td>
</tr>
<tr>
<td></td>
<td>For all messages</td>
<td>All email is flagged. You can create a compliance rule that applies to all messages, for example to universally attach an annotation to all inbound or outbound email messages.</td>
</tr>
</tbody>
</table>

### Filtering actions and verdicts for email messages

Table 3-2 describes the filtering actions available for each verdict category.

When using Table 3-2, note the following:

- See Table 3-1 for the specific verdicts included in each category.
- The Sender Groups column includes both good and bad sender groups, but does not include Fastpass. You cannot specify any actions for the Fastpass verdict.
- In general, messages from senders in the good sender groups bypass spam filtering, but do not bypass virus filtering or content filtering.

See “Verdict combinations” on page 512.
## Table 3-2

**Email filtering actions by verdict category**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Attacks</th>
<th>Virus</th>
<th>Spam</th>
<th>Content Compliance</th>
<th>Sender Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a header</td>
<td>Add an email header.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Add annotation</td>
<td>Insert predefined text (a disclaimer, for example).</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Add BCC recipients</td>
<td>Blind carbon copy to the designated SMTP address(es).</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Archive the message</td>
<td>Forward a copy to the designated SMTP address and, optionally, host.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Bypass compliance policy</td>
<td>Do not filter spam messages for content compliance policies. You can choose all content compliance policies or specify the policies to bypass.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Bypass spam scanning</td>
<td>Do not scan messages that meet this policy for spam. Cannot be added to the list of approved or rejected actions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Clean the message</td>
<td>Repair repairable virus infections and delete unrepairable virus infections. Only available for the virus verdict.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create an incident</td>
<td>Create a record of a compliance or regulatory incident. Optionally, hold for review and defer certain actions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Defer SMTP connection</td>
<td>Using a 4xx SMTP response code, tell the sending MTA to try again later. Cannot be used with the Local Bad Sender Domains or Local Good Sender Domains groups.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Delete message</td>
<td>Delete the message.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Deliver message normally</td>
<td>Deliver the message. Viruses and mass-mailing worms are neither cleaned nor deleted.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Attacks</td>
<td>Virus</td>
<td>Spam</td>
<td>Content Compliance</td>
<td>Sender Groups</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-------</td>
<td>------</td>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Deliver the message to the recipient's Spam folder</td>
<td>Deliver to end-user Spam folder(s). Requires use of the Symantec Spam Folder Agent for Exchange or the Symantec Spam Folder Agent for Domino. <strong>Note:</strong> Symantec no longer provides technical support for the Symantec Spam Folder Agent for Exchange and the Symantec Spam Folder Agent for Domino.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Deliver message with TLS encryption</td>
<td>Send the message over an encrypted channel.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward a copy of the message</td>
<td>Copy the message to designated SMTP address(es), and also deliver the original message to the recipient.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Hold message in Spam Quarantine</td>
<td>Send to the Spam Quarantine.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Hold message in Suspect Virus Quarantine</td>
<td>Hold in the Suspect Virus Quarantine for a configured number of hours (default is six), then refilter for viruses only, using the latest virus definitions. Only available for the suspicious attachment verdict.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify the Subject line</td>
<td>Add a tag to the message's Subject: line.</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Reject messages failing bounce attack validation</td>
<td>If a message fails bounce attack validation, reject the message. Only available for the Failed bounce attack validation verdict.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reject SMTP connection</td>
<td>Using a 5xx SMTP response code, notify the sending MTA that the message is not accepted. Cannot be used with the Local Bad Sender Domains or Local Good Sender Domains groups.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Attacks</td>
<td>Virus</td>
<td>Spam</td>
<td>Content Compliance</td>
<td>Sender Groups</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-------</td>
<td>------</td>
<td>---------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Remove unresolved recipients (for Directory Harvest Attacks only)</td>
<td>If a directory harvest attack is taking place, remove each unresolved recipient rather than sending a bounce message to the sender. You must configure LDAP recipient validation, complete LDAP synchronization, and complete Scanner replication before enabling this feature.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Route the message</td>
<td>Deliver via the designated SMTP host.</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send a bounce message</td>
<td>Return the message to its From: address with a custom response and deliver it to the recipient, with or without attaching the original message.</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Send notification</td>
<td>Deliver the original message and send a predefined notification to designated SMTP address(es) with or without attaching the original message.</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Strip and Delay in Suspect Virus Quarantine</td>
<td>Remove all non-text content and deliver the stripped message immediately. Hold the complete message in Suspect Virus Quarantine for a configured number of hours (default is six hours), then release and rescan. Only available for the Suspicious Attachment verdict.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strip attachments</td>
<td>Remove all attachments according to a specific attachment list. Cannot be used with sender authentication.</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat as a bad sender</td>
<td>Process using the action(s) specified in the Local Bad Sender Domains group. Applies even if the Local Bad Sender Domains group is disabled.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Treat as a mass-mailing worm</td>
<td>Process using the action(s) specified in the associated worm policy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Treat as a good sender</td>
<td>Process using the action(s) specified in the Local Good Sender Domains group. Applies even if the Local Good Sender Domains group is disabled. When used in a compliance policy, messages that match the policy will not be scanned for spam.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td>Attacks</td>
<td>Virus</td>
<td>Spam</td>
<td>Content Compliance</td>
<td>Sender Groups</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-------</td>
<td>------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Treat as a virus</td>
<td>Process using the action(s) specified in the associated virus policy.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Treat as spam</td>
<td>Process using the action(s) specified in the associated spam policy.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Treat as suspected spam</td>
<td>Process using the action(s) specified in the associated suspected spam policy.</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

When using Table 3-2 consider the following limitations:

- By default, inbound and outbound messages containing a virus are cleaned of the virus. Inbound and outbound messages containing a mass-mailing worm, and unscannable messages, including malformed MIME messages, are deleted. If you are concerned about losing important messages, you may want to create a different filter policy for unscannable messages and apply that new filter policy to some or all of your groups. See Table 3-4 on page 68.

- The Send a bounce message action returns the message to its From: address with a custom response, and also delivers the original message to the recipient. Symantec does not recommend using the Send a bounce message action for virus or spam policies. Virus and spam messages often use falsified headers. An attempt to deliver a bounce message to an uninvolved party named in the From: address is basically sending a spam message. This could result in your domains being blacklisted by other domains or by third-party black lists.

- If a message matches a compliance policy that invokes the Bypass spam scanning action and also matches a spam policy that invokes the Bypass compliance policy action, neither spam nor compliance actions are applied to that message.

- When you select certain actions, you can encode an optional archive tag for Western European (ISO-8859-1, default), Unicode (UTF-8), Japanese (ISO-2022-JP, EUC-JP, or Shift_JIS), Simplified Chinese(GB2312 or GB18030), Traditional Chinese (Big5), or Korean (KS_C_5601-1987).
When using Table 3-3, note the following regarding the columns:

- The Virus category includes verdicts for viruses, mass-mailing worms, spyware/adware, and suspicious attachments.
- There are no attack, content compliance, sender group, or sender authentication policies for IM.

Table 3-3 IM filtering actions by verdict category

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Virus</th>
<th>Spim</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add annotation</td>
<td>Add an annotation to an IM message informing the recipient that the message contains spim or suspected spim.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Allow file transfer</td>
<td>Allow an infected, encrypted, or unscannable file to be transferred to its recipient.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Block file transfer</td>
<td>Block an infected, encrypted, or unscannable file from being transferred to its recipient.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Delete the message</td>
<td>Delete an IM message that contains spim or suspected spim.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Deliver message normally</td>
<td>Deliver an IM message that contains spim or suspected spim.</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Send notification</td>
<td>Send a predefined notification to the sender of an IM message that contains spim or an infected file informing the sender of the action.</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Multiple actions per verdict

Within a filtering policy, you can create compound actions, performing multiple actions for a particular verdict.

An example follows:

1. Defining a virus policy, the administrator selects the Virus verdict and then assigns the actions, Clean, Add annotation, and Send notification to the policy.
2. Defining a group, the administrator assigns members then selects the new virus policy.
3. An email message is received whose recipients include someone in the new group.
4. Symantec Brightmail Gateway cleans the message, annotates it, delivers it, then sends a notification to its intended recipients.
When more than one filtering policy applies to a message, Symantec Brightmail Gateway uses special logic to combine actions from different filtering policies. See “Verdict and action combinations” on page 62.

**Verdict and action combinations**

Symantec Brightmail Gateway offers the ability to combine multiple actions for different verdicts on the same message. This capability provides advantages over a model in which only one verdict for a message can result in actions. For example, suppose a spam message also contains a virus and your policies specify quarantining of spam messages and cleaning of viruses. Instead of cleaning the virus and delivering the spam to user inboxes, Symantec Brightmail Gateway cleans the virus and holds the cleaned spam message in Spam Quarantine. Or, if your policies specify modification of the subject line of spam messages and cleaning of viruses, Symantec Brightmail Gateway cleans the virus from the message and modifies the subject line.

Other types of messages can be affected by more than one filtering policy. A message can meet the criteria for two different content compliance policies. Or, the same spam message could contain a virus and meet the criteria for several content compliance policies. Symantec Brightmail Gateway combines the various filtering policies to determine which actions should be taken on the message.

In order to implement multiple actions, Symantec Brightmail Gateway includes sophisticated processing logic that automatically resolves potential conflicts between actions. In general, there is no need to worry about how actions will combine between your filtering policies. However, because a particular message can match multiple filtering policies, the resulting actions may not match your expectations. This section explains the basics of how actions from different policies can combine.

What happens to a message depends on the particular combination of actions applied to that message by the one or more policies that affect the message. In other words, actions combine with each other (or not, in some cases) based solely on action types. The kind of policy that called for the action has no impact on processing. The order in which actions are listed in the Control Center has no impact on processing.

For example, you create a compliance policy to take action on messages that contain two or more words from your Profanity custom dictionary in the subject, body, or attachments of the message. You only use this policy for your Sales group. The action you specify for these messages is Delete message. Your default virus policy specifies the action Clean the message, and your default spam policy specifies the action Modify the subject line, placing [SPAM] before the subject
line text. Your Sales group uses the default virus and spam policies. A spam message addressed to a member of your Sales group arrives containing three words from your Profanity dictionary and also containing a virus. What happens to that message?

Because one of the actions specified is Delete message, Symantec Brightmail Gateway deletes the message and does not apply the other actions. In most cases, the Delete message action prevents other actions from occurring. However, what if the compliance policy did not apply because the message contained only one word from your Profanity dictionary? In that case, the message is cleaned and delivered to the user's inbox with [SPAM] prepended to the subject line.

Many types of actions from different policies can be combined for the same message.

See “Limits on combining actions” on page 507.

About multiple content compliance policies

When more than one content compliance policy applies to a message, some of the actions specified may not take place.

- The order of policies on the Email Content Compliance Policies page determines content compliance policy priority. Higher priority content compliance policies appear higher up in the list.

- Actions specified for the highest priority content compliance policy that applies to a message are triggered according to the rules for combining actions. See “Limits on combining actions” on page 507.

- For the other content compliance policies that apply to the message, the only actions that can happen are the Send notification and Create an incident (without holding for review) actions.

About groups

You can specify configurable message management options for an unlimited number of user groups that you define. Groups collect the spam, virus, and compliance verdicts and actions for a set of users.

When Symantec Brightmail Gateway processes a message, the results for each sender or recipient can differ, based on group membership. If an inbound message goes to recipients in more than one group, the message is processed for the recipients in each group according to the filtering policies assigned to that group. For an outbound message, it is the sender's group that determines processing, not the groups of the recipients.
For a particular recipient or sender who is a member of more than one group, only the group with the highest group precedence applies. Group precedence is determined by the order of groups on the Groups page.

See “Creating groups and adding or removing members” on page 64.

See “Importing and exporting group members” on page 65.

See “About assigning filter policies to groups” on page 68.

The group management options let you do the following:

- Set group precedence, which determines the filter policies applied to each message.
- Edit group membership and actions.
- Enable and disable groups.
- Delete groups.
- View group information for particular users.

See “Working with groups” on page 66.

See “Setting group precedence” on page 67.

See “Researching group membership for a user” on page 67.

Creating groups and adding or removing members

You can specify groups of users based on email addresses, domain names, or LDAP groups. For each group, you can specify email filtering actions for different categories of email.

Note: To edit a group member, such as to correct a typo, delete the member and add the member again. There is no Edit button for group members.

To create a new Group

1. In the Control Center, click Administration > Users > Groups.

   The Groups page lists each Group. The Default group, which contains all users and all domains, always appears last. Although you can add or modify actions for the Default group, you cannot add members to the Default group. You cannot delete or disable the Default group.

2. On the Groups page, click Add.

3. Enter a name in the Group name text box.

4. Click Save.
To add a new member to a Group

1. In the Control Center, click **Administration > Users > Groups**.

2. Click the underlined name of the Group you want to edit.

3. Ensure that the Members tab is displayed, and click **Add**.

4. Specify members using one or both 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. Use * to match zero or more characters and ? to match a single character. To add all recipients of a particular domain as members, type any of the following:
     - domain.com
     - @domain.com
     - *@domain.com
   - Check the box next to one or more LDAP groups.
     - The LDAP groups listed on this page are loaded from your LDAP server. See About the supported LDAP services and directories for information about configuring LDAP source definitions.

5. Click **Add members** to add the new member(s).

6. Click **Save** on the Edit Group page.

To delete a Group member

1. In the Control Center, click **Administration > Users > Groups**.

2. Click the underlined name of the Group that you want to edit.

3. On the Members tab of the Edit Group page, check the box next to one or more email addresses, domains, or LDAP groups, and then click **Delete**.

4. Click **Save** on the Edit Group page.

Importing and exporting group members

You can import group members from a file, and you can export group members to a file. You cannot import or export LDAP groups. If you export from a group that includes LDAP groups, the LDAP groups will be omitted from the export.

To import Group members from a file

1. In the Control Center, click **Administration > Users > Groups**.

2. Click the underlined name of the Group that you want to edit.
3 On the **Members** tab of the Edit 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** on the Edit Group page.

**To export Group members to a file**

1 In the Control Center, click **Administration > Users > Groups**.

2 Click the underlined name of the Group you want to edit.

3 In the Members tab of the Edit Group page, click **Export**.

4 Complete your operating system's save file dialog box as appropriate.

---

**Working with groups**

The following sections describe common administrative tasks for groups.

**To edit an existing group**

1 In the Control Center, click **Administration > Users > Groups**.

2 Click the policy name or check the box next to a group, and then click **Edit**.

   Add or delete members or change filtering actions for this group as you did when you created it.

   See “Creating groups and adding or removing members” on page 64.
To enable a Group

1. In the Control Center, click Administration > Users > Groups.
2. Check the box next to a group, and then click Enable.

To disable a Group

1. In the Control Center, click Administration > Users > Groups.
2. Check the box next to a group, and then click Disable.

**Note:** You cannot disable or delete the Default group.

To delete a Group

1. In the Control Center, click Administration > Users > Groups.
2. On the Groups page, check the box next to a Group, and then click Delete.

**Setting group precedence**

The Groups page lists groups in a specific order. Groups higher in the list have a higher precedence. If a user is a member of more than one group, only the group with higher precedence applies in determining how messages are processed for that user.

See “About groups” on page 63.

To set group precedence

1. In the Control Center, click Administration > Users > Groups.
2. Select the checkbox next to the group whose precedence you want to change, and click Move Up or Move Down to change the order of precedence.

**Note:** The Default group is always the last group in the list. You cannot change the precedence of the Default group.

**Researching group membership for a user**

You can identify all of the groups to which a user is assigned.

To identify all of the groups to which a user is assigned

1. Do one of the following:
   - In the Control Center, click Administration > Users > 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 first enabled group in which the specified user exists, searching in the order that groups are listed on the Groups page.

### About assigning filter policies to groups

By default, groups that you create are assigned the default filter policies for spam, spim, and viruses (there is no default for compliance policies). Follow the steps in the sections below to assign different filter policies to groups. You may first want to create your own filter policies.

### Selecting virus policies for a group

Virus policies determine what to do with inbound and outbound email and IM messages that contain any of the threat categories listed in Table 3-4.

<table>
<thead>
<tr>
<th>Category</th>
<th>Default email action</th>
<th>Default IM action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>Clean the message</td>
<td>Inbound message: Block the file transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound message: Block the file transfer and send a notification to the sender</td>
</tr>
<tr>
<td>Mass-mailing worms</td>
<td>Delete the message</td>
<td>Inbound message: Block the file transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound message: Block the file transfer and send a notification to the sender</td>
</tr>
<tr>
<td>Unscannable messages</td>
<td>Delete the message</td>
<td>Inbound message: Block the file transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound message: Block the file transfer and send a notification to the sender</td>
</tr>
</tbody>
</table>
Table 3-4  Virus categories and default actions (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Default email action</th>
<th>Default IM action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted attachments</td>
<td>Prepend [WARNING ENCRYPTED ATTACHMENT NOT VIRUS SCANNED] to Subject: header.</td>
<td>Inbound message: Block the file transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound message: Block the file transfer and send a notification to the sender</td>
</tr>
<tr>
<td>Spyware or adware</td>
<td>Prepend [SPYWARE OR ADWARE INFECTED] to Subject: header.</td>
<td>Inbound message: Block the file transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outbound message: Block the file transfer and send a notification to the sender</td>
</tr>
<tr>
<td>Suspicious attachments</td>
<td>Inbound message: Strip and Delay in Suspect Virus Quarantine.</td>
<td>Inbound message: Block the file transfer</td>
</tr>
<tr>
<td></td>
<td>Outbound message: Hold message in Suspect Virus Quarantine.</td>
<td>Outbound message: Block the file transfer and send a notification to the sender</td>
</tr>
</tbody>
</table>

For a description of each of these categories, see Table 3-1.

See “Creating email virus policies” on page 179.

See “About the default virus policies” on page 175.

By default, inbound and outbound email messages containing a mass-mailing worm, and unscannable messages, including malformed MIME messages, will be deleted. If you are concerned about losing important messages, you may want to create a different filter policy for unscannable messages and apply that new filter policy to some or all of your groups.

**To select virus policies for a group**

1. In the Control Center, click **Administration > Users > Groups**.
2. On the Groups page, click the group for which you want to select virus policies.
3. Click the **Virus** 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 group**, and then select the desired policy from each of the following drop-down lists:
   - Inbound email antivirus policy
   - Inbound email mass-mailing worm policy
Unscannable inbound email message policy
Inbound encrypted email attachment policy
Inbound suspicious email attachment message policy
Inbound email spyware/adware policy
6 If desired, under Email, check Enable outbound email virus scanning for this group, and then select the desired policy from each of the following drop-down lists:
- Outbound email antivirus policy
- Outbound email mass-mailing worm policy
- Unscannable outbound email message policy
- Outbound encrypted email attachment policy
- Outbound suspicious email attachment policy
- Outbound email spyware/adware policy
7 If desired, under Instant Messaging, check Enable inbound instant messaging virus scanning for this group. You can view the following policy:
- Inbound instant messaging antivirus policy
  This policy includes the mass-mailing worm, spyware/adware, and suspicious attachment policies that are listed in Table 3-4.
- Inbound encrypted instant messaging attachment policy
- Unscannable inbound instant messaging message policy
8 If desired, under Instant Messaging, check Enable outbound instant messaging virus scanning for this group. You can view the following policy:
- Outbound instant messaging antivirus policy
  This policy includes the mass-mailing worm, spyware/adware, and suspicious attachment policies that are listed in Table 3-4.
- Outbound encrypted instant messaging attachment policy
- Unscannable outbound instant messaging message policy
9 Click Save.
You cannot change virus policy details from the Edit Group page.
See “Creating email virus policies” on page 179.
Selecting spam and spim policies for a group

Spam and spim policies determine what to do with inbound and outbound email messages that contain spam or suspected spam and IM messages that contain spim or suspected spim.

See “Creating email spam policies” on page 211.

See “Creating IM spim policies” on page 274.

By default, an email that is detected as spam or suspected spam is marked with [Spam] or [Suspected Spam], respectively, at the beginning of its subject line.

By default, an IM message that is detected as spim or suspected spim is deleted. In addition, the sender of an outbound IM message receives a notification that the message was deleted.

To select spam or spim policies for a group

1. In the Control Center, click Administration > Users > Groups.
2. On the Groups page, click the group for which you want to select spam or spim policies.
3. Click the Spam 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 spam scanning for this group, and then select the desired policy from each of the following drop-down lists:
   - Inbound email antispam policy
   - Inbound email suspected spam policy
6. If desired, under Email, check Enable outbound email spam scanning for this group, and then select the desired policy from each of the following drop-down lists:
   - Outbound email antispam policy
   - Outbound suspected email spam policy
7 If desired, under Email, check **Enable bounce attack prevention for this group**, and then select the desired policy from **Bounce attack prevention policy** drop-down list.

Symantec Brightmail Gateway provides a default policy: Failed Bounce Attack Validation: Reject message. You can also edit this policy or create a new policy, which must contain the condition, **If a message fails bounce attack validation** and actions to be taken should bounce address tag validation fail.

See “About defending against bounce attacks” on page 159.

8 If desired, under Instant Messaging, check **Enable inbound instant messaging spim scanning for this group**. You can view the following policy:

- **Inbound instant messaging spim policy**

9 If desired, under Instant Messaging, check **Enable outbound instant messaging spim scanning for this group**. You can view the following policy:

- **Outbound instant messaging spim policy**

10 Click **Save**.

You cannot change spam policy details from the Edit Group page.

### Selecting compliance policies for a group

By associating an appropriate compliance 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 compliance policies to check for compliance with statutory regulations or organizational policies.

**Note:** Because there are no default compliance policies, the drop-down list on the Edit Group page is initially blank. Before selecting compliance policies for a group, you must first create at least one compliance policy.

See “About configuring compliance policies” on page 280.

**To select compliance policies for a group**

1 In the Control Center, click **Administration > Users > Groups**.

2 On the Groups page, click the group for which you want to select compliance policies.

3 Click the **Compliance** tab.

4 Check **Enable Inbound Content Compliance for this group**.
5 Select the desired policy from the **Content Compliance Policies** drop-down list.

You must already have applied the policy to the group on the Email Content Compliance Policy page for it to appear in the drop-down list.

If desired, click **View** to see a summary of the compliance policy, and then click **OK** to return to the Edit Group page. As you add compliance policies from the drop-down list, they are displayed in the bottom list and become unavailable in the drop-down list.

6 Click **Add**.

7 If desired, add additional policies from the **Content Compliance Policies** drop-down list.

8 To configure outbound content compliance policies for the group, check **Enable Outbound Compliance for this group** and follow 5 through 7 again.

9 Click **Save**.

You cannot change compliance policy details (such as conditions and actions) from the Edit Group page. Although you can add existing policies to the lists on this page, you cannot add new compliance policies from this page.

---

**Selecting Network Access Control policies for a group**

Network Access Control (or NAC) policies determine which public IM networks members of a particular group can access.

By default, all of the public IM networks that are supported by Symantec Brightmail Gateway can be accessed by all of the IM users that are in your network. If you want to block access to a particular IM network for a group, enable a Network Access Control policy for that group.

See “Blocking access to an IM network” on page 269.

**To select a Network Access Control policy for a group**

1 In the Control Center, click **Administration > Users > Groups**.

2 On the Groups page, click the group for which you want to select a Network Access Control policy.

3 Click the **IM NAC** tab.

4 Check **Enable Network Access Control policies for this group**.

5 Select the desired policy from the **Network access control policy** drop-down list.
6 Optionally, click **View** next to any policy to view the details of that policy.
7 Click **Save**.

### Enabling and disabling end user settings

End-user settings determine whether end users in a 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 both an LDAP authentication and a synchronization source defined and enabled to perform these tasks. Synchronization source data must have undergone at least one full synchronization cycle and been replicated to attached and enabled Scanners.

See “About the supported LDAP services and directories” on page 477.

**Note:** Depending on your system and the group that you are editing, you may not be able to view the End Users tab on the Edit Group page.

See “Requirements for enabling end-user settings” on page 75.

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 *Symantec Brightmail Gateway Installation Guide*.

**Note:** End users are limited to a total of 200 entries in their combined Good Senders and Bad Senders lists.

**Note:** Symantec no longer provides technical support for the Symantec Outlook Spam Plug-in. Users of the Symantec Outlook Spam Plug-in should note that the Specify language settings check box enables or disables user access to the language identification offered by Symantec Brightmail Gateway, not the Symantec Outlook Spam Plug-in. If the Symantec Outlook Spam Plug-in is installed and enabled, end users can set their language preferences using the Options dialog box accessible from the Symantec Outlook Spam Plug-in toolbar.
Note: Although the language identification technology employed by Symantec Brightmail Gateway 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 policies for a group
1 In the Control Center, click Administration > Users > Groups.
2 On the 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 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
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 LDAP synchronization source must be configured and enabled.
- An LDAP source configured for authentication must be defined and saved.
- Scanner replication frequency must be defined and enabled.
- End-user preferences must be enabled for the given group on the End Users tab on the Edit Group page.
- Members of the group can only be LDAP users, not a locally defined user (that is, an email address you typed manually).

Allowing or blocking email based on language
Using the language identification offered by Symantec Brightmail Gateway, 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.
Note: If the Language tab in the Edit Group page is inaccessible, the Symantec Outlook Spam Plug-in has been enabled. To disable support for the Symantec Outlook Spam Plug-in and enable support for built-in language identification, set Language Identification to No on the Spam > Settings > Scan Settings page. Choosing No makes the Language tab accessible.

To allow or block email based on language for a group
1. In the Control Center, click Administration > Users > Groups.
2. On the 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 Symantec Brightmail Gateway 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.

Configuring Sender Authentication

Symantec Brightmail Gateway can authenticate a sender's IP address by checking it against the published DNS record for the named mail server. If the DNS record includes a hard outbound email policy (one that requires compliance), and it does not include the sending IP address, Symantec Brightmail Gateway processes the inbound message according to the action that you specify on the Sender Authentication page. If the sender's IP address matches the IP address published in DNS record, or if the domain publishes only an informational policy or does not publish a policy at all, no action is taken.

Authenticating the IP addresses of senders can reduce spam because spammers often attempt to forge the mail server name to evade detection. Symantec Brightmail Gateway uses the Sender Policy Framework (SPF) or the Sender ID standard to authenticate sender IP addresses. If you specify domains whose IP addresses you want Symantec Brightmail Gateway to authenticate, best practice is to specify the highest-level domain possible, such as example.com, because
tests for compliance include all subdomains of the specified domain—e.g., my.example.com and your.example.com.

**Warning:** Authenticating all domains can significantly increase processing load. Many domains do not publish an outbound email policy, or they publish only an informational policy. Attempting to authenticate the IP addresses belonging to such domains will not produce any action on mail sent from them and can unnecessarily expend processing resources, at times excessively. Authentication is most effective for domains that publish hard policies that are frequently spoofed in phishing attacks.

---

**To enable sender authentication**

1. In the Control Center, click **Spam > Settings > Sender Authentication**.
2. Check **Enable Sender Authentication**.
3. Under Authentication Types, check **Sender Policy Framework (SPF)** or **Sender ID**.

Choosing Sender ID also enables SPF. This is because authenticating Sender ID with DNS also provides SPF authentication.

4. To attempt sender authentication on incoming messages from all domains, click **Authenticate all domains** and click **Save**. To choose domains to authenticate, click **Authenticate only the following domains** and proceed with the remaining steps.

5. Click **Add**, type a domain name in the text field under Add Sender Authentication Domains, and click **Save** to add the domain to the list.

You can click on a domain in the list to edit the spelling of that domain. You can also check a box by the domain name and click **Delete** to delete that entry from the list.

6. If desired, change the default action, or add additional actions. Some action choices display additional fields where you can provide specifics for the action. By default, each failed message has the phrase [sender auth failure] prepended to its subject line.

See “Filtering actions and verdicts for email messages” on page 56.

7. Click **Save**.
Configuring email settings

This chapter includes the following topics:

- About email domains
- Adding or editing local domains
- Adding or editing non-local domains
- Importing a domains list
- Deleting domains
- About invalid recipients
- Configuring invalid recipient handling
- Adding or editing address masquerades
- About aliases

About email domains

When inbound mail arrives at a Scanner for processing, Symantec Brightmail Gateway verifies that the message is addressed to a valid domain before accepting it to the appropriate message queue for email filtering, routing, and delivery.

You must define any domain for which you want Symantec Brightmail Gateway to accept inbound email as a local domain. Symantec Brightmail Gateway only accepts inbound email addressed to local domains.

Defining more than one domain allows you to 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 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.

In general, you specify a domain as a local domain so that Symantec Brightmail Gateway will accept inbound email messages addressed to that domain. However, several features of Symantec Brightmail Gateway make use of local 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 81.
- Define different delivery options for each domain. You can also designate an LDAP 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 addressed to non-local domains. See “Adding or editing local domains” on page 81. See “Adding or editing non-local domains” on page 84.
- Configure Recipient Validation, to validate recipients of email addressed to specified domains against your LDAP directory. See “About invalid recipients” on page 87.
- Configure static routing, to route inbound or outbound email to specified mail servers for internal delivery. See “Message routing phase processing details” on page 50.

You can import lists of domains that you then edit individually. See “Importing a domains list” on page 85.

Typically, a domain is that 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 the domain for somebody@somewhere.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 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 and
somewhere.anywhere as separate domains in order to accept email 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 addressed to them are routed.

About email domain acceptance settings

During site setup, you designate at least one local domain for which Symantec Brightmail 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. See “About invalid recipients” on page 87.
- Detect directory harvest attacks directed against a domain. See “Configuring directory harvest attack recognition” on page 140.

You must enable recipient validation for any domain for which you want Symantec Brightmail 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 or Synchronization profile and enabling recipient validation on a per-domain basis. If recipient validation is enabled for a local domain, Symantec Brightmail Gateway checks with an LDAP source to determine that the full email address matches an entry 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.

See “Configuring invalid recipient handling” on page 88.

Symantec Brightmail Gateway accepts all email from internal mail hosts. See “Changing Scanner outbound mail acceptance settings” on page 105.

Adding or editing local domains

Local domains are domains and email addresses for which Symantec Brightmail Gateway accepts inbound messages. When adding or editing a local domain, you
can assign routing characteristics and enable or disable recipient validation for
messages accepted from the domain. You can also import lists of local domains.
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 up to
three 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.

See “Adding or editing non-local domains” on page 84.

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 Brightmail 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 one or two additional destination
servers as default relays for inbound email addressed to local domains.

Once your installation is up and running, use the Control Center to do the
following:

■ Add more local domains for which you want Symantec Brightmail Gateway to
accept inbound email.

■ Limit inbound mail that is addressed to local domains to valid recipients
Symantec Brightmail Gateway checks recipients of email addressed to specified
local domain against an LDAP source before allowing the sender IP to connect
to the scanner to inbound email interface.
You must configure an appropriate LDAP source and enable Invalid Recipient
Handling to reject or drop inbound email that is addressed to invalid recipients.

■ Define different delivery options for separate domains.

■ Masquerade addresses of email recipients from senders.
See “Adding or editing address masquerades ” on page 90.
To add or edit a local 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 Brightmail Gateway to accept all subdomains.

4. If you wish to reject or drop invalid recipients, click Enable Recipient Validation for this domain.

   You can enable recipient validation for fully qualified domain names for but not for recipient email addresses. Enabling recipient validation has no impact on mail processing until you complete Invalid Recipients settings.

   See “Configuring invalid recipient handling” on page 88.

5. To define delivery options for this domain, click the Delivery tab.

6. If you wish to have messages addressed to this domain routed to a specific destination server or via an LDAP router, check Optionally route this domain or email address.

7. Check Destination host to send messages to a specific host. Choose one of the following options:

   - Specify a Destination host and Port to which messages addressed to this domain are routed. You can also enable MX Lookup for the destination host name.
     If you do not specify a destination host, the domain or email address is routed to the default relay that you configure on the SMTP Settings page.
     See “About Scanner email settings ” on page 98.

   - Alternatively, check LDAP server to route messages through an LDAP server for delivery resolution. Choose the LDAP router from the accompanying drop-down list.
     You must have an LDAP server defined for routing if you plan to have messages routed via LDAP.
     See “About the LDAP routing service” on page 485.

8. 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.

9. Click Save to add the domain, subdomain, or email address to the list or to confirm your edits.
Adding or editing non-local domains

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:

- Statically route outbound email addressed to non-local domains to any one of up to three 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.
- Query an LDAP Routing source to route outbound email addressed to recipients at remote domains.
- Enable TLS encryption options for specified domains.

To add or edit a non-local 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.
4. Deselect the Local domain checkbox.
5. To define delivery options for this domain, click the Delivery tab.
6. If you wish to have messages addressed to this domain routed to a specific destination server or via an LDAP router, check Optionally route this domain or email address.
7. Check Destination host to send messages to a specific host. Choose one of the following options:
   - Specify a Destination host and Port to which messages addressed to this domain are routed. You can also enable MX Lookup for the destination host name.
     If you do not specify a destination host, the domain or email address is routed to the default relay that you configure on the SMTP Settings page. See “About Scanner email settings ” on page 98.
Alternatively, check **LDAP server** to route messages through an LDAP server for delivery resolution. Choose the LDAP router from the accompanying drop-down list. You must have an LDAP server defined for routing if you plan to have messages routed via LDAP. See “About the LDAP routing service” on page 485.

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.

### Importing a domains list

Lists of local domain definitions and email addresses can be imported from a US-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.

After successfully importing a list of domains, each domain appears in the list on the Domains page. You can then edit any domain and, if desired, uncheck Local domain to use that domain as a non-local domain instead.

---

**Note:** LDAP routing information cannot be imported as a part of a domain definition. You can add LDAP routing for a domain once it has been imported by editing the domain name in the Domains list.

See “Adding or editing local domains” on page 81.

You can also indicate in the file which domains for which you want to enable Recipient Validation. You must also enable Recipient Validation Handling and configure an LDAP profile that validates recipient domains.

See “Configuring invalid recipient handling” on page 88.

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.
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:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:local1@domain.com">local1@domain.com</a></td>
<td>smtp:local1.com</td>
</tr>
<tr>
<td><a href="mailto:local2@domain.com">local2@domain.com</a></td>
<td>smtp:local2.com:20</td>
</tr>
<tr>
<td><a href="mailto:local3@domain.com">local3@domain.com</a></td>
<td>smtp:[local3.com]:30</td>
</tr>
<tr>
<td><a href="mailto:local4@domain.com">local4@domain.com</a></td>
<td>smtp:[local4.com]</td>
</tr>
<tr>
<td>.local5.com</td>
<td>smtp:[192.168.248.105]</td>
</tr>
<tr>
<td>local6.com</td>
<td>smtp:[192.168.248.106]:60 VALIDATE_RCPTS</td>
</tr>
</tbody>
</table>

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.
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 invalid recipients**

By default, when an email message arrives addressed to your domain that is not addressed to a valid user, Symantec Brightmail 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 140.

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

- If you choose to accept all recipients, Symantec Brightmail Gateway accepts all messages, whether or not the recipients are valid. However, if the internal mail server rejects a recipient, Symantec Brightmail 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 Brightmail Gateway rejects any messages that are addressed to user names that do not exist in your LDAP directory. The sending MTA may generate a bounce message to the sender. You must have an LDAP source configured for recipient validation. Recipients are rejected at the initial SMTP conversation with a 5xx SMTP error. See “About recipient validation” on page 488.

- If you choose to drop invalid recipients, Symantec Brightmail Gateway drops from the mail stream any messages that are addressed to user names that do not exist in your LDAP directory. No bounce messages are returned to the sender. You must have an LDAP source configured for synchronization. For
this setting to take effect, a full LDAP synchronization and Scanner replication cycle must be completed.
See “About LDAP synchronization” on page 481.

■ If you choose to reject or drop invalid recipients, Symantec Brightmail 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 local domains” on page 81.

---

**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 “To configure invalid recipient handling” on page 89.

## Configuring invalid recipient handling

To validate recipients, Symantec Brightmail Gateway requires access to an LDAP source. You must configure an LDAP source for recipient validation before enabling Reject invalid recipients. You must configure an LDAP source for synchronization, complete LDAP synchronization, and complete Scanner replication before enabling Drop invalid recipients.

See “About the supported LDAP services and directories” on page 477.

See “About replicating data to Scanners” on page 504.

---

**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.
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 configure 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 will be 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 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 have an LDAP source configured for recipient validation. 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 user names that do not exist in your LDAP directory from the mail stream. No bounce messages are returned to the sender. For this setting to take effect, a full synchronization and replication cycle must be completed. You must have an LDAP source configured for recipient validation. 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.
4. If you chose to reject or drop invalid recipients, click Protocols > SMTP > Domains.
   The Domains page appears.
5. Click on the first local domain for which you want to reject or drop invalid recipients.
   The Edit Domain page appears.
6. Check Enable recipient validation for this domain.
7. Click Save.
8. Repeat steps 5 through 7 for each local domain for which you want to reject or drop invalid recipients.
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. Symantec Brightmail 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.

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.
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.
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@domain.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.
About aliases

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 a target domain, example-internetsecurity.com. Symantec Brightmail Gateway translates email addressed to someone@example.com delivered to someone@example-internetsecurity.com.

Alias translation only applies to inbound or internal messages processed by Symantec Brightmail 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.

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 Brightmail Gateway does not route to the message to the alias address or domain.

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 Brightmail Gateway accepts inbound email.

See “Adding or editing local domains” on page 81.

Note: The alias functionality available on the Aliases page operates independently of the Email alias attribute used in LDAP sources.

See “About the supported LDAP services and directories” on page 477.

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

See “Importing aliases” on page 93.

See “Adding or editing aliases” on page 93.
Adding or editing aliases

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” 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. In 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” 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:someone@example.com">someone@example.com</a>, <a href="mailto:somebody@example.com">somebody@example.com</a></td>
</tr>
<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 Brightmail Gateway accepts inbound email.

See “Adding or editing local domains” on page 81.

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>
Configuring email settings

About aliases
Configuring Scanner settings

This chapter includes the following topics:

■ About Scanner email settings
■ About configuring inbound SMTP Scanner settings
■ About configuring outbound SMTP Scanner settings
■ Working with Services
■ Specifying DNS server addresses
■ Configuring Scanner time settings
■ Specifying proxy settings for Scanner updates
■ Configuring Ethernet settings
■ Configuring SMTP Advanced Settings
■ Specifying internal mail hosts for non-gateway deployments
■ Adding Scanners
■ Modifying Scanners
■ Enabling and disabling Scanners
■ Deleting Scanners
■ Stopping and starting Scanners
About Scanner email settings

Scanner email settings allow you to control the sender IP addresses that Symantec Brightmail Gateway accepts email from for message filtering and where it delivers email that has been filtered. 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 its SMTP settings to:

- Accept connections only from specified IP addresses.
- Limit the number of connections to a local or non-local mail host within a given period of time.
- Limit the number of messages that a mail host can attempt to send during a connection session.
- Limit the number of connections over which a Scanner can attempt to deliver messages at any given time.
- Deliver email once it is filtered to the most appropriate local or non-local mail host.

**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 on the same machine that runs the Control Center or on another machine connected to the Control Center. You can instead configure separate inbound and outbound Scanners to run on separate hosts or add dedicated Scanners later.

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 125.
Note: A Scanner that is configured to filter email can also be configured to filter instant messages. However, IM connections must be made over a separate, virtual IP address.

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

- Changing the Scanner role or limiting it to IM only
  See “Defining a scanner role” on page 99.

- Modifying the Scanner’s inbound email settings.
  See “About configuring inbound SMTP Scanner settings” on page 100.

- Modifying the Scanner’s outbound email settings.
  See “About configuring outbound SMTP Scanner settings” on page 104.

- Configuring the Scanner’s MTA settings
  See “Working with Services” on page 107.

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

See “About managing connection load at the gateway” on page 134.

Defining a scanner role

Scanners can be configured to filter inbound, outbound, or both inbound and outbound email.

To define the role of a scanner

1. In the Control Center, click Administration > Hosts > Configuration.
2. In the Hosts list, click the name of the scanner whose role you want to define.
3. Click the SMTP tab.
4. Enter a different name for the Scanner if necessary to identify it by its role.
5. Modify the definition of the Scanner to reflect its new role.
6. Select the option that describes the role of this Scanner.
   - No mail filtering – Select this option if you plan to use this Scanner for IM only and click Save.
   - 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 inbound and outbound SMTP Scanner settings.
7 Check **Apply above settings to all hosts** if you want settings to apply to all Scanners.

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

### About configuring inbound SMTP Scanner settings

After you have installed or added a Scanner using the Add Scanner Wizard, you can edit a Scanner's inbound email settings to:

- Change the Scanner IP address or port number and enable the Scanner to filter inbound TLS-encrypted connections.
  
  See “Changing Scanner inbound mail settings” on page 100.

- Add or edit the IP addresses (or CIDR addresses) from which the Scanner will accept inbound connections.
  
  See “Changing Scanner inbound mail acceptance settings” on page 101.

- Relay filtered email to one or more downstream local or non-local mail servers.
  
  You can designate up to three mail servers to which you can relay inbound or outbound mail.
  
  See “Configuring Scanner inbound email delivery settings” on page 102.

### 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 On the Host Configuration page, click the name of the inbound scanner whose settings you want to modify.

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

4 Select the address that you want to receive inbound messages in the **Inbound mail IP address** drop-down menu.

  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 Enter the port number at which you want inbound mail to be received in **Inbound mail SMTP port** text box.

Typically the port number is 25.

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

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

---

**Note:** You must configure an MTA TLS certificate and assign it to this Scanner before it can accept TLS encrypted email from a connection.

---

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 configuring certificate settings” on page 457.

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 scanning 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 decide to accept mail only from selected IP addresses, and your Scanner is not at the gateway, you must add the IP addresses of all upstream mail servers in use by your organization. Using this setting, Symantec Brightmail Gateway rejects email from unspecified upstream servers.

---

**To change inbound mail acceptance settings**

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

2 On the Host Configuration page, click the name of the inbound scanner whose settings you want to modify.

3 On the Edit Host Configuration page, click the **SMTP** tab.
4 Either:
  - Check **Accept inbound mail connections from all IP addresses** if you want the Scanner to accept connections from senders of all inbound messages, and click **Save**. Skip the rest of this procedure.
  - Check **Accept inbound mail connections from only the following IP addresses** if you want the Scanner to accept only those connections from the addresses that you check in the Inbound Mail Acceptance IP Addresses checklist. Proceed to the next step.

5 Check the boxes next to the IP addresses from which you want this Scanner to accept inbound mail.

6 If needed, click **Add** to add an IP address to the checklist of addresses.

7 You can check the box next to any existing IP address and click **Edit** to alter the address.

8 To delete an address from the checklist, select its check box in IP Addresses and click **Delete**.

9 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 Scanner, you designate the IP addresses and port numbers for both local and non-local mail hosts where inbound mail that has been filtered should be routed. For a combined inbound and outbound Scanner, inbound mail that has been filtered is delivered to a local mail host.

You can designate up to three 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 addressed to different domains. Additional mail servers can also accept email if delivery to the primary mail server for a local domain fails. You must specify the order by which a default relay (static route) attempts to deliver 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.

See “Message routing phase processing details” on page 50.

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

See “About email domains” on page 79.
You can enable MX Lookup for any mail host. MX Lookup determines which server IP address to use to deliver email addressed to a recipient at a local domain.

**To add or edit an IP address for delivery of inbound email**

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. On the Host Configuration page, click the name of the Scanner host to which you want to add or edit a local mail server for delivery of filtered mail.
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 up to three local mail hosts.
5. Enter or modify the IP address and port number in the text boxes that appear.
6. Check **MX Lookup** if you want the local mail host to use MX Lookup to determine which client IP address to use for delivery to email recipients.
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 Brightmail Gateway route mail for non-local recipients via MX query on recipient domains.
   - **Relay non-local mail to** in order to specify up to three mail hosts for delivery of non-local mail.
10. Click **Add** to add the IP address and port number for a non-local mail host. You can configure inbound mail delivery for up to three non-local mail hosts. You can select the checkbox next to the name of the non-local host whose delivery information you want to change 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 client IP address to use for delivery to email recipients.
If you have more than one host specified, type a number in the Preference field. Connections for lower numbered servers are attempted first.

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

About configuring outbound SMTP Scanner settings

After you have installed or added a Scanner using the Add Scanner Wizard, you can edit a Scanner's outbound email settings to:

- Change the Scanner IP address or port number and enable the Scanner to accept outbound TLS-encrypted connections.
  See “Changing Scanner outbound mail settings” on page 104.
- Add or edit the IP addresses (or CIDR addresses) from which the Scanner accepts outbound connections.
  See “Changing Scanner outbound mail acceptance settings” on page 105.
- Relay filtered email to one or more downstream local or non-local mail servers. You can designate up to three mail servers to which you can relay inbound or outbound mail.
  See “Configuring Scanner outbound mail delivery settings” on page 106.

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. On the Host Configuration page, click the name of the Outbound or Inbound and Outbound scanner whose settings you want to modify.
3. On the Edit Host Configuration page, click the SMTP tab.
4. Enter the IP address where you want outbound messages to be received in Outbound mail IP address.
5. Enter the port number where outbound mail is received in Outbound mail SMTP port.

Typically the port is 25.
6 Check **Accept TLS encryption** if you want the host to accept TLS-encrypted outbound connections.

**Note:** You must configure an MTA TLS certificate and assign it to this Scanner before you can accept TLS encrypted outbound mail for filtering.

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

See “About configuring certificate settings” on page 457.

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 up to three mail servers. By allowing connections from only certain IP addresses and domains, you exclude all other hosts from sending messages at connection time.

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

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

2 On the Host Configuration page, click the name of the Outbound or Inbound and Outbound scanner whose settings you want to modify.

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

4 Under Outbound Mail Acceptance, click **Add** and enter the IP address of a local domain from which you want to filter outbound email. You can enter a range of IP addresses using the CIDR format.

   By default, Symantec Brightmail Gateway accepts outbound email sent from all domains. If any domains are listed, it only accepts outbound email sent from those domains.

5 Check the IP address of the email client whose settings you want to change and click **Edit**.

6 Edit the IP address or CIDR addresses of a range.

7 Select an existing addresses or domain from which you no longer want to accept outbound connections and click **Delete** to delete it from the list.

8 Click **Save** or check **Apply above settings to all hosts** 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 Scanner, designate the IP addresses and port numbers for both local and non-local mail hosts where outbound mail that has been filtered should be relayed. For a combined inbound and outbound Scanner, outbound mail is typically delivered to non-local domains.

You can designate up to three mail servers to relay outbound email to the Internet or the next hop in your network. Multiple downstream servers can be used for load balancing or for failover support of the primary mail server for local delivery.

To configure Scanner outbound mail delivery settings for an inbound and outbound Scanner

1. In the Control Center, click Administration > Hosts > Configuration.
2. On the Host Configuration page, click the name of the inbound scanner whose settings you want to modify.
3. On the Edit Host Configuration page, click the SMTP tab.
4. Click either one of the radio buttons under Outbound Non-Local Mail Delivery:
   - Use MX Lookup for non-local mail to have Symantec Brightmail Gateway route mail for non-local recipients through MX query on recipient domains. Skip the rest of this procedure.
   - Relay non-local mail to in order to specify up to three mail hosts for non-local delivery of outbound email.
5. Check the non-local host whose delivery information you want to change and click Edit.
   Alternatively, click Add to add delivery information about a local email host.
   You can configure outbound mail delivery for up to three non-local mail hosts.
6. Enter the IP address and Port number of the mail server to which you want filtered outbound mail delivered.
7. Check MX Lookup if you want to enable MX lookup for this host.
8. If you have more than one host listed, enter a number in the Preference field. Connections for lower numbered servers are attempted first.
9. Select the check box next to any mail server to which you no longer want to send local outbound mail and click Delete.
10. Click Save to save settings or check Apply above settings to all hosts and then click Save.
To configure Scanner outbound mail delivery settings for an outbound-only Scanner

1 Perform the first 8 steps of the previous procedure.
   See “To configure Scanner outbound mail delivery settings for an inbound and outbound Scanner” on page 106.

2 Under Outbound 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 email host.
   You can configure outbound mail delivery for up to three local mail hosts.

3 Edit or enter the IP address and Port number of the mail server to which you want filtered outbound mail delivered.

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

5 If you have more than one host listed, enter a number in the Preference field. Connections for lower numbered servers are attempted first.

6 Select the check box next to any mail server to which you no longer want to send local outbound mail and click Delete.

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

Working with 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.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUpdate</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Service** | **Description**
--- | ---
Brightmail Engine | Scans email and attachments, instant messages, and file transfers for viruses, spam, and content compliance according to filter policies that you have configured.
MTA | The mail transfer agent routes inbound and outbound messages to the Brightmail Engine for processing and deliver filtered messages to their internal destinations or to the Internet.
IM Relay | Retrieves new and updated virus definitions and Spim filters from Symantec Security Response. Uploads suspected Spim to Symantec Security Response and subsequently downloads filters to other Symantec Brightmail Gateway appliances that are configured to detect heuristic-based Spim.

**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.

- Enable or disable individual Scanner replication.
  See “About replicating data to Scanners” on page 504.
- 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 “Managing services, Scanner replication, and MTA operations” on page 108.

### Managing services, Scanner replication, and MTA operations

Table 5-1 lists the various settings that you use to start or stop services, view the status of services, enable Scanner replication, and configure MTA operations.
Table 5-1  Edit Host Configuration page—Services tab

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Start/Stop            | 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 > SMTP > Message Queues page.  
See “MTA and message queue behavior ” on page 111.  
**Note:** 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 > Settings > Control Center page. |
| Scanner Services      | Lists the Scanner services available to the selected host. These are:  
- Conduit  
- LiveUpdate  
- Brightmail Engine  
- MTA  
- IM Relay  
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 running or not on this Scanner.                                                                                                                                                                                                                                                                  |
| Enable Scanner        | Allows replication to update this host when checked.                                                                                                                                                                                                                                                                                        |
| Replication for this host |                                                                                                                                                                                                                                                                                                                                            |
### Table 5-1  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>■ Accept and deliver messages normally – Processes messages in accordance with defined policies</td>
</tr>
<tr>
<td></td>
<td>■ Pause message scanning and delivery – 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>■ Do not accept incoming messages – 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 service not available (450) 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 111.

Use the following procedures from the Services tab to manage individual Scanner services, replication, 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 enable or disable Scanner replication for a host**

1. In the Control Center, click **Administration > Hosts > Configuration**.
2. Click the name of the Scanner on which you want to enable or disable Scanner replication.
3 Under Scanner Replication, perform one of the following actions:
   
   To enable Scanner replication, check **Enable Scanner Replication for this host**.
   
   See “About replicating data to Scanners” on page 504.
   
   Replication is enabled by default.
   
   To disable Scanner replication, uncheck **Enable Scanner Replication for this host**.
   
   The Control Center will not update directory information for this Scanner when the box is unchecked.

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

**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**. See “MTA and message queue behavior” on page 111.

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

**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.

Table 5-2 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 5-2
Manage MTA and message queues on the Edit Host Configuration page, Services tab

<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>
<tr>
<td>Click Pause message scanning and delivery</td>
<td>Accepted.</td>
<td>Not scanned, not delivered. Accumulate in the inbound and outbound message queues.</td>
<td>Stops.</td>
</tr>
<tr>
<td><strong>Note</strong>: This is equivalent to issuing the pause-mode pause command.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Click Do not accept incoming messages</td>
<td>Rejected, issuing SMTP service not available (450) error messages.</td>
<td>Scanned and delivered.</td>
<td>Continues.</td>
</tr>
<tr>
<td><strong>Note</strong>: This is equivalent to issuing the pause-mode reject command.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5-3 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 5-3 affects only one message queue. For example, stopping the inbound message queue has no effect on the outbound or delivery message queues.

Table 5-3
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 Flush.</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 Delete All.</td>
<td>Accepted.</td>
<td>Deleted.</td>
<td>Continues.</td>
</tr>
<tr>
<td>Display the inbound message queue, click Stop.</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 Stop.</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 5-3 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>Not scanned, not delivered. Accumulate in the delivery message queue.</td>
<td>Stops.</td>
</tr>
</tbody>
</table>

Specifying DNS server addresses

Domain Name System (DNS) servers translate domain names into IP addresses. You must specify the IP addresses of the DNS servers that a Scanners uses. If your Scanner hosts email and instant message scanning, the DNS servers that you specify are used for email delivery and external IM communication.

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 > Configuration.
2. Click the name of the host whose DNS definitions you want to modify.
3. Click the DNS/Time tab.
4. Optionally, you can check Use internal DNS server.
   If disabled, you can specify three DNS servers. If the setting is enabled, you can specify two additional DNS servers.
5. Change or add the IP addresses for DNS servers as appropriate.
6. When necessary, you can also flush buffers for DNS servers or routers.

See “Managing services, Scanner replication, and MTA operations” on page 108.
See “Working with Services” on page 107.
See “Components of Symantec Brightmail Gateway” on page 24.
See “Turning off an appliance ” on page 466.
See “About message queues” on page 424.
Configuring Scanner time settings

You can specify primary, secondary, and tertiary Network Time Protocol (NTP) time servers or you can manually specify the time.

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

To configure Scanner time settings

1. In the Control Center, click Administration > Configuration.
2. Click the name of the host whose NTP server definitions you want to modify.
3. 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 hostnames or IP addresses.
   You can choose to specify up to three NTP servers, or you can set the time manually.
6. 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 for Scanner updates

The Conduit service runs on each Scanner and receives filter updates from Symantec. If you use a proxy host to receive these updates, you must add the Conduit proxy server information to your Scanner definition.

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 195.

To specify proxy settings for Scanner updates

1. In the Control Center, click Administration > Hosts > Configuration.
2. Check the name of the Scanner for which you want to specify a proxy.
Configuring Scanner settings

A Scanner's Ethernet settings 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 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 IP 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.

Table 5-4 lists the Scanner Ethernet options that you can configure.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Provides a free-form description for the Ethernet interface.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specifies the IP address of the Ethernet interface. You can change the IP address of a Scanner or the Control Center. If you change the IP address of the Control Center, you must subsequently log into each Scanner's command-line interface and use the <code>agentconfig</code> command to re-allow the secured connection to the Scanner from the new Control Center IP. See “agentconfig” on page 593.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Specifies which part of an IP address is the network address and which is the host address.</td>
</tr>
</tbody>
</table>
Table 5-4  Ethernet connection parameter descriptions  *(continued)*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast</td>
<td>Specifies a common address that is used to direct (broadcast) a message to all terminals on a network. The broadcast address is based on the IP address and the subnet mask.</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies an address identifying the node.</td>
</tr>
<tr>
<td>Negotiation</td>
<td>Check Auto Negotiation if you want Symantec Brightmail Gateway to negotiate the rate for this connection or choose the speed (10, 100, or 1000 GB per second) and duplex setting (half or full) for your high-speed Ethernet connection.</td>
</tr>
<tr>
<td>Segmentation</td>
<td>Check Enable TCP Segmentation Offload if you want the network interface card (NIC) to segment data for outbound transmission. This feature can reduce the load on the CPU resources that are needed to process large volumes of mail for high-bandwidth networks.</td>
</tr>
<tr>
<td>Maximum transmission unit</td>
<td>Works in tandem with the TCP segmentation offload. You can enter a value from 512 bytes to 1500 bytes. When TSO is enabled and the default maximum transmission unit is blank, the value is whatever the NIC (network interface card) specifies for its maximum value. Typically, this value is 1500 bytes maximum for an Ethernet link.</td>
</tr>
<tr>
<td>Virtual</td>
<td>Allows for a virtual IP address to be defined. Depending on the interfaces you specify, one or more virtual networks can appear.</td>
</tr>
<tr>
<td>Enable this interface</td>
<td>Activate the second Ethernet interface.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Address of a router to handle IP traffic between networks (required). Specify an IP address.</td>
</tr>
<tr>
<td>Destination address</td>
<td>Computer or network destination for a static route. Specify an IP address, IP address with subnet mask, or CIDR address. Static routes direct data from one subnet to a different subnet faster than dynamic routes. Static routes must be updated if addresses change.</td>
</tr>
<tr>
<td>Gateway address</td>
<td>Address of a router to use for a static route. Specify an IP address.</td>
</tr>
<tr>
<td>Interface</td>
<td>The appliance’s Ethernet port to use for a static route.</td>
</tr>
</tbody>
</table>
To configure Ethernet settings

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

2. Check the name of the Scanner host whose Ethernet settings you want to modify.

3. Click Edit.

4. Click the Ethernet tab.

5. 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 `agentconfig` command to re-allow the secured connection to the Scanner from the new Control Center IP.

6. For each Ethernet NIC, check Auto Negotiation. Otherwise, select a speed for the connection, and specify half or full duplex operation of the connection.

7. Check Segmentation to offload TCP segmentation from the gateway CPU to the Ethernet card.

8. Check Enable this interface to activate a second Ethernet interface.
   
   You can dedicate a second Ethernet interface to handling inbound or outbound traffic only.

9. Add or delete virtual IP address to an Ethernet interface as needed.
   
   See To add or delete a virtual IP address.

   If you use this Scanner to filter IM traffic, you must configure a virtual IP address. This IP address must be routable on your organization’s internal network so that IM clients inside your network can connect to it.

10. 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.

11. 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, 192.30.250.00/18)

    ■ Gateway address—IP address

    ■ Interface—None, Ethernet 1, or Ethernet 2
12 Click Add to add a static route.
13 Click Save.

To add or delete a virtual IP address
1 Click Administration > Hosts > Configuration.
2 Click the name of the Scanner whose virtual IP addresses you want to modify.
3 Click the Ethernet tab.
4 To add or delete a virtual IP address to either Ethernet interface, perform one of the following tasks:

   To add a virtual address
   In the Virtual field, type the IP address and details for that virtual IP address and then click Add.
   You must have checked Enable this interface for additions to the second Ethernet interface to take effect when settings are saved.

   To delete a virtual IP address
   Check the box beside the name that is associated with the virtual address and click Delete.

5 Click Save.

Configuring SMTP Advanced Settings

Additional SMTP settings are available from the SMTP Advanced Settings page.

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.

You can configure advanced SMTP settings for:
- Inbound messages
- Outbound messages
- Delivering messages
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.

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

### Table 5-5  
**SMTP Advanced Settings—Inbound 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 inbound connections. The default is 2,000 connections.</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 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 recipients per message</td>
<td>Sets the maximum number of recipients for a message. The default is 1,024 recipients.</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>
</tbody>
</table>
| Defer new connections when inbound queue is full   | 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.  

See “Troubleshooting the message queue” on page 428. |
| Insert a RECEIVED header to inbound messages      | Places a RECEIVED header in the message during inbound SMTP processing.                                                                      |
| Enable reverse DNS lookup                          | 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. |
| Session Timeout                                   | 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. |
Table 5-6 describes the advanced outbound SMTP settings that you can use to further define your SMTP 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 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>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>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><strong>Warning:</strong> Enabling this setting can impact the ability of the Symantec Brightmail Gateway MTA (and other MTAs) to detect and stop mail loops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-6  
SMTP Advanced Settings—Outbound Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. <strong>Warning:</strong> Enabling this setting can impact the ability of the Symantec Brightmail Gateway MTA (and other MTAs) to detect and stop mail loops.</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>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>

Table 5-7 describes SMTP delivery configuration message settings for your site.

Table 5-7  
SMTP Advanced Settings—Delivery Configuration

<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>
</tbody>
</table>
**Table 5-7**  SMTP Advanced Settings—Delivery Configuration (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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>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>Offer TLS client certificate</td>
<td>Instructs the MTA to offer a client certificate with every TLS connection.</td>
</tr>
</tbody>
</table>

Table 5-8 describes the settings available for delivery bindings. Delivery bindings allow you to specify the IP addresses from which messages are sent.

See “Message delivery phase processing details” on page 51.

**Table 5-8**  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. 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 Brightmail Gateway automatically chooses the best route based on current traffic flow.</td>
</tr>
</tbody>
</table>
### Table 5-8  SMTP Advanced Settings—Delivery Bindings (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-local messages</td>
<td>Sets the IP address that delivers non-local messages. 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 Brightmail Gateway automatically chooses the best route based on current traffic flow.</td>
</tr>
<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 Brightmail Gateway automatically chooses the best route based on current traffic flow.</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. 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 Brightmail Gateway automatically chooses the best route based on current traffic flow.</td>
</tr>
</tbody>
</table>

### 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 IP addresses of these MTAs as internal mail hosts.

If your network has MTAs that are upstream from Symantec Brightmail 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 Brightmail Gateway includes a series of IP address ranges in the internal hosts list.

See “Internal mail servers: non-gateway deployments” on page 124.

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.
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**.
7. Click **Save** to store the information.

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

When deployed at the gateway, Symantec Brightmail 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 Brightmail 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 Brightmail Gateway appliance.

See “Specifying internal mail hosts for non-gateway deployments” on page 123.

In addition to internal mail hosts you can add, Symantec Brightmail 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 Brightmail 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
- Sender Authentication

### 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.

See “Viewing the status of software and services” on page 394.
Note: If you use LDAP synchronization, you must manually trigger an LDAP synchronization after you add a new Scanner. Wait until the synchronization completes before you let mail be sent to the new Scanner. See “Synchronizing LDAP servers manually” on page 398.

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 Brightmail Gateway Installation Guide for information about completing the Add Scanner Wizard.

Modifying Scanners

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 Scanners
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.
   See “Adding Scanners” on page 125.
   See “About Scanner email settings ” on page 98.

Enabling and disabling Scanners

You can also disable or enable a Scanner, or delete a Scanner. When you disable a Scanner, you stop the flow of statistics, logs, and configuration information between that Scanner and your Control Center. The Scanner can still process messages. The Control Center can still route 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.

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 lose 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.

See “Stopping and starting Scanners” on page 127.

See “Enabling and disabling Scanners” on page 126.

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**.

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.

See “Adding administrators” on page 439.
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 127.

**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 111.

See “Managing services, Scanner replication, and MTA operations” on page 108.

**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 Hosts drop-down list, choose a Scanner.
7. In the Queues 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.
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.

16 Click Save to save your changes and return to the Host Configuration page.

17 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.
Configuring Scanner settings

Stopping and starting Scanners
Blocking and allowing messages at connection time

This chapter includes the following topics:

- About blocking and allowing messages at connection time
- About managing connection load at the gateway
- Configuring email virus attack recognition
- Configuring directory harvest attack recognition
- About blocking and allowing messages using sender groups
- Enabling or disabling good and bad sender groups
- Choosing actions for good and bad sender groups
- Adding senders to administrator and third party sender groups
- About conserving resources using Fastpass
- About defending against bounce attacks
- Researching IP address reputation
About blocking and allowing messages at connection time

Scanning email for spam, viruses, and compliance issues is a resource-intensive task. Any email that must be processed past the gateway taxes your mail infrastructure, resource capacity, and system performance. Symantec Brightmail 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 Brightmail 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 6-1

<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. 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. 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). See “About managing connection load at the gateway” on page 134. See “Configuring Connection Classification” on page 136.</td>
</tr>
<tr>
<td>Email virus attack prevention</td>
<td>If Symantec Brightmail 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. See “Configuring email virus attack recognition” on page 138.</td>
</tr>
<tr>
<td>Directory harvest attack prevention</td>
<td>If Symantec Brightmail Gateway detects a specified number and percentage of invalid recipient from an IP address, directory harvest attack prevention can then defer further connections. Or, you can choose other actions. See “Configuring directory harvest attack recognition” on page 140.</td>
</tr>
</tbody>
</table>
Table 6-1  (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Sender Policies</td>
<td>You can add senders to administrator-defined groups and use Symantec Global Bad Senders to block email from bad senders, or choose other actions. See “About blocking and allowing messages using sender groups” on page 143.</td>
</tr>
<tr>
<td>Good Sender Policies</td>
<td>You can add senders to administrator-defined groups and use Symantec Global Good Senders to deliver messages from good senders normally, or choose other actions. See “About blocking and allowing messages using sender groups” on page 143.</td>
</tr>
<tr>
<td>Fastpass</td>
<td>The Fastpass feature conserves resources by exempting senders with the best local reputation from spam scanning. Symantec Brightmail Gateway automatically collects local sender reputation data to support Fastpass determinations and regularly re-evaluates senders granted a pass. Symantec Brightmail Gateway grants and revokes passes based solely on how many messages from each sender it determines to be spam. You can exclude specific senders from ever receiving a pass. See “About conserving resources using Fastpass” on page 155. See “Configuring Fastpass” on page 157.</td>
</tr>
</tbody>
</table>

About managing connection load at the gateway

In most networks the great majority of email traffic today is spam. By intelligently managing connection load and distinguishing between connections from senders known to send spam and legitimate senders, you can significantly reduce processing costs. The Connection Classification feature dynamically manages connection load based on automatically collected local reputation data. 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.

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 and 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.

**Note:** To take advantage of Connection Classification, your Symantec Brightmail Gateway appliance must be deployed at the gateway.

Connection Classification works by assigning each connecting IP address to one of 10 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 Brightmail 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 Brightmail 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 35.

Symantec Brightmail 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 have been 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 be 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 136.

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 Brightmail 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 enable or disable Connection Classification

1. In the Control Center, click **Reputation > Policies > Connection Classification**. The Connection Classification page appears.

2. Check **Enable Connection Classification** to enable Connection Classification, or uncheck **Enable Connection Classification** to disable Connection Classification.

3. Click **Save**.

To configure Connection Classification

1. In the Control Center, click **Reputation > Policies > Connection Classification**. The Connection Classification page appears.

2. 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 138.

3. 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.

4. To change the connections that are allowed on a per-IP address basis, type new values in the **Maximum Connections per IP** fields.

5. To vary the number of messages that are allowed on a per-connection basis, type new values in the **Messages per Connection** fields.

6. To vary the time, in seconds, before a sender IP is allowed to reconnect, type new values in the **Reconnect Timeout** fields.
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%.

To abandon your changes and return to the default values, click **Load Defaults**.

If you are satisfied with your changes, click **Save**.

### Connection class default settings

Table 6-2 shows the default values for each connection class. A value of zero (0) indicates that there is no limit.

<table>
<thead>
<tr>
<th>Field</th>
<th>Class 1 (best)</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
<th>Class 5</th>
<th>Class 6</th>
<th>Class 7</th>
<th>Class 8</th>
<th>Class 9 (worst)</th>
<th>Maximum connections (must total 100%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum connections per IP</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>25</td>
<td>50</td>
<td>100</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Messages per connection</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>20</td>
<td>40</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Reconnect timeout</td>
<td>10 sec</td>
<td>60 sec</td>
<td>30 sec</td>
<td>30 sec</td>
<td>15 sec</td>
<td>5 sec</td>
<td>2 sec</td>
<td>1 sec</td>
<td>1 sec</td>
<td>0 sec</td>
</tr>
<tr>
<td>Deferred messages</td>
<td>10%</td>
<td>95%</td>
<td>80%</td>
<td>60%</td>
<td>30%</td>
<td>10%</td>
<td>5%</td>
<td>0%</td>
<td>0%</td>
<td></td>
</tr>
</tbody>
</table>

See “About managing connection load at the gateway” on page 134.

### 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 Brightmail 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 Brightmail Gateway takes upon recognizing a virus attack.

Symantec Brightmail 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 “Filtering actions and verdicts for email messages” on page 56.

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 Brightmail Gateway accepts inbound messages only for the domains you specify.  
  See “Adding or editing local domains” on page 81.

- Either:
Enable invalid recipient handling, configured to reject invalid recipients. See “Configuring invalid recipient handling” on page 88. Or,

Create and enable an LDAP source with synchronization configured, and wait until replication completes. See “About the supported LDAP services and directories” on page 477. See “About replicating data to Scanners” on page 504.

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 Brightmail 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 Brightmail Gateway takes upon recognizing a directory harvest attack.

Symantec Brightmail 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 “Filtering actions and verdicts for email messages” on page 56.
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” on page 74.

Symantec Brightmail Gateway lets you customize spam detection in the following ways:

- **Define good senders**: Symantec Brightmail 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 Brightmail 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.
Use global sender groups

By default, Symantec Brightmail 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 Brightmail 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.

Incorporate lists managed by other parties

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 message 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 6-3 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 6-3: Use cases for good and bad sender groups

<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 Administration &gt; Users &gt; Groups, edit the group containing the end user, and click on the End User 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” on page 74.</td>
<td><a href="mailto:colleague@trustedco.com">colleague@trustedco.com</a></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 148.</td>
<td><a href="mailto:latest@newsletter.com">latest@newsletter.com</a></td>
</tr>
<tr>
<td>An individual is sending unwanted mail 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 148.</td>
<td><a href="mailto:Joeunwanted@getmail.com">Joeunwanted@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 148. See “Supported methods for identifying senders” on page 154.</td>
<td>218.187.0.0/255.255.0.0</td>
</tr>
</tbody>
</table>

When evaluating domain name matches, Symantec Brightmail Gateway automatically expands the specified domain to include subdomains. For example, Symantec Brightmail 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 154.

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 Brightmail 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 Brightmail 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 Brightmail Gateway appliance.

See “Specifying internal mail hosts for non-gateway deployments” on page 123.

In addition to internal mail hosts you can add, Symantec Brightmail 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 Brightmail 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
Enabling or disabling good and bad sender groups

Follow the steps below to enable or disable sender groups.

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.

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.

3. Under Actions, click on the Perform the following action drop-down list and choose the action you want to add.

4. Click Add Action.
5 Repeat steps 3 and 4 to add more actions, if desired.
   Symantec Brightmail 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 “Filtering actions and verdicts for email messages” on page 56.

6 Inspect the Actions list and, if desired, delete one or more actions by checking
   the action and clicking Delete.

7 Click Save.

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 good or bad sender groups

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 page for that sender group appears.

3 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 154.

5 Click Save.

6 On the group 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.

To edit information for senders in your good or bad sender lists

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 on the page for that sender group, check the box next to the sender whose information you want to modify, and then 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 then click Save.
5. Click Save on the Group page.

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.

Enabling or disabling good and bad sender group members

When you add a new sender to a Sender Group, Symantec Brightmail 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 Brightmail 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 senders in your lists

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

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 sender information from 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.
   
   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 151.

5. Click **Import**.
   
   Symantec Brightmail 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 150.

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:

  ```
  dn: cn=mailwall, ou=bmi
  objectclass: top
  objectclass: bmiBlackWhiteList
  ```

- 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.

```ldif
## 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
|           |             | AC: 76.86.37.00/18   |
| 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   |
### Attribute | Description | Examples
--- | --- | ---
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.

**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, the 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:

<table>
<thead>
<tr>
<th>Method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-based</td>
<td>Specify IP connections. Symantec Brightmail Gateway checks the IP address of the mail server initiating the connection to verify if it is in your good sender groups or bad sender groups. Wildcards are not supported. Although you can use network masks to indicate a range of addresses, you cannot use subnet masks that define non-contiguous sets of IP addresses (for example, 69.84.35.0/255.0.255.0). The following notations are supported: ■ Single host: 128.113.213.4 ■ IP address with subnet mask: 128.113.1.0/255.255.255.0 ■ Classless Inter-Domain Routing (CIDR) IP address: 192.30.250.00/18</td>
</tr>
<tr>
<td>Third-party services</td>
<td>Supply the lookup domain of a third-party sender service. Symantec Brightmail Gateway can check the message source against third party DNS-based lists to which you subscribe—for example, list.example.org. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Domain-based</td>
<td>Specify sender addresses or domain names. Symantec Brightmail 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. You can use the * or ? wildcards in the pattern to match any portion of the address. ■ From: address in the message headers. Specify a pattern that matches the value for localpart@domain in the FROM: header. You can use wildcards in the pattern to match any portion of this value.</td>
</tr>
</tbody>
</table>

If you choose to identify senders by address or domain name, use the following examples to model entries when you add members to a sender group:
Scanning email messages for spam 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.

Once a source has received a pass, the amount of antispam processing applied to messages from that source decreases over time. The number of messages 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. Full antispam analysis is performed 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 two tables:

<table>
<thead>
<tr>
<th>Fastpass trial table</th>
<th>Contains entries 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fastpass table</td>
<td>Contains entries that have been granted a pass by Fastpass based on no spam coming from the IP address for a specified number of messages.</td>
</tr>
</tbody>
</table>

You can configure:
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, by specifying 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. If set to 1/3, for example, there may be occasions when 5 sequential different unknown IPs are not added, or when 2 IPs in a row are added.

The rate of growth of the Fastpass table, by specifying 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 and 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 compliance. 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 and suspected spam verdicts into account. Virus verdicts, compliance verdicts, spim verdicts, sender authentication verdicts, and sender group verdicts do not affect the granting or revoking of passes.
Configuring Fastpass

Fastpass conserves processing resources by exempting sending IP addresses with the best local reputation from spam scanning. Symantec Brightmail Gateway automatically collects data on the level of spam sent by each IP address, and uses this data to grant or revoke passes. After Symantec Brightmail Gateway grants a pass to a sender, it still scans a small sample of the email from that sender for spam. If Symantec Brightmail Gateway identifies a spam 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. Use the procedure below to enable or disable Fastpass. Fastpass is designed to work without any custom configuration. Advanced users can customize Fastpass using the procedures in this section.

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. To change the database size, type an integer between 1,000 and 1,000,000, inclusive in the Maximum number of sending IPs tracked in the database field.

Do not type commas. The default value is 250,000. The database includes two tables. The Fastpass trial table includes sending IPs 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.
To vary the rate of growth of the Fastpass trial table, type an integer between 1 and 100, inclusive, in the **Chance that a new IP will be added to the Fastpass trial table** field.

A smaller value will result in more frequent sampling. For example, a value of 1 means that every new IP that sends a legitimate message will be 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. The default value is 3, which indicates a 1 in 3 probability. All messages from IP addresses in the Fastpass trial table are scanned for spam. If a spam message is received, the entire /24 range of sending IP addresses is removed from both the Fastpass trial table and the Fastpass table.

To vary the rate of growth of the Fastpass table, type in integer between 1 and 1,000, inclusive, in the **Minimum required legitimate messages before granting fastpass** field.

Do not type commas. The default value is 15. 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.

To vary the rate at which IPs that have passes are checked for current behavior, type an integer between 2 and 50, inclusive, in the **Initial message sample rate after pass is issued** field.

A smaller value will result 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. A value of 25 means that 1 of every 25 messages is scanned for spam. The default value is 5, which indicates a 1 in 5 probability. 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.

**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 Brightmail 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 To import a list of IP addresses, click **Import**.

Imported files must be plain text files containing a single entry per line.

6 To delete and entry from the list, check the box next to the IP address and click **Delete**.

7 To delete all entries on the current page of the list, click **Delete All**.

8 To export the currently saved list of excluded IPs in a text file, click **Export**.

# 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.

Symantec Brightmail Gateway uses bounce attack prevention to eliminate NDRs that are a result of such redirection while still delivering legitimate NDRs.

To set up bounce attack prevention for your mail system, you must:

- Provide a Bounce attack prevention seed value in your Control Center.
  
  See “Configuring your 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 your groups for bounce attack prevention” on page 161.
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 policy for bounce attack prevention” on page 162.

Once your system is configured for bounce attack prevention, Symantec Brightmail 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 groups. If the message is returned as undeliverable, the envelope’s return address will contain this tag.

When the system receives a messages that appears to be a message returned as undeliverable, the system will compare the inbound message’s recipient with the group configuration to see if the user's group is configured for bounce attack prevention. If the 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 Brightmail 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.
Configuring your 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 159.

Create a seed value to be used when creating validation tags for outgoing messages

1 In your Control Center, select Administration > Settings > Control Center.
2 Under Control Center Certificate, enter a Bounce attack prevention seed. This seed value should consist of eight alphanumeric characters.
3 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.

You must now enable your user 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 user group, bounce attack prevention will be disabled and your system will not be protected from bounce attacks.

See “Configuring your groups for bounce attack prevention” on page 161.

A default 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 policy for bounce attack prevention” on page 162.

Configuring your groups for bounce attack prevention

Once you configure bounce attack prevention in the Control Center Settings page, you must enable the groups to which the system should apply validation and assign a bounce attack prevention policy.

See “About defending against bounce attacks” on page 159.

Configure your groups for bounce attack prevention

1 In your Control Center, select Administration > Groups.
2 Select the group you wish to edit, or create a new one, then select the Spam tab for that group.
3 Under **Email**, check **Enable bounce attack prevention for this 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 Brightmail 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 policy for bounce attack prevention” on page 162.

5 Click **Save**.

### Creating an email spam policy for bounce attack prevention

In order to enable bounce attack prevention, you must enable your user groups and assign a spam 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 159.

Symantec Brightmail 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 policy for bounce attack prevention conditions

1 In your Control Center, select **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.
Under Apply to the following groups, select or add the 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 IP 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. Clearing the sender policy removes the IP address from the Local Good Sender IPs or Local Bad Sender IPs group.

You can also reset the local reputation of this 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 Brightmail Gateway is deployed at the network edge. However, if you have deployed Symantec Brightmail 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 Brightmail 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 IP address that you want to query.

3 Click **Find**.

The following information is displayed for an IP address that you specify:
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Bad Reputation - Global Bad Senders</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>Request Removal</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>Bad Reputation - Local Bad Sender IPs</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>Good Reputation - Global Good Senders</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>
</tbody>
</table>
Table 6-4  
Reputation Status (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good Reputation - Local Good Sender IPs</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.

Table 6-5  
Local status

<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 Brightmail Gateway &quot;forgets&quot; 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 &quot;About managing connection load at the gateway&quot; on page 134.</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>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Current Action    | 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:  
  ■ Reject: This IP address is in a Bad Sender Group and the action for that group is to reject the SMTP connection  
  ■ Defer: This IP address is in a Bad Sender Group and the action for that group is to defer the SMTP connection.  
  ■ 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 Brightmail Gateway will not filter messages from this IP address for spam, the messages will undergo all other filtering, including antivirus filtering.  
  ■ Filter Partially: This IP address was granted a pass by the Fastpass feature. In most cases, Symantec Brightmail Gateway does not filter messages from this IP address for spam. However, Symantec Brightmail Gateway does filter a sample of the messages for spam. All the messages undergo all other filtering, including antivirus filtering.  
  ■ Filter Normally: This IP address has no negative local or global reputation, and has not been granted a pass by the Fastpass feature.                                                                                                                                                                                                 |
| Message Volume    | The quantity of messages from this IP address. One of the following four values appears:  
  ■ None (this is the default value)  
  ■ Low  
  ■ Medium  
  ■ High                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Total % Spam      | The percentage of messages from this IP address identified as spam                                                                                                                                                                                                                                                                                                                                                                                                               |
| Connection Class  | 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.                                                                                                                                                                                                                                        |
| Fastpass          | 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.                                                                                                                                                                                                                                                                                                                                 |
| DHA               | If this IP address is under DHA restriction based on your settings in Reputation > Bad Senders > Directory Harvest Attack, a green check appears. If not, a black dash appears.                                                                                                                                                                                                                                                                                                                                 |

Table 6-5: Local status (continued)
Table 6-5  Local status (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td>Last Message</td>
<td>The last time traffic was seen from this IP address.</td>
</tr>
</tbody>
</table>

Table 6-6  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
Detecting viruses and malicious attacks

This chapter includes the following topics:
- About detecting viruses and malicious attacks
- Creating email virus policies
- Modifying email virus policies
- Enabling or disabling email virus policies
- Deleting email virus policies
- Copying email virus policies
- Excluding file types from virus scanning
- Modifying the file types to exclude from scanning
- Enabling or disabling the lists of file types to exclude from scanning
- Deleting lists of file types to exclude from scanning
- Exporting lists of the file types to exclude from scanning
- Modifying the heuristic level
- Configuring container settings
- About updating virus definitions
About detecting viruses and malicious attacks

Viruses and other types of malicious attacks can wreak havoc in an organization. The damage can range from email server crashes to network downtime and the compromise and destruction of company data. Given the damage that can result from viruses and other types of malicious attacks, it is essential to employ virus protection as early in the mail flow process as possible. Virus and malicious threat detection is optional.

See “About configuring viruses and malicious threat detection” on page 172.

Create group policies to protect your server from the following types of attacks:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>Symantec Brightmail 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 171.</td>
</tr>
<tr>
<td>Mass-mailer worms</td>
<td>Symantec Brightmail 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 Brightmail 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 Brightmail Gateway to process encrypted container files.</td>
</tr>
<tr>
<td>Adware and spyware</td>
<td>Symantec Brightmail Gateway detects the security risks that do any of the following:</td>
</tr>
<tr>
<td></td>
<td>- Provide unauthorized access to computer systems</td>
</tr>
<tr>
<td></td>
<td>- Identity theft or fraud by logging keystrokes</td>
</tr>
<tr>
<td></td>
<td>- Capture email and instant messaging traffic</td>
</tr>
<tr>
<td></td>
<td>- Harvest personal information, such as passwords and logon identifications</td>
</tr>
<tr>
<td></td>
<td>- Present some type of disruption or nuisance</td>
</tr>
</tbody>
</table>

See “Spyware or adware verdict details” on page 180.

See “Creating email virus policies” on page 179.
Symantec Brightmail 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 “Configuring container settings” on page 189.

When Symantec Brightmail Gateway scans a message and detects a virus policy violation, it takes the verdict that you specify in that policy.

See “Selecting virus policies for a group” on page 68.

See Table 3-1 on page 54.

You must have a valid antivirus license to perform antivirus scanning functions. You must also have a valid content license to obtain updated virus definitions.

See “Licensing your product” on page 436.

### Product technologies that detect viruses and malicious attacks

Table 7-1 describes the technologies that Symantec Brightmail Gateway uses to detect viruses and malicious attacks.

<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>Heuristics technology</td>
<td>The product uses Symantec Bloodhound heuristic technology to detect virus-like behavior to identify and repair unknown viruses. You can adjust heuristic settings for more or less aggressive identification of viruses. The technology detects up to 90 percent of new macro viruses and up to 80 percent of new and unknown executable file viruses. You can modify the heuristics detection level. See “Modifying the heuristic level” on page 189.</td>
</tr>
</tbody>
</table>
Table 7-1  Technologies that detect viruses and malicious attacks *(continued)*

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
</table>
| Virus definitions| 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 from Symantec Security Response. By default, the appliance downloads certified virus definitions. However, you can obtain more frequent, less tested Rapid Response definitions. You can also obtain certified daily Platinum definitions for faster response to emerging threats.  
You can configure how and when you want to obtain updated definitions.  
See “About updating virus definitions” on page 191. |
| Antivirus policies| You can create policies to detect viruses or malicious attacks. When you create a policy, you specify the action that you want Symantec Brightmail 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 virus policies” on page 179. |
| Day-zero detection| 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 Brightmail 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 199. |

See “About detecting viruses and malicious attacks” on page 170.  
See “Product technologies that detect viruses and malicious attacks” on page 171.  

**About configuring viruses and malicious threat detection**

Table 7-2 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 7-2  Configure virus and malicious threat detection

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. Email virus attack recognition is disabled by default and must be enabled to be activated.  
See “Configuring email virus attack recognition” on page 138. |
| Create and enable email virus policies. | Symantec Brightmail Gateway comes with the pre-configured virus policies that are automatically enabled. You can modify these polices and create your own custom policies.  
See “About the default virus policies” on page 175.  
See “Creating email virus policies” on page 179. |
| Set the heuristic detection level. | Symantec Brightmail Gateway contains Symantec Bloodhound heuristics 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 Bloodhound off. Bloodhound heuristics involve a trade-off between higher virus detection rates and the speed with which Symantec Brightmail Gateway processes mail. Lower heuristic levels may miss more viruses but require less processing power. Higher heuristic levels may catch more viruses but consume more processing power.  
See “Modifying the heuristic level” on page 189. |
| 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 Brightmail 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 184. |
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure virus attack recognition.</td>
<td>Symantec Brightmail Gateway contains a feature that detects potential virus attacks.</td>
</tr>
<tr>
<td></td>
<td>This feature is disabled by default. When you enable the feature, Symantec Brightmail Gateway applies default settings. You can use these default settings or you can modify them.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring email virus attack recognition” on page 138.</td>
</tr>
<tr>
<td>Configure the Suspect Virus Quarantine.</td>
<td>You can create virus policies to quarantine suspicious message attachments in the Suspect Virus Quarantine.</td>
</tr>
<tr>
<td></td>
<td>Symantec provides default values for the following Suspect Virus Quarantine settings; however, you can change these settings as needed:</td>
</tr>
<tr>
<td></td>
<td>■ Maximum amount of the time that messages are held in the quarantine</td>
</tr>
<tr>
<td></td>
<td>The default setting is 6 hours.</td>
</tr>
<tr>
<td></td>
<td>■ Disk space available for the quarantine</td>
</tr>
<tr>
<td></td>
<td>The default setting is 10 GB.</td>
</tr>
<tr>
<td></td>
<td>See “About quarantining suspected viruses” on page 199.</td>
</tr>
<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.</td>
</tr>
<tr>
<td></td>
<td>See “About updating virus definitions” on page 191.</td>
</tr>
<tr>
<td>Configure outbreak notification alerts.</td>
<td>Set up alert notifications to let you know any of the following virus-related events occur:</td>
</tr>
<tr>
<td></td>
<td>■ An outbreak is detected</td>
</tr>
<tr>
<td></td>
<td>■ Virus filters are older than the time period that you specify</td>
</tr>
<tr>
<td></td>
<td>■ New virus filters are available</td>
</tr>
<tr>
<td></td>
<td>■ The antivirus license has expired</td>
</tr>
<tr>
<td></td>
<td>See “Types of alerts” on page 447.</td>
</tr>
</tbody>
</table>
Table 7-2  Configure virus and malicious threat detection (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor reports.</td>
<td>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. See “About working with reports” on page 356.</td>
</tr>
</tbody>
</table>

About the default virus policies

Symantec Brightmail Gateway installs with pre-configured virus policies. These policies are enabled by default. You can disable the policies that you do not want to use. You can also modify the policy actions and the 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 “Selecting virus policies for a group” on page 68.

Table 7-3 lists the pre-configured virus policies.

Table 7-3  Pre-configured virus 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 user 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: Delete message</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for viruses</td>
<td>Delete the message</td>
<td>Default group</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 user group</td>
<td>Default status</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------</td>
<td>--------------------------------------</td>
<td>--------------------------</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>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>
</tbody>
</table>
### Table 7-3: Pre-configured virus 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 user group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<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: Modify subject line with &quot;[WARNING -NOT VIRUS SCANNED]&quot;</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for viruses</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: Deliver normally</td>
<td>Inbound and outbound messages</td>
<td>Message is unscannable for viruses</td>
<td>Deliver the message normally</td>
<td>None</td>
<td>Enabled by default</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 180.</td>
<td>Prepend the subject line with &quot;[SPYWARE OR ADWARE INFECTED]&quot;</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
</tbody>
</table>
Table 7-3 Pre-configured virus 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 user group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound suspect virus: Strip attachments and hold 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>

See “Creating email virus policies” on page 179.
See “Modifying email virus policies” on page 181.
See “Enabling or disabling email virus policies” on page 182.
See “Deleting email virus policies” on page 183.
See “Copying email virus policies” on page 183.

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 199.

See “Creating email virus policies” on page 179.

Creating email virus policies

Symantec Brightmail Gateway installs with pre-configured virus the policies that are enabled by default. In addition to these policies, you can create your own custom policies. Compliance, spam, and virus policy names must be unique. For example, if you have a compliance policy called XYZ, you cannot have a spam policy or virus policy called XYZ. Email virus policies are enabled by default when you create them.

See “About the default virus policies” on page 175.

See “Modifying email virus policies” on page 181.

See “Enabling or disabling email virus policies” on page 182.

See “Deleting email virus policies” on page 183.

See “Copying email virus policies” on page 183.

To create email virus policies

1  In the Control Center, click Virus > Policies > Email.

2  Click Add.

3  In the Policy name box, type a name for the virus policy.

4  Under Conditions, click the Apply todrop-down list and choose to which type of message the virus policy should apply:

   ▪ Inbound messages
   ▪ Outbound messages
   ▪ Inbound and Outbound messages
This option specifies where this virus policy is available on the Virus tab when you configure a group.
For example, assume you choose Inbound messages and the If the message contains a mass-mailing worm condition. This virus policy is only available in the Inbound mass-mailing worm policy drop-down list when you configure a group.

5 Click the If the following condition is met drop-down list to select a condition.
See “What you can do with suspicious attachments” on page 178.

6 Under Actions, click the Perform the following action drop-down list and select an action.
See “Selecting virus policies for a group” on page 68.
For some actions you need to specify additional information in the fields beneath the action.
For example, assume 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 which you want to forward the message.

7 Click Add Action to add more actions, if needed.
See “User interface action combinations” on page 509.

8 Under Groups, check one or more groups to which this policy should apply.

9 Click Save.

Spyware or adware verdict details
Symantec Brightmail 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 Brightmail Gateway applies the spyware or adware verdict to all of the security risks that it detects.
See “About detecting viruses and malicious attacks” on page 170.
Table 7-4 lists the categories of security risks that Symantec Brightmail Gateway detects.
### Table 7-4

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<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>

### Modifying email virus policies

You can modify default and custom email virus policies to fine-tune them or to expand or reduce their scope.

Table 7-5 describes the setting that you can modify for default email virus policies and custom email virus policies.

### Table 7-5

<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>
</tbody>
</table>
Table 7-5  Modifiable email virus 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>Apply to</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>If the following condition is met</td>
<td>Yes</td>
<td>Yes</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>

See “About the default virus policies” on page 175.
See “Enabling or disabling email virus policies” on page 182.
See “Deleting email virus policies” on page 183.
See “Copying email virus policies” on page 183.

To modify email virus policies
1. In the Control Center, click **Virus > 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 virus policies

Default email virus policies are enabled by default. When you create a new email virus policy, it is enabled by default. You can disable any policy that you do not want Symantec Brightmail Gateway to use when it scans email messages.

You can disable a virus policy to troubleshoot email virus scanning issues. You can also create custom email virus policies to use for outbreaks and 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.

See “Creating email virus policies” on page 179.
See “About the default virus policies” on page 175.
See “Modifying email virus policies” on page 181.
See “Deleting email virus policies” on page 183.

To enable or disable email virus policies

1. In the Control Center, click Virus > Policies > Email.
2. Check the box beside the policy that you want to enable or disable.
3. Click 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 email virus policies

You can delete the email virus 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 virus policies” on page 182.

To delete email virus policies

1. In the Control Center, click Virus > 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 virus policies

You may have instances in which you create a complicated email antivirus policy and want to create a similar policy with only a few variances. Symantec Brightmail Gateway lets you copy email virus policies.

When you copy an email virus policy, the new policy must have a unique name. For example, if you have a compliance policy called XYZ, you cannot have a spam policy or virus policy called XYZ. Email virus policies are enabled by default when you create them.
See “Creating email virus policies” on page 179.
See “About the default virus policies” on page 175.
See “Modifying email virus policies” on page 181.
See “Enabling or disabling email virus policies” on page 182.
See “Deleting email virus policies” on page 183.

To copy email virus policies
1. In the Control Center, click Virus > Policies > Email.
2. Check the box beside the policy that you want to copy.
3. Click Copy.
4. On the Email Virus Policies page, type a new name for the policy.
5. Make any other changes you want.
6. Click Save.

Excluding file types from virus scanning

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.

Symantec Brightmail Gateway lets you create the lists that contain the file types that can bypass antivirus scanning. Multiple lists can help you categorize the file types.

When you create a list, select from the following pre-configured lists:

File classes | Symantec Brightmail Gateway provides pre-configured file classes from which to choose.
---|---
An example of some file classes are as follows:
- Movie file
- Library format
- Desktop publishing

The All File Classes file class contains all of the file types in all of the file classes.
When you select a file class, the pre-configured file types for that class appear.

You can select all of the file types for a file class to include in the Exclude scanning list. Or you can select only the file types that you want to include in the list.

The list must be enabled if you want it to be used during scans. When you create a new list, it is enabled by default.

See “Modifying the file types to exclude from scanning” on page 186.

See “Enabling or disabling the lists of file types to exclude from scanning” on page 187.

See “Deleting lists of file types to exclude from scanning” on page 187.

See “Exporting lists of the file types to exclude from scanning” on page 188.

**To exclude file types from virus scanning**

1. In the Control Center, click **Virus > Settings > Scan Settings**.
2. Click the **Exclude Scanning** tab.
3. Click **Add** to create a definition of files for exclusion from virus scanning.
4. In the Exclude scanning list name box, type a name for the list.
5. 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.
6. Perform one of the following tasks:

   To exclude all file types in a class or group of classes
   
   Click **Add File Classes**.

   To exclude only certain file types
   
   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**.

7. Click **Save**.

   The names of the file types appear in the Description list.
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 virus 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 184.

See “Enabling or disabling the lists of file types to exclude from scanning” on page 187.

See “Deleting lists of file types to exclude from scanning” on page 187.

See “Exporting lists of the file types to exclude from scanning” on page 188.

To modify the file types to exclude from scanning

1. In the Control Center, click Virus > Settings > Scan Settings.
2. Click the Exclude Scanning tab.
3. Check the box besides the Exclude Scanning List that you want to modify.
4. Click Edit
5. Do any of the following tasks:

   - To add a file type to the list
     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.
     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.

6. Click Save.
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 Brightmail 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 outbreaks 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.

See “Excluding file types from virus scanning” on page 184.
See “Modifying the file types to exclude from scanning” on page 186.
See “Deleting lists of file types to exclude from scanning” on page 187.
See “Exporting lists of the file types to exclude from scanning” on page 188.

To enable or disable the lists of file types to exclude from scanning

1. In the Control Center, click Virus > Settings > Scan Settings.
2. Click the Exclude Scanning tab.
3. Check the box beside the policy that you want to enable to disable.
4. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>When you enable a policy, a green check mark appears in the Enabled column.</td>
</tr>
<tr>
<td>Disable</td>
<td>When you disable a policy, a horizontal line appears in the Enabled column.</td>
</tr>
</tbody>
</table>

Deleting lists of 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.
To delete lists of file types to exclude from scanning
1 In the Control Center, click Virus > Settings > 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 OK 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.

See “Excluding file types from virus scanning” on page 184.
See “Modifying the file types to exclude from scanning” on page 186.
See “Enabling or disabling the lists of file types to exclude from scanning” on page 187.
See “Deleting lists of file types to exclude from scanning” on page 187.

To export lists of file types to exclude from scanning
1 In the Control Center, click Virus > Settings > 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.
Modifying the heuristic level

The heuristic level determines the way in which the system uses heuristics to detect viruses. Symantec Brightmail Gateway uses Symantec Bloodhound heuristics technology to scan for threats for which no known definitions exist. Bloodhound heuristics technology scans for unusual behaviors, such as self-replication, to target potentially infected message bodies and attachments. Bloodhound technology can detect up to 80 percent of new and unknown executable file threats. Bloodhound-Macro technology detects and repairs over 90 percent of new and unknown macro viruses.

Bloodhound requires minimal overhead because it examines only message bodies and attachments that meet stringent prerequisites. In most cases, Bloodhound determines in microseconds whether a message or attachment is likely to be infected. If it determines that a file is not likely to be infected, it moves to the next file.

Bloodhound heuristics involve a trade-off between higher virus-detection rates and the speed with which Symantec Brightmail Gateway processes mail. Lower heuristic levels may miss more viruses but require less processing power. Higher heuristic levels may catch more viruses but consume more processing power.

See “About detecting viruses and malicious attacks” on page 170.

See “About configuring viruses and malicious threat detection” on page 172.

See “Product technologies that detect viruses and malicious attacks” on page 171.

To modify the heuristic level

1. Click Virus > Settings > Scan Settings.
2. Click the General tab.
3. Under Bloodhound Level, click the level that you want.
   The default setting is Medium.
4. Click Save.

Configuring container settings

When Symantec Brightmail Gateway processes certain zip files and other types of 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 Brightmail 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 Brightmail Gateway processes in memory. You can also specify a time limit for scanning containers. If a configured limit is reached, Symantec Brightmail Gateway performs the action that you specify for the Unscannable for viruses 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. 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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum time to open container</td>
<td>The specified time elapses during a scan of container attachments (such as .zip files). 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>
</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>

See “About detecting viruses and malicious attacks” on page 170.

See “About configuring viruses and malicious threat detection” on page 172.

See “Product technologies that detect viruses and malicious attacks” on page 171.

To configure container settings

1. In the Control Center, click Protocols > SMTP > Settings.
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.

About updating virus definitions

Symantec Brightmail 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.

Table 7-6 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.</td>
</tr>
<tr>
<td></td>
<td>See “Scheduling automatic virus definition updates” on page 193. See “Initiating virus definition updates on demand” on page 194.</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 Brightmail 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 195.

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.
Viewing the status of your virus definitions

Symantec Brightmail Gateway provides details about the status of your virus definitions.

The LiveUpdate status provides the following details:

<table>
<thead>
<tr>
<th>Last LiveUpdate attempt</th>
<th>The day, date, and time that Symantec Brightmail Gateway last attempted a virus definition update.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last virus definitions LiveUpdate status</td>
<td>Whether the last attempted virus definition update was successful.</td>
</tr>
<tr>
<td>Virus definitions version (revision)</td>
<td>The version of the current virus definitions.</td>
</tr>
<tr>
<td>Current virus definition manifest</td>
<td>A list of virus definitions that are contained in this update.</td>
</tr>
</tbody>
</table>

See “About updating virus definitions” on page 191.

See “Scheduling automatic virus definition updates” on page 193.

See “Disabling automatic virus definition updates” on page 194.

See “Initiating virus definition updates on demand” on page 194.

See “Obtaining definitions when a new, emerging threat is discovered” on page 196.

See “Specifying from where to obtain virus definitions” on page 195.

To view the status of your virus definitions

◆ In the Control Center, click Virus > Settings > LiveUpdate.

   The LiveUpdate status appears under LiveUpdate Settings.

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 Brightmail Gateway to attempt to obtain virus definitions.

You can only schedule automatic updates through LiveUpdate. Rapid Response does not support scheduled updates.

See “Specifying from where to obtain virus definitions” on page 195.

See “Disabling automatic virus definition updates” on page 194.
To schedule automatic virus definition updates

1  In the Control Center, click **Virus > Settings > LiveUpdate**.
2  Under LiveUpdate Schedule, click **Enable automatic updates on the following schedule**.
3  Specify a day or days of the week and time at which to begin LiveUpdate.
4  Specify the time that you want the first LiveUpdate attempt to begin.
5  Specify the frequency (in minutes) with which LiveUpdate runs after the first time.
   Enter a value between 3 and 60. The default value is 10.
6  Specify how long Symantec Brightmail Gateway should attempt the LiveUpdate before it times out.

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.

See “Initiating virus definition updates on demand” on page 194.
See “Scheduling automatic virus definition updates” on page 193.
See “Initiating virus definition updates on demand” on page 194.
See “Obtaining definitions when a new, emerging threat is discovered” on page 196.
See “Specifying from where to obtain virus definitions” on page 195.

To **disable automatic virus definition updates**

1  In the Control Center, click **Virus > 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.

See “Viewing the status of your virus definitions” on page 193.
See “Obtaining definitions when a new, emerging threat is discovered” on page 196.
See “Specifying from where to obtain virus definitions” on page 195.

To initiate virus definition updates on demand

1. Click Virus > Settings > LiveUpdate.
2. Click LiveUpdate Now.

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 Brightmail 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 193.
See “Initiating virus definition updates on demand” on page 194.
See “Obtaining definitions when a new, emerging threat is discovered” on page 196.

To obtain virus definition updates from Symantec LiveUpdate server

1. In the Control Center, click Virus > Settings > LiveUpdate.
2. Under Source, click Download Platinum virus definitions from the Symantec web site.

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 Virus > 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.

Obtaining definitions when a new, emerging threat is discovered

You can use Rapid Response when you need quick responses to emerging threats. Rapid Response definitions are most useful for a perimeter defense to mitigate quickly spreading threats.

**Warning:** Rapid Response definitions do not undergo the same rigorous quality assurance testing as LiveUpdate definitions. Symantec encourages users to rely on the full quality-assurance-tested definitions whenever possible. Ensure that you deploy Rapid Response definitions to a test environment before you install them on your network.

When you enable Rapid Response virus definition updates, Symantec Brightmail Gateway uses the Symantec Web site as the source for definition updates by default. But you can modify the source to a LAN host.

See “Specifying from where to obtain virus definitions” on page 195.

You cannot schedule definition updates through Rapid Response. If you want to schedule automatic virus definition updates, use LiveUpdate.
See “Scheduling automatic virus definition updates” on page 193.

To obtaining definitions when a new, emerging threat is discovered

1. Click **Virus > Settings > LiveUpdate**.
2. Click **Enable Rapid Response updates**.
   Symantec Brightmail Gateway checks for updated definitions every 10 minutes after this setting is saved.
3. Click **Save**.
Detecting viruses and malicious attacks

About updating virus definitions
Quarantining suspected viruses

This chapter includes the following topics:

- About quarantining suspected viruses
- Viewing suspect virus messages in quarantine
- Choosing the language encoding for suspect virus messages
- Specifying the number of suspect virus message entries to view per page
- About navigating Suspect Virus Quarantine
- Sorting suspect virus messages in quarantine
- Searching quarantined virus messages
- Deleting suspect virus messages in quarantine
- Releasing suspect virus messages from quarantine
- Specifying how long suspect virus messages are retained in quarantine
- Modifying the disk space allotted for Suspect Virus Quarantine

About quarantining suspected viruses

Symantec Brightmail Gateway can quarantine the suspicious messages that might contain viruses. Messages are held in Suspect Virus Quarantine for the period of time that you specify (6 hours by default). Then the messages are released and rescanned. This delay provides time for Symantec to release updated virus definitions with which to scan the suspicious messages. If Symantec Brightmail
Gateway rescans the message, is unable to detect a virus, but still deems the attachment suspicious, the message is returned to Suspect Virus Quarantine.

See “Specifying how long suspect virus messages are retained in quarantine” on page 207.

To use the quarantine, your virus policy must use one of the following actions for suspicious attachments:

- Hold message in Suspect Virus Quarantine
- Strip and Delay in Suspect Virus Quarantine

See “Creating email virus policies” on page 179.

You can do the following with the messages that are in Suspect Virus Quarantine:

- View messages
  See “Viewing suspect virus messages in quarantine” on page 200.
- Sort messages
  See “Sorting suspect virus messages in quarantine” on page 203.
- Search messages
  See “Searching quarantined virus messages” on page 203.
- Delete messages
  See “Deleting suspect virus messages in quarantine” on page 206.
- Release messages
  See “Releasing suspect virus messages from quarantine” on page 206.

Quarantined messages are stored on the Control Center. You can specify the amount of disk space that you want to allocate to Suspect Virus Quarantine.

See “Modifying the disk space allotted for Suspect Virus Quarantine” on page 207.

### 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.

See “About navigating Suspect Virus Quarantine” on page 202.

See “Specifying the number of suspect virus message entries to view per page” on page 201.

See “Sorting suspect virus messages in quarantine” on page 203.

See “Searching quarantined virus messages” on page 203.
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.

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 200.

See “About navigating Suspect Virus Quarantine” on page 202.

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 Virus > 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 Virus > Quarantine > Email Suspect Virus.
2. Click the Entries per page drop-down list, and select a number.

**About navigating 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**
- **Go to the end of messages. This icon is displayed if there are less than 50 pages of messages after the current page.**
- **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 200.

See “Specifying the number of suspect virus message entries to view per page” on page 201.

See “Sorting suspect virus messages in quarantine” on page 203.

See “Searching quarantined virus messages” on page 203.
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.

See “Viewing suspect virus messages in quarantine” on page 200.

See “Specifying the number of suspect virus message entries to view per page” on page 201.

See “About navigating Suspect Virus Quarantine” on page 202.

See “Searching quarantined virus messages” on page 203.

To sort suspect virus messages in quarantine

1. From the Control Center, click Virus > Quarantine > Email Suspect Virus.
2. Click on the Date column heading to sort by ascending order or descending order.

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.

See “Viewing suspect virus messages in quarantine” on page 200.

See “Specifying the number of suspect virus message entries to view per page” on page 201.

See “About navigating Suspect Virus Quarantine” on page 202.

See “Sorting suspect virus messages in quarantine” on page 203.

To search quarantined virus messages

1. In the Control Center, click Virus > 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 Brightmail 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
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.

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:

Tokens

Tokens are matched with substring semantics. Searching for a subject with the search target `<in>` will match "Lowest rate in 45 years," "RE: re: Sublime Bulletin (verification)," "Up to 85% off Ink Cartridges + no shipping!," and "Re-finance at todays super low rate."

Multiple word searches

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 "red carpet," "red wine," and "flying carpet."

Case sensitivity

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.

Exact phrases

To search for an exact phrase, enclose the phrase in " " (double quotes).

Wildcards

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 & (ampersand), ! (exclamation point), $ (dollar sign), and # (pound sign).

Single characters

Even a single character is treated as a substring target.

Special characters

You can search on special characters such as & (ampersand), ! (exclamation point), $ (dollar sign), and # (pound sign).

Multiple characteristics

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.

Forged header information

Spammers usually "spoof" 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.

Time to perform a search

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.

See “Searching quarantined virus messages” on page 203.
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 200.

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 207.

To delete individual messages in quarantine

1. From the Control Center, click Virus > 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 Virus > 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 Brightmail 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 of the messages at once.

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 206.
To release individual messages from quarantine
1. From the Control Center, click Virus > Quarantine > Email Suspect Virus.
2. Click on the check box to the left of each message that you want to release.
3. Click Release.
See “About Scanner email settings” on page 98.

To release all messages from quarantine
1. From the Control Center, click Virus > Quarantine > Email Suspect Virus.
2. Click Release All to release all the messages in Suspect Virus Quarantine, including those on other pages.

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. Only administrators with Full Administration rights or Manage Settings modify rights can modify Suspect Virus Quarantine settings.

See “Modifying the disk space allotted for Suspect Virus Quarantine” on page 207.
You can also delete messages manually from Suspect Virus Quarantine.
See “Deleting suspect virus messages in quarantine” on page 206.

To specify how long suspect virus messages are held in quarantine
1. On the Control Center, click Virus > 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 6 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.

See “Specifying how long suspect virus messages are retained in quarantine” on page 207.

See “Deleting suspect virus messages in quarantine” on page 206.

See “Releasing suspect virus messages from quarantine” on page 206.

**To modify the disk space allotted for Suspect Virus Quarantine**

1. Click Virus > 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**.
Filtering spam

This chapter includes the following topics:

■ About filtering spam
■ Creating email spam policies
■ Enabling and disabling spam policies
■ Modifying spam policies
■ Copying spam policies
■ Deleting spam policies
■ Identifying messages written in specific languages
■ Configuring the threshold for suspected spam identification

About filtering spam

Symantec Brightmail Gateway comes with default spam policies that are enabled by default. However, you can modify these policies or create your own.

See “About the default spam policies” on page 210.
See “Creating email spam policies” on page 211.

You can also modify the settings that further detect spam.

See “Configuring the threshold for suspected spam identification” on page 216.
See “Identifying messages written in specific languages” on page 215.

You can specify how you want spam or suspected spam 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.
See Table 3-2 on page 57.

See “Filtering actions and verdicts for email messages” on page 56.

See “About quarantining spam” on page 220.

## About the default spam policies

Symantec Brightmail Gateway installs with pre-configured spam policies. You can only modify the policy actions and the groups to which the policies apply.

See “Selecting spam and spim policies for a group” on page 71.

Table 9-1 lists the pre-configured spam policies.

### Table 9-1  Pre-configured 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 user 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 by default</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 by default</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 the message</td>
<td>Default group</td>
<td>Enabled by default</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 the message in Spam Quarantine</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
</tbody>
</table>
Table 9-1  Pre-configured 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 user group</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam or Suspected Spam: Deliver to Spam folder</td>
<td>Inbound and outbound</td>
<td>If a message is spam or suspected spam</td>
<td>Deliver the message to the recipient's spam folder</td>
<td>Default group</td>
<td>Enabled by default</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>Default group</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Failed Bounce Attack Validation: Reject message</td>
<td>Inbound only</td>
<td>If a bounce message does not pass tag validation</td>
<td>Rejects messages failing bounce attack validation</td>
<td>Default group</td>
<td>Enabled by default</td>
</tr>
</tbody>
</table>

See “Creating email spam policies” on page 211.
See “Enabling and disabling spam policies” on page 213.

Creating email spam policies

You can create the email spam policies that determine the actions to be taken for specific spam conditions.

Symantec Brightmail Gateway installs with several pre-configured policies. You can use these policies as is, edit them to suit your needs, or create your own custom policies.

See “About the default spam policies” on page 210.
When you create a new spam policy, it is enabled by default.
See “Enabling and disabling spam policies” on page 213.
See “Modifying spam policies” on page 213.
See “Copying spam policies” on page 214.
See “Deleting spam policies” on page 215.
To create the policies that detect spam

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.

   Compliance, spam, and virus policy names must be unique. For example, if you have a compliance policy called "XYZ," you cannot have a spam policy or virus 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 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 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 the **Perform the following action** drop-down list and select the action that you want to take on a message that meets the specified spam condition.

   For some actions, you need to specify additional information.

   See Table 3-2 on page 57.

   See “Filtering actions and verdicts for email messages” on page 56.

   See “About defending against bounce attacks” on page 159.

7. Click **Add Action**.

8. If you want, add more actions.

   See Table A-3 on page 510.
9 Under Apply to the following groups, check one or more groups to which this policy should apply.

See “Creating groups and adding or removing members” on page 64.

10 Click Save.

Enabling and disabling spam policies

Default and newly created spam policies are enabled by default. When you create a new spam policy, it is enabled by default. You can disable any policy that you do not want Symantec Brightmail Gateway to use when it scans email messages.

You can disable a virus 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.

See “About filtering spam” on page 209.

See “Creating email spam policies” on page 211.

See “Modifying spam policies” on page 213.

See “Copying spam policies” on page 214.

See “Deleting spam policies” on page 215.

To enable or disable spam 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.

Modifying spam policies

You can modify spam policies to fine-tune them or to expand or reduce their scope.

Table 9-2 describes the setting that you can modify for default spam policies and custom spam policies.
Table 9-2 Modifiable spam 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>Yes</td>
</tr>
<tr>
<td>If the following condition is met</td>
<td>Yes</td>
<td>Yes</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>

See “About filtering spam” on page 209.
See “Creating email spam policies” on page 211.
See “Enabling and disabling spam policies” on page 213.
See “Copying spam policies” on page 214.
See “Deleting spam policies” on page 215.

To modify spam 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.

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 Brightmail 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 compliance policy called XYZ, you cannot have a spam policy or virus policy called XYZ. Spam policies are enabled by default when you create them.

See “About filtering spam” on page 209.
See “Creating email spam policies” on page 211.
See “Enabling and disabling spam policies” on page 213.
See “Modifying spam policies” on page 213.
See “Deleting spam policies” on page 215.

**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 policies” on page 213.
See “Copying spam policies” on page 214.
See “Modifying spam policies” on page 213.

**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 **OK** in the confirmation dialog box.

**Identifying messages written in specific languages**

If you use the Outlook Spam Plug-in, you can block or allow any messages that are written in a specific language. For example, you can choose to only allow English and Spanish messages. Or you can block messages in English and Spanish and allow messages in all other languages.

**Note:** Symantec no longer provides technical support for the Outlook Spam Plug-in.

See “About filtering spam” on page 209.
To identify messages written in specific languages

1. In the Control Center, click Spam > Settings > Scan Settings.
2. Click the Email tab.
3. Under Language Identification, click Yes if you have installed the Symantec Outlook Spam Plug-in and want to enable its Language feature.
4. Click Save.

Configuring the threshold for suspected spam identification

When Symantec Brightmail 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 Brightmail Gateway categorizes the spam scores as follows:

<table>
<thead>
<tr>
<th>Score 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</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. 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 Brightmail 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>75 by default</td>
<td>If a message receives a score that is less than the suspected spam threshold, Symantec Brightmail 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 spam” on page 209.

To configure the threshold for suspected spam identification

1 In the Control Center, click Spam > Settings > Scan Settings.
2 Click the Email tab.
3 Under Do you want messages to be flagged as suspected spam, click Yes or No.
4 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.
5 Click Save.
Filtering spam

Configuring the threshold for suspected spam identification
Quarantining spam

This chapter includes the following topics:

■ About quarantining spam
■ Before you use Spam Quarantine
■ Forwarding spam messages for non-existent addresses to quarantine
■ Configuring Spam Quarantine for administrator-only access
■ Viewing spam and suspected messages in quarantine
■ Viewing spam and suspected spam messages sent to the postmaster mailbox
■ About navigating Spam Quarantine
■ Specifying the number of entries to appear on the Spam Quarantine Message list page
■ Sorting spam and suspected messages in quarantine by date
■ Redelivering messages misidentified as spam
■ Deleting spam messages in quarantine
■ Searching quarantined spam messages
■ Viewing spam message headers
■ Choosing the language encoding for spam messages
■ Modifying Spam Quarantine thresholds
■ Specifying who to notify of false positive messages
■ About configuring the user and distribution list notification digests
■ Specifying how long spam messages are retained in quarantine
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.

See “Creating email spam policies” on page 211.

See “Before you use Spam Quarantine” on page 220.

See “Viewing spam and suspected messages in quarantine” on page 223.

See “About navigating Spam Quarantine” on page 226.

Spam Quarantine stores spam messages, and it 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.

See “Configuring Spam Quarantine for administrator-only access” on page 222.

See “Specifying who to notify of false positive messages” on page 236.

See “About configuring the user and distribution list notification digests” on page 237.

You can configure thresholds to control the space that is allocated for Spam Quarantine.

See “Modifying Spam Quarantine thresholds” on page 234.

See “Specifying when and how often Spam Quarantine is purged” on page 245.

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:
<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and enable the spam policies that quarantine spam and suspected spam.</td>
<td>One or more 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 email spam policies” on page 211.</td>
</tr>
<tr>
<td>Configure your LDAP server and ensure it works properly.</td>
<td>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 LDAP synchronization” on page 481.</td>
</tr>
<tr>
<td>Ensure that you have an SMTP mail server available.</td>
<td>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 118.</td>
</tr>
</tbody>
</table>

See “About quarantining spam” on page 220.

**Forwarding spam messages for non-existent addresses to quarantine**

If LDAP is configured, the messages that are sent to non-existent email addresses (based on LDAP lookup) are deleted by default. If you uncheck the check box for Delete messages sent to unresolved email addresses, these messages are stored in the Spam Quarantine postmaster mailbox. Only the administrators that have Full Administration rights or Manage Settings modify rights can modify this setting.

See “Viewing spam and suspected spam messages sent to the postmaster mailbox” on page 225.

The deletion of unresolved email is disabled by default if LDAP is not configured. In that case, the option Delete messages sent to unresolved email addresses is unchecked and is grayed out.
Note: If an LDAP server connection fails or LDAP settings have not been configured correctly, then quarantined messages addressed to non-existent users 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.

See “About quarantining spam” on page 220.

To forward spam messages for non-existent addresses to quarantine
1. In the Control Center, click Spam > Settings > Quarantine Settings.
2. Uncheck Delete messages sent to unresolved email addresses.
3. Click Save.

Configuring Spam Quarantine for administrator-only access

If you do not have an LDAP directory server configured or do not want users in your LDAP directory to access Quarantine, you can configure Quarantine so that only administrators can access the messages in Quarantine.

When administrator-only access is enabled, you can still perform all the administrator tasks available for sites with LDAP integration enabled. These tasks include redelivering misidentified messages to local users, whether or not you use an LDAP directory at your organization. However, notification of new spam messages is disabled when administrator-only access is enabled.

The Administrator-only Quarantine option is enabled by default if LDAP is not configured. In that case, this option is checked and grayed out.

See “Viewing spam and suspected messages in quarantine” on page 223.

See “How Spam Quarantine differs for administrators and users” on page 224.

To configure Spam Quarantine for administrator-only access
1. In the Control Center, click Spam > Settings > Quarantine Settings.
2. If it is unchecked, check Administrator-only Quarantine.
3. Click Save.
Viewing spam and suspected 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 suppress 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 226.

See “Configuring Spam Quarantine for administrator-only access” on page 222.

See “How Spam Quarantine differs for administrators and users” on page 224.
To view spam and suspected 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 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.

How Spam Quarantine differs for administrators and users

Table 10-1 describes the differences between the Spam Quarantine for administrators and users.
Table 10-1  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. Quarantine administrators can view and delete all users’ quarantined messages, either one by one, deleting all messages, or deleting the results of a search.</td>
</tr>
<tr>
<td></td>
<td>■ When users click Release, the message is delivered to their own inbox. When a Quarantine administrator clicks Release, the message 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 contains the intended recipient of each message. Users can only see 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 Center.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Users access Spam Quarantine by logging into the Control Center. They use the user name and password that your LDAP server requires.</td>
</tr>
<tr>
<td>Message Details page</td>
<td>Users can only view and delete their own quarantined messages. Quarantine administrators can view and delete messages for all users.</td>
</tr>
<tr>
<td>Search filters</td>
<td>Quarantine administrators can search for recipients. In the search results, users can only delete their own quarantined messages. Quarantine administrators can delete all users’ quarantined messages.</td>
</tr>
</tbody>
</table>

See “Configuring Spam Quarantine for administrator-only access” on page 222.

See “Viewing spam and suspected messages in quarantine” on page 223.

See “About navigating Spam Quarantine” on page 226.

**Viewing spam and suspected spam messages sent to the postmaster mailbox**

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 accessible from 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.

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.

See “Viewing spam and suspected messages in quarantine” on page 223.

See “About navigating Spam Quarantine” on page 226.

See “Configuring Spam Quarantine for administrator-only access” on page 222.

See “How Spam Quarantine differs for administrators and users” on page 224.

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.

About navigating Spam Quarantine

The following icons show how to navigate through the Spam Quarantine message list page:

- Go to beginning of messages
- Go to the end of messages
  - This icon appears when there are less than 50 pages of messages after the current page.
- 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:
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 messages in quarantine” on page 223.
See “About navigating Spam Quarantine” on page 226.

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 messages in quarantine” on page 223.

See “About navigating Spam Quarantine” on page 226.

See “Searching quarantined spam messages” on page 230.

See “Viewing spam message headers” on page 233.

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.

Redelivering messages misidentified as spam

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 236.

Only the administrators that have Full Administration rights or Manage Quarantine modify rights can release messages from quarantine.

See “Viewing spam and suspected messages in quarantine” on page 223.

See “About navigating Spam Quarantine” on page 226.

See “Modifying Spam Quarantine thresholds” on page 234.

See “Specifying when and how often Spam Quarantine is purged” on page 245.

See “Deleting spam messages in quarantine” on page 229.

To redeliver messages misidentified as spam 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 a misidentified message and then click Release to redeliver the message to the intended recipient.
To redeliver messages misidentified as spam from the 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 keep the database size manageable. When you delete a message in the administrator's Spam Quarantine, you also delete it from the user's Spam Quarantine. For example, assume 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. The result is that users cannot determine if the message was legitimate spam or a false positive. When you or a user deletes a message, it is no longer accessible.

See “Redelivering messages misidentified as spam” on page 228.

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.

You can also use a purge utility to automatically delete messages from Spam Quarantine. This utility frees you from having to manually delete messages from Spam Quarantine to free up space. The utility purges messages based on the schedule that you specify.

See “Specifying when and how often Spam Quarantine is purged” on page 245.

## 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.
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.

Searching quarantined spam 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 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 messages in quarantine” on page 223.

See “About navigating Spam Quarantine” on page 226.

See “Sorting spam and suspected messages in quarantine by date” on page 227.

To search quarantined spam messages

1. In the Control Center, click Virus > 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 Brightmail 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 233.

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:

- **Tokens**
  Tokens are matched with substring semantics. Searching for a subject with the search target `<in>` will match "Lowest rate in 45 years," "RE: re: Sublime Bulletin (verification)," "Up to 85% off Ink Cartridges + no shipping!," and "Re-finance at todays super low rate."

- **Multiple word searches**
  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 "red carpet," "red wine," and "flying carpet."

- **Case sensitivity**
  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.

- **Exact phrases**
  To search for an exact phrase, enclose the phrase in " " (double quotes).

- **Wildcards**
  You can use *(asterisk)* to perform wildcard searches. It also functions as a logical AND character.

- **Single characters**
  Even a single character is treated as a substring target.

- **Special characters**
  You can search on special characters such as & (ampersand), ! (exclamation point), $ (dollar sign), and # (pound sign).

- **Multiple characteristics**
  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.

- **Forged header information**
  Spammers usually "spoof" 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.

- **Time to perform a search**
  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.

See “Searching quarantined spam messages” on page 230.
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.

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.

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 messages in quarantine” on page 223.
See “About navigating Spam Quarantine” on page 226.

See “Sorting spam and suspected messages in quarantine by date” on page 227.

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

You can modify the size of the Spam Quarantine database and the size of messages that are stored in the database. 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.

See “Specifying how long spam messages are retained in quarantine” on page 245.

See “Specifying when and how often Spam Quarantine is purged” on page 245.

Before you modify the Spam Quarantine thresholds, ensure that you understand the implications and considerations.

See “Spam Quarantine threshold considerations” on page 235.

Table 10-2 describes the Spam Quarantine thresholds that you can configure and their default values.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of quarantine database</td>
<td>Maximum amount of disk space that is used for quarantined messages for all users</td>
<td>10 GB</td>
</tr>
<tr>
<td>Maximum size per user</td>
<td>Maximum amount of disk space that is used for quarantine messages per user</td>
<td>1 GB</td>
</tr>
</tbody>
</table>
Table 10-2  Spam Quarantine Thresholds (continued)

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of messages</td>
<td>Maximum number of messages for all users (the same message that are sent to multiple recipients counts as one message)</td>
<td>10000000</td>
</tr>
<tr>
<td>Maximum number of messages per user</td>
<td>Maximum number of quarantine messages per user</td>
<td>10000</td>
</tr>
</tbody>
</table>

To modifying 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 10-3 describes the issues that you should consider before you modify Spam Quarantine thresholds.

Table 10-3  Issues to 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>
</tbody>
</table>
Table 10-3  Issues to consider before you modify Spam Quarantine thresholds (continued)

<table>
<thead>
<tr>
<th>Issues to consider</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>The “Maximum size of quarantine database threshold” and “Maximum number of messages” threshold 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 Available Spam Quarantine is less than.</td>
</tr>
<tr>
<td></td>
<td>See “Types of alerts” on page 447.</td>
</tr>
</tbody>
</table>

See “Modifying Spam Quarantine thresholds” on page 234.

**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 Brightmail 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 “Redelivering messages misidentified as spam” on page 228.

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.

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, it 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 238.

See “Specifying when to notify users of spam messages in their quarantine” on page 239.

See “Modifying the spam notification message digest templates” on page 240.

See “Enabling notification digests for distribution lists” on page 243.

See “Selecting the notification digest format” on page 243.

### 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 Brightmail 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.

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 10-4 provides an example of how messages are routed to members of distribution lists.

<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>

See “About configuring the user and distribution list notification digests” on page 237.

See “Specifying when to notify users of spam messages in their quarantine” on page 239.

See “Modifying the spam notification message digest templates” on page 240.

See “Enabling notification digests for distribution lists” on page 243.

See “Selecting the notification digest format ” on page 243.

**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 not send 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.

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 237.

See “About how spam is handled when addressed to distribution lists” on page 238.

See “Modifying the spam notification message digest templates” on page 240.

See “Enabling notification digests for distribution lists” on page 243.

See “Selecting the notification digest format ” on page 243.

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.

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
Table 10-5 describes the variables that you can use in spam notification 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 237.

See “About how spam is handled when addressed to distribution lists” on page 238.

See “Specifying when to notify users of spam messages in their quarantine” on page 239.

See “Enabling notification digests for distribution lists” on page 243.

See “Selecting the notification digest format” on page 243.

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 10-5 on page 242. 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 10-5 lists the spam notification message variables.

**Table 10-5**  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 From:, Subject:, and Date: 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 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:
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.

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.

See “About configuring the user and distribution list notification digests” on page 237.

See “About how spam is handled when addressed to distribution lists” on page 238.

See “Specifying when to notify users of spam messages in their quarantine” on page 239.

See “Modifying the spam notification message digest templates” on page 240.

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 View link next to each message in the notification digest message summary.

5 Click Save.

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 purged” on page 245.

See “Modifying Spam Quarantine thresholds” on page 234.

You can also delete messages manually from Spam Quarantine.

See “Deleting spam messages in quarantine” on page 229.

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 purged

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 245.

See “Modifying Spam Quarantine thresholds” on page 234.

See “Deleting spam messages in quarantine” on page 229.

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.

Troubleshooting Spam Quarantine

Table 10-6 lists some problems that may occur with Spam Quarantine.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot log on due to conflicting LDAP and Control Center accounts</td>
<td>If there is an account in your LDAP directory with the user name of admin, you won’t be able to log on to Spam Quarantine as admin, but you will still be able to log into the Control Center as admin. This is because your LDAP administrator account name conflicts with the default Control Center administrator account name. To address this problem, you can change the user name in LDAP. You cannot change the “admin” user name in the Control Center.</td>
</tr>
</tbody>
</table>
Table 10-6  Spam Quarantine issues *(continued)*

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
</table>
| Error in log file due to very large spam messages                    | If you check the Control Center error log file and see lines similar to those listed below, the messages forwarded from the Scanner to Spam Quarantine are larger than the standard packet size used by MySQL (1 MB). See “Checking the Control Center error log” on page 435.  
| Error in log file "cannot release mail" from Spam Quarantine        | This error can occur if the IP address of the Control Center is not specified for inbound and outbound mail settings on the Administration > Hosts > Configuration Add or Edit page, SMTP tab. See “About Scanner email settings ” on page 98. |
### Table 10-6  
Spam Quarantine issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
</table>
| Users do not see distribution list messages in their Spam Quarantine | 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 “About how spam is handled when addressed to distribution lists” on page 238.                                          |
| Undeliverable quarantined messages go to Spam Quarantine postmaster  | If Spam Quarantine cannot determine the proper recipient for a message that is received by Symantec Brightmail 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.  
**Note:** No notification messages are sent to the postmaster mailbox.  
See “Viewing spam and suspected spam messages sent to the postmaster mailbox” on page 225. |
| Error in log file due to running out of disk space                    | If you check the Control Center error log file and see lines similar to those listed below, make sure that you have not run out of disk space where Spam Quarantine is installed.  
See “Checking the Control Center error log” on page 435.  
9 Jan 2004 00:00:22 (ERROR:5396:6396):[2032] Error connecting to 192.168.1.4:41025: Unknown Error; Out of range.  
9 Jan 2004 00:00:22 (ERROR:5396:6396):[4042] smtp_direct: failed to connect to SMTP server. |
Table 10-6  Spam Quarantine issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
<tbody>
<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 LDAP in the Control Center to use a Global Catalog. 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 “Configuring LDAP settings and adding source definitions” on page 493.</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>
<tr>
<td>Maximum number of messages in Spam Quarantine</td>
<td>If you don't set any Spam Quarantine thresholds and your system has adequate capacity, there is an 80 GB MySQL limit on the number of messages that can be stored in Spam Quarantine (the same message sent to multiple recipients counts as one message). See “Modifying Spam Quarantine thresholds” on page 234.</td>
</tr>
<tr>
<td>Copies of misidentified messages are not delivered to administrator</td>
<td>If you typed an email address in the Administrator box under Misidentified Messages on the Quarantine Settings page but messages are not delivered to the email address, make sure the email address is not an email alias. The administrator email address for misidentified messages must be a primary email address including the domain name, such as <a href="mailto:admin@symantecexample.com">admin@symantecexample.com</a>. See “Forwarding spam messages for non-existent addresses to quarantine” on page 221.</td>
</tr>
</tbody>
</table>
Table 10-6  Spam Quarantine issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description/solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message &quot;Cannot release the message&quot; is displayed</td>
<td>This message may occur if there is a problem with message traffic on your inbound or outbound mail flow. 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 and Suspect Virus Quarantine and emailing reports and alerts. See “Specifying SMTP host settings for product generated alerts, reports, and messages” on page 454.</td>
</tr>
</tbody>
</table>
| Quarantining spam messages and suspected spam messages takes longer than expected | 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 “Configuring LDAP settings and adding source definitions” on page 493.  
  ■ Check the base DN query. A more specific DN query returns faster than a more general one. For example, "ou=quarantine-test,dc=brightmail,dc=com" is a more specific query than "dc=brightmail,dc=com." |
Filtering IM

This chapter includes the following topics:

■ About IM
■ Enabling IM filtering
■ About spim
■ About how spim works
■ About detecting spim
■ About registering IM users
■ Blocking access to an IM network
■ About default IM virus policies
■ Creating IM virus policies
■ Creating IM spim policies

About IM

Symantec Brightmail Gateway offers enterprises a gateway-based instant messaging (IM) solution. Along with its email security solutions, Symantec Brightmail Gateway provides threat protection solutions to your enterprise for IM through the features that are described in Table 11-1.

You can install Instant Messaging filtering on a Scanner by itself or on a Scanner with email filtering. The IM settings that you configure in the Control Center apply to all the Scanners on which IM is filtered.

After you deploy a Scanner with Instant Messaging filtering, configure your enterprise DNS to route IM messages from your IM users to that Scanner. You
must then configure the DNS for the Scanner to route IM messages to their public IM networks over the Internet.

See the *Symantec Brightmail Gateway Installation Guide* for more information.

The IM messages that are routed through your Instant Message-filtering Scanner are subject to the settings that you define in the Control Center.

Table 11-1 describes the features that Symantec Brightmail Gateway uses to detect, block, and monitor certain IM-related activity.

**Table 11-1**  IM Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Access Control</td>
<td>You can create policies to block access to the IM networks that you do not use. You can also specify whether file transfers and extended features are enabled for the networks that you do use. When you block access to an IM network, each IM-filtering Scanner is prevented from connecting to that network's public IM network servers. The IM client notifies IM users who attempt to sign on to a blocked IM network that the connection attempt failed. See “Blocking access to an IM network” on page 269.</td>
</tr>
<tr>
<td>Network Status</td>
<td>You can view the connection status of each IM network that you support from each Scanner that is in your corporate network. Viewing the network connection status may help you to troubleshoot IM connectivity problems after you configure a Scanner and your DNS. See “Viewing the connection status of your IM networks” on page 432.</td>
</tr>
</tbody>
</table>
Table 11-1  IM Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Users</td>
<td>You can register your IM users with Symantec Brightmail Gateway to ensure that only qualified users within your organization can sign on. Unregistered IM users can sign on to their IM networks but cannot send IM messages or transfer files to other IM users. Unregistered IM users who attempt to send IM messages are given the option to self-register at that time if they qualify. See “About registering IM users” on page 259.</td>
</tr>
<tr>
<td>Active Users</td>
<td>You can view a list of both the registered and unregistered IM users that are currently signed on. IM users that are currently signed on are known as active IM users. You can view all active IM users, or you can create a filter to display only the active IM users that you want to view. See “Viewing IM users that are signed on” on page 429.</td>
</tr>
<tr>
<td>IM Virus Policies</td>
<td>You can create policies to allow or block your IM users from performing file transfers. Transferred files can contain viruses that may pose a security threat to your corporate network when opened. If you allow file transfers, Symantec Brightmail Gateway scans each file for known viruses, worms, and other threats and, optionally, blocks infected files from delivery. In addition to known threats, Symantec Brightmail Gateway also detects unscannable and encrypted files. Because these files cannot be scanned, Symantec Brightmail Gateway considers them a security threat and treats them as it would a virus. See “Creating IM virus policies” on page 272.</td>
</tr>
</tbody>
</table>
Table 11-1  IM Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Spim Policies</td>
<td>Symantec Brightmail Gateway detects spim through the following features:</td>
</tr>
</tbody>
</table>
|                  | ■ Known spim detection  
|                  | Symantec Brightmail Gateway periodically downloads the latest virus definitions, worm signatures, and spim signatures from the Symantec Security Response. You can configure the appliance to scan and, optionally, block the IM messages that contain these known threats.  
|                  | ■ Heuristic-based spim detection  
|                  | Symantec Brightmail Gateway can detect heuristic-based IM activity, such as a URL that is sent in multiple IM messages in rapid succession. You can configure the appliance to detect these threats and share them with Symantec Security Response for download to other organizations that use Symantec Brightmail Gateway.  
|                  | See “Creating IM spim policies” on page 274.                                                                                               |
| Reports          | Based on your IM settings, you can generate reports that detail IM-related activity, such as spim and virus detection and file transfer blocking.  
|                  | See “About working with reports” on page 356.                                                                                              |

Enabling IM filtering

You can enable instant messaging for a host when you install Symantec Brightmail Gateway or configure a Scanner to route instant messages and file transfers. You must configure an external DNS server to enable IM scanning.

See “Specifying DNS server addresses” on page 113.

For Yahoo IM, you can specify whether you are using the standard Yahoo IM network or the Japanese IM network. However, you cannot specify both.

Use the following procedure to enable instant messaging for a host.
To configure instant messaging for a host

1. Click Administration > Hosts > Configuration.

2. Check the Scanner for which you want to configure instant messaging.

3. Click Edit.

4. Click the IM tab.

5. Click Enable IM on this Scanner.

6. Under Outbound IM Interface, from the Ethernet drop-down list, select the Ethernet network interface that IM clients use to communicate internally.

   **Note:** You must have an Ethernet interface already configured for this Scanner. Use the Ethernet tab to configure an outbound Ethernet network if necessary. See “Configuring Ethernet settings” on page 115.

7. Under Outbound IM Interface, select outbound IP addresses from the Outbound IP address and Secondary IM IP address drop-down lists.

   The outbound IP address listens for incoming instant messages. You can use the same outbound IP address for outbound IM as you use for incoming email.

   The secondary IP address routes file transfers through the Scanner. The secondary IP address must be a different address from the outbound IP address. You can, however, use the same inbound IP address for inbound IM as you use for outgoing mail.

8. Under Inbound IM Interface, from the Ethernet drop-down list, select the Ethernet network that IM clients use to communicate with public servers.

   The same Ethernet network card can be used for both the internal IM interface and the inbound IM interface.

9. Under Inbound IM Interface, select the inbound IP address from the Inbound IP address drop-down list.

   The inbound IP address can be the same as the outbound IP address. You can, however, assign an inbound IP address for your Inbound IM Interface to a different card from the one that you use for the Outbound IP address of your Outbound Interface. If you are using different Ethernet networks for incoming and outgoing email traffic, it is best to assign one Ethernet network to the Outbound IP address and the other Ethernet network card to the Inbound IP address.

10. Under Network Options, click the version of Yahoo IM in use on your network. The Standard version is selected by default.
11 Check or uncheck **Limit AOL file transfers to known ports** as desired.
12 Click **Save**.

### About spim

Symantec Brightmail Gateway is integrated with Symantec Security Response to protect your network against the threats posed by spim.

Spim is unsolicited commercial IM messages that typically contain links to the Web sites that a spimmer wants to market. Bots that simulate IM users are used to generate spim. These bots send spim to a pre-determined set of IM screen names that are generated randomly, or are harvested off of the Internet. Ill-intentioned programmers also generate spim to infect other computer systems with malware (malicious software), such as viruses, worms, and Trojan Horses. This malware is designed to infiltrate or damage computer systems without the owners' informed consent.

### About how spim works

Spim is often generated from a computer system that is infected with malware, such as viruses, worms, and Trojan horses.

A virus is a computer program that attaches itself to another computer program. When the infected program is run, the virus is activated and attaches itself to another program. For example, an activated virus can attach itself to a messenger service on your computer. Once the virus detects your IM screen name, it can then send IM messages to users on your contact list using your screen name. These messages typically contain URLs that, when clicked, direct the user to a Web site that the spimmer wants to market. These URLs can also contain links that, when clicked, automatically download viruses through which the computer can be accessed.

Spim takes advantage of the social aspect of instant messaging. Most IM users regard spim as safe content because they are under the impression that it was sent to them from a trusted source. Most spim typically contains friendly, inviting text—such as "Hey, check this site out!"—along with the targeted URL. Such messages can lead spim recipients to believe that the URLs point to interesting Web sites that contain inoffensive online pictures or games.

The malware that generates spim can spread from computer to computer in a number of different ways. Viruses and Trojan horses typically spread to other computers by users who unknowingly share infected files, most often through email. Worms typically spread to other computers by using the originating computer's transport features.
About detecting spim

Symantec Brightmail Gateway is integrated with Symantec Security Response to protect your network against the threats that spim poses through Instant Messaging providers. Spim detection does not detect the malicious software that generates spim. Instead spim detection blocks known spim that an external IM user or bot sends to your IM users. It also blocks spim that an internal IM user can unknowingly spread from a computer that is infected with a virus. Finally, it blocks the IM messages that are suspected of containing spim based on a configured set of heuristic-based rules.

Symantec Brightmail Gateway detects spim through the following features:

- **Known spim detection**
  Symantec Brightmail Gateway periodically downloads the latest virus definitions, worm signatures, and spim signatures from the Symantec Security Response. By default, known spim detection is enabled.

- **Heuristic-based spim detection**
  Symantec Brightmail Gateway can detect heuristic-based IM activity, such as a URL that is sent in multiple IM messages in rapid succession. These threats are then shared with Symantec Security Response for download to other organizations that use Symantec Brightmail Gateway. By default, heuristic-based spim detection is enabled.

After you configure your IM spim settings, you can create spim policies to scan and optionally block the IM messages that contain spim. If you allow a suspected IM message to be delivered, you can append it with an annotation to alert the recipient. You can also send a notification to the sender, recipient, or both, to indicate that a suspected IM message has been deleted or delivered.

See “Creating IM spim policies” on page 274.

You can generate reports that provide spim-related statistics.

See “About working with reports” on page 356.

About detecting known spim

When you create a spim policy, each Scanner that is configured to filter IM downloads a group of rule sets from Symantec Security Response. These rule sets include the following:

<table>
<thead>
<tr>
<th>Settings</th>
<th>A list of predefined settings that determine the blocking and reporting behavior of spim. Symantec Security Response defines these settings.</th>
</tr>
</thead>
</table>

### Known Spim
A list of words, phrases, and URLs that are known to constitute spim.

### Known Spammers
A list of IM users who are known to send spim.

### White Lists
A list of URLs that are not detected as spim, even if they appear in the Known Spim list or violate heuristic-based settings. IM messages that contain URLs that appear in white lists are not blocked.

Symantec Security Response updates its list of known spim and spammers as it identifies new instances of these threats. Symantec Brightmail Gateway updates your network with these lists by downloading them several times an hour and sending them to each IM-enabled scanner. In addition to new spim definitions, these lists also identify spim that is no longer considered a threat by Symantec Security Response.

### About detecting suspected spim
Symantec Brightmail Gateway uses heuristic-based technology to detect and block the IM messages that contain content that is suspected of being spim.

Symantec Brightmail Gateway uses predefined settings from Symantec Security Response to scan each IM message for the content that is characteristic of spim. These settings define the number of times that particular content (such as a URL) appears in multiple IM messages during a specified number of seconds. For example, the URL [www.geocities.com/some_recent.pictures](http://www.geocities.com/some_recent.pictures) is suspected of being spim if it is detected 5 times within a 75-second interval.

Suspected spim is uploaded to Symantec Security Response and subsequently downloaded by other Symantec Brightmail Gateway systems that are configured to detect heuristic-based spim. However, suspected spim is blocked only for a pre-configured length of time. (The default is 4 hours.) If the suspected spim does not continue to violate the heuristic-based spim settings during this time, it is no longer suspected of being spim. Its new status is then uploaded to Symantec Security Response and subsequently downloaded to the other Symantec Brightmail Gateway systems.

Additionally, you also receive suspected spim from other Symantec Brightmail Gateway systems that are configured to detect heuristic-based spim.
Enabling spim detection

By default, Symantec Brightmail Gateway is configured to detect both known and heuristic-based spim. You can configure Symantec Brightmail Gateway to enable or disable spim detection.

To enable or disable spim detection

1. In the Control Center, click Spam > Settings > Scan Settings.
2. Click the Instant Messaging tab.
   
   By default, both known spim and heuristic-based spim detection are enabled.
3. Do one or both of the following:
   - To disable known spim detection, uncheck Enable detection of known spim attacks.
   - To disable heuristic-based spim detection, uncheck Enable heuristic based spim detection.
4. Click Save.

About registering IM users

User registration is the process of associating an IM user's corporate email address with the user's IM screen names in Symantec Brightmail Gateway. You can register an IM user if the user's email address is included in your LDAP directory or contains one of your local domains (for example, symantec.com). You can then configure Symantec Brightmail Gateway to allow only the internal IM users that are registered to use IM.

If registration is required, unregistered IM users can sign on to their IM networks. However, unregistered users cannot send IM messages or transfer files to other IM users. Unregistered IM users who attempt to do so are given the option to self-register at that time by using IM. Symantec Brightmail Gateway notifies the unregistered IM users that they cannot use IM.

User registration is also required if you want to create IM-related policies. If user registration is required, the IM users that belong to a group must adhere to that group's policies. Default policies apply to a user that does not belong to a group, or belongs to a group that has no IM-related policies. If user registration is not required, all IM users must adhere to the default policies.

By default, user registration is not required.
About the IM user registration process

As an administrator, you can register IM users in the Control Center.
See “Registering an IM user as an administrator” on page 265.

As an IM user, you can register yourself when you attempt to send an IM message for the first time as an unregistered user. This process is known as self-registration.
See “Self-registering an IM user” on page 266.

Using a single email address, you can register an IM user in the following ways:

■ Multiple IM screen names for the same IM network
  For example, you can register both john_smith and j_smith for the same AOL IM user.

■ Same IM screen for multiple IM networks
  For example, you can register john_smith for both AOL and Yahoo IM for the same IM user.

Note: You cannot register the same IM screen name for multiple email addresses. For example, you cannot register john_smith for both john_smith@symantec.com and j_smith@symantec.com.

To ensure that only a valid IM user can register, Symantec Brightmail Gateway validates the user’s email address with your Control Center's LDAP database. If the user's email address is not found in your LDAP database, Symantec Brightmail Gateway tries to register the user by validating the domain of the user's email address with your local domains. If the domain cannot be validated, the user cannot be registered.

You can view a list of both the registered and unregistered IM users that are currently signed on.
See “Viewing IM users that are signed on” on page 429.

Enabling IM user registration

If you want to allow only registered IM users to send IM messages and transfer files, or if you want to create IM-related policies, you must enable IM user registration. By default, IM user registration is not required.

To enable IM user registration, you must have at least one local domain configured. If you do not have any local domains configured when you enable user registration, you are directed automatically to the Domains page where you are required to add one.
See “Adding or editing local domains” on page 81.

To enable user registration

1 In the Control Center, click Protocols > Instant Messaging > Registered Users.

2 Under Registration Settings, click Require users to register.

   If you do not have a local domain configured for Symantec Brightmail Gateway, the following message appears: User registration requires at least one local email domain to be configured.

   You are directed automatically to the Domains page.

3 (Optional) To edit the text of the registration notifications, click Notification Text.

   See “To edit registration notification text” on page 261.

4 Click Save.

Editing IM user registration text

Unregistered IM users receive a series of default notifications that instruct them through the process of self-registration.

See “Self-registering an IM user” on page 266.

You can edit these notifications to be more suitable to your organization or rewrite them in another language. These notifications can be 256 characters in length and can contain a hyperlink. However, they cannot contain HTML characters.

To edit registration notification text

1 In the Control Center, click Protocols > Instant Messaging > Registered Users.

2 Click Notification Text.
3 Under Registration IM Text, edit one or more of the following notifications:

<table>
<thead>
<tr>
<th>Notification Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start registration text</strong></td>
<td>The IM notification that appears when an unregistered IM user tries to send an IM message. This notification should inform the user to send the user's email address in an IM message by responding to this notification. Default text: You must enter your screen name with your admin before you can use IM. Please specify your email address in this window.</td>
</tr>
<tr>
<td><strong>Valid email entered</strong></td>
<td>The IM notification that appears when an unregistered IM user sends a valid email address. This notification should inform the user that a registration key was emailed to the user's email address. It should also inform the user to send the registration key in an IM message by responding to this notification. Default text: A registration key will be sent to your email address. When you receive it, enter the registration key into this window to complete registration.</td>
</tr>
<tr>
<td><strong>Successful registration</strong></td>
<td>The IM notification that appears when an IM user successfully registers. Default text: Registration complete. You may now use IM.</td>
</tr>
</tbody>
</table>
4 Under Registration Error Messages, edit one or more of the following notifications:

Invalid email address

The IM notification that appears when an IM user sends an invalid email address.

An invalid email address is an address that does not contain the @ character, contains spaces, or exceeds its maximum length. It also includes email addresses that are created for distribution lists (for example, everyone@symantec.com).

This notification should instruct the user to resend a valid email address.

Default text: The email address you entered is invalid.

Invalid Domain

The IM notification that appears when an IM user sends an email address during self-registration that does not exist in your LDAP database and does not contain a valid local domain (for example, symantec.com).

This notification should instruct the user to resend an existing email address (i.e., the user's corporate email address), or one that contains a valid local domain.

Default text: You must use your internal email address.

No local domain

The IM notification that appears when an IM user sends an email address that does not exist in your LDAP database and when you do not have any local domains configured.

This notification should instruct the user to resend an existing email address, or contact a system administrator to configure a local domain.

Default text: Unable to verify email address. No internal emails domain has been configured.
<table>
<thead>
<tr>
<th><strong>Invalid registration key</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The IM notification that appears when an IM user sends an invalid registration key. This notification should instruct the user to resend the registration key, or to type the restart command that you specify in the Restart command field. Default text: The registration key you entered is invalid. Try again. If you want to start over, type restart.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Restart Command</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The command that an IM user types to restart the user registration process. Default restart command: Restart.</td>
</tr>
</tbody>
</table>

5 Under External Notification Text, edit the following notifications:

<table>
<thead>
<tr>
<th><strong>Unregistered user</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The IM notification that an IM user receives when that user tries to send an IM message to an unregistered user. Default text: This user is not permitted to send or receive messages via IM.</td>
</tr>
</tbody>
</table>

6 Under Registration Key Email Template, edit one or more of the following notifications:

<table>
<thead>
<tr>
<th><strong>File Encoding</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>From the Encoding drop-down list, select the character encoding that is used to send the email message that contains the registration key to the IM user who is self-registering.</td>
</tr>
<tr>
<td>- Unicode (UTF-8) – default</td>
</tr>
<tr>
<td>- Western European (ISO-8859-1)</td>
</tr>
<tr>
<td>- Simplified Chinese (B2312 or GB18030)</td>
</tr>
<tr>
<td>- Traditional Chinese (Big5)</td>
</tr>
<tr>
<td>- Korean (KS_C_5601-1987)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Sent from</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The email address that appears in the From field of the email message that contains the registration key.</td>
</tr>
</tbody>
</table>
Subject

The text that appears in the Subject field of the email message that contains the registration key.

Content

The text that appears in the body of the email message that contains the registration key.

This text should instruct the user to send the enclosed registration key in an IM message.

Default text: You are receiving this email because you have specified this email ID for Symantec IM Security registration. To confirm registration, please copy and paste the registration key specified below in your IM window.

7 Do one of the following:

■ Click Default to restore the default text for each notification.
■ Click Save to save your customized notifications.

Registering an IM user as an administrator

As an administrator, you can register IM users in the Control Center. For a single corporate email address, you can register as many IM screen names as you want for each IM network that you support. When you register an IM user in the Control Center, that user can sign on and use IM immediately.

To register an IM user as an administrator in the Control Center

1 In the Control Center, click Protocols > Instant Messaging > Registered Users.

2 Under Users, click Add.

3 Under Add IM User, in the Email address field, type the IM user’s corporate email address.

4 Under IM Network Accounts, type the IM user’s IM screen name for each IM network that you support.

   Separate multiple IM screen names for the same IM network with a comma.

5 Click Save.
Self-registering an IM user

As an unregistered IM user, you can register yourself if your email address contains a local domain that is configured for Symantec Brightmail Gateway.

See “Adding or editing local domains” on page 81.

The following sequence describes the self-registration process for an unregistered IM user:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An unregistered IM user sends an IM message to another IM user.</td>
<td>Symantec Brightmail Gateway sends an IM message to the unregistered user that requests the user's email address. The IM message sent to the user is blocked.</td>
</tr>
<tr>
<td>The unregistered IM user sends an IM message with the requested email address to Symantec Brightmail Gateway.</td>
<td>If the email address (or its domain) is valid, Symantec Brightmail Gateway sends an email to the user that contains a registration key. This email instructs the user to send the registration key to Symantec Brightmail Gateway in an IM message. If the email address (or domain) is invalid, Symantec Brightmail Gateway sends an IM message to the user that requests the email address again.</td>
</tr>
<tr>
<td>The unregistered IM user sends an IM message with the requested registration key to Symantec Brightmail Gateway.</td>
<td>If the IM message contains a valid registration key, Symantec Brightmail Gateway sends an IM message to the user that states that the registration process is complete. The user is able to use IM. If the IM message contains an invalid registration key, Symantec Brightmail Gateway sends an IM message to the user that requests the registration key again. If the user wants to resend the email address instead, the user can type restart.</td>
</tr>
</tbody>
</table>

When you self-register, you can register only one IM screen name at a time. If you want to register an additional screen name for the same email address, you must sign on using that screen name.

**Note:** If the self-registration process is disrupted (for example, the IM user logs off or is disconnected), the process starts over the next time the user attempts to use IM.
To self-register as an IM user

1. Sign on to your IM network using your IM client.
2. Send an IM message to another IM user.
   The following IM message appears: You must register your screen name before you can use IM. To register, please specify your email address.
3. Type your corporate email address in the IM message window, and then click Send.
   The following IM message appears: A registration key will be sent to your email address. When you receive it, enter the registration key into this window to complete your registration.
   If your email address is valid, Symantec Brightmail Gateway sends you an email that contains a registration key.
   See Step 4.
   If your email address is invalid (for example, it does not contain the @ character), you receive the following IM message: The email address you entered is invalid.
   If your email address contains an invalid domain, you receive the following IM message: You must use your internal email address. To register, please specify your email address.
   See Step 3.
4. Copy the registration key into the message window, and then click Send.
   If your registration key is valid, the following IM message appears: Registration complete. You may now use IM.
   If your registration key is invalid, the following IM message appears: The registration key you entered is invalid. Try again. If you want to start over, type "restart".
   See Step 4.

Editing and deleting registered IM users

As an administrator, you can add, edit, or delete the IM screen names associated with a registered IM user. You cannot edit the email address for a registered IM user. If an IM user's email address changes, you must delete and re-register the user with the new email address.

You can also delete a registered IM user, which deletes the user's email address and the IM screen names associated with it. Based on the results of your search, you can delete one or more specific IM users, or all IM users.
When you edit or delete an IM user, the changes that you make are not applied for 30 minutes. Until that time, the IM user's previous settings are in effect. For example, an IM user that you delete can temporarily sign on and use IM.

You can search for one or more of the registered IM users that you want to edit or delete by specifying one of the following:

- **Email address**
  The email address of the IM user. You can specify the complete email address of a single IM user, or you can use a wildcard (*) to represent one or more characters within an email address to search for multiple IM users. For example, if you specify `john_smith@*.com`, IM users john_smith@hotmail.com and john_smith@gmail.com appear.

- **IM account**
  The screen name of the IM user. You can specify the complete screen name of a single IM user, or you can use a wildcard (*) to represent one or more characters within a screen name to search for multiple IM users. For example, if you specify `jsmith*`, IM users jsmith1 and jsmith2 appear.

- **IM network**
  The IM network of the IM user. If you search by IM network, all of the registered IM users for the network that you specify appear.

You can specify the number of registered IM users that you want to appear on each page of your search results based on increments of 10, 25, 50 or 100. Based on the increment that you specify, you can navigate immediately to any page that contains additional search results. For example, if you specify that you want 10 users to appear on each page, and your search results yield 100 users, you can navigate to the page that contains users 21-30. Using the control buttons, you can also navigate to the first page, the previous page, the next page, or the last page at any time.

**To edit a registered IM user**

1. In the Control Center, click **Protocols > Instant Messaging > Registered Users**.

2. Under Users, under Search for user by, select one of the following from the drop-down list:
   - Email address
   - IM account
   - IM network

3. Do one of the following:
   - If you selected Email address or IM account, type the value.
If you selected IM network, select an IM network from the drop-down list.

4 Click **Search**.

5 Check the IM user that you want to edit, and then click **Edit**.

6 From the Edit IM User page, under IM Network Accounts, add or edit the user's IM screen names.

7 Click **Save**.

To delete a registered IM user

1 In the Control Center, click **Protocols > Instant Messaging > Registered Users**.

2 Under Users, under Search for users by, select one of the following options from the drop-down list:
   - Email address
   - IM account
   - IM network

3 Do one of the following:
   - If you selected Email address or IM account, type the value.
   - If you selected IM network, select an IM network from the drop-down list.

4 Click **Search**.

5 Do one of the following:
   - Check the specific IM users that you want to delete.
   - Check **Email** to delete all of the IM users that are displayed.

6 Check **Delete**, and then click **OK**.

## Blocking access to an IM network

You can create a policy to determine which IM networks that members of a particular group can access. You can also enable or disable file transfers and extended features for each IM network to which you allow access. Most IM clients provide extended features that allow IM users to communicate with each other by a means other than IM, such as audio or video. Extended features also include such features as application sharing and games. If you do not want your IM users to use these features, you can disable them. You can also send a notification to an IM user who attempts to use an extended feature that is disabled.
You can view the connection status of each IM network that you support from each Scanner that is in your corporate network.

See “Viewing the connection status of your IM networks” on page 432.

Symantec Brightmail Gateway is installed with a default Network Access Control policy that allows access to the following public IM networks:

- AOL
- Yahoo IM
- MSN Messenger
- Google Talk

This policy also enables file transfers and extended features for each IM network.

You can configure Symantec Brightmail Gateway to block access to an IM network that you do not support. When you block access to an IM network, each IM filtering Scanner is prevented from connecting to that network’s public IM network servers. IM users that attempt to sign on to a blocked IM network are notified by the IM client that the connection attempt failed.

If you block access to an IM network on which IM users are currently signed on, those users remain signed on until they purposely sign off.

**Note:** Before you create a Network Access Control policy, you must first create any notifications that you want to select for that policy.

See “Adding notifications” on page 295.

**Note:** When you block access to an IM network, you prevent your IM users from signing on to that network from their client workstations. However, some networks allow their users to sign on by using a Web-based IM client that is available on that network’s public Web site. IM conversations that occur in this manner are not directed through Symantec Brightmail Gateway; instead, they are directed through your corporate network, and may therefore pose a security threat.

To prevent unauthorized IM conversations, you must block access to Web-based IM clients. See the *Symantec Brightmail Gateway Installation Guide.*

**To create a Network Access Control policy**

1. In the Control Center, click **Protocols > Instant Messaging > Network Access Control.**
2. Click **Add.**
3. In the **Policy name** box, type a name for this policy.
4 Under Enabled Networks and Features, check each IM network that you want to enable for this policy. If you enable an IM network, file transfers and extended features are automatically enabled for that network.

5 (Optional) Under each IM network, uncheck **File Transfers** if you want to disable file transfers for that network.

6 (Optional) Under each IM network, uncheck **Extended Features** if you want to disable extended features for that network.

7 Under Actions, check **If a blocked network feature is detected send the following notification** if you want to send a notification to an IM user who is blocked from sending a file or using an extended feature. This option is only available if you disabled extended features for one of the IM networks.

8 Select a notification from the **Notification** drop-down list.

9 Under Apply to the following groups, check each group to which this policy applies.

10 Click **Save**.

### About default IM virus policies

Symantec Brightmail Gateway is installed with the default IM virus policies that are listed in Table 11-2. These policies are automatically enabled and assigned to the default group. However, if you create or make precedent another IM virus policy for a group, that policy overrides the default policy.

See “Creating IM virus policies” on page 272.

**Note:** If a group does not have an enabled IM virus policy, Symantec Brightmail Gateway allows the IM users that belong to that group to send infected, encrypted, and unscannable files.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Inbound Virus Detected</td>
<td>Blocks the infected files that are sent from external IM users</td>
</tr>
<tr>
<td>IM Inbound Encrypted File</td>
<td>Blocks the encrypted files that are sent from external IM users</td>
</tr>
</tbody>
</table>
### Table 11-2 Default IM virus policies (continued)

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Inbound Unscannable File</td>
<td>Blocks the unscannable files that are sent from external IM users</td>
</tr>
<tr>
<td>IM Outbound Virus Detected</td>
<td>Blocks the infected files that are sent from internal IM users and sends a notification to those users</td>
</tr>
<tr>
<td>IM Outbound Encrypted File</td>
<td>Blocks the encrypted files that are sent from internal IM users and sends a notification to those users</td>
</tr>
<tr>
<td>IM Outbound Unscannable File</td>
<td>Blocks the unscannable files that are sent from internal IM users and sends a notification to those users</td>
</tr>
</tbody>
</table>

---

**Creating IM virus policies**

Most IM networks allow their IM users to send files to each other. However, these files, such as EXE and BAT files, can contain viruses that may pose a security threat to your corporate network when opened. Using the Network Access Control settings, you can allow or block file transfers for each IM network that you support.

See “Selecting Network Access Control policies for a group” on page 73.

If you allow file transfers, you can use the Instant Messaging Virus Policies page to add, edit, copy, delete, and enable or disable IM virus policies. Symantec Brightmail Gateway scans each file for known viruses, worms, and other threats, and optionally blocks infected files from being delivered. If an infected outbound file is blocked, you can notify the sender, recipient, or both that the file was blocked.

**Note:** Symantec Brightmail Gateway does not allow file transfers for Google Talk.

In addition to viruses, you can also create policies for encrypted and unscannable files. Encrypted files are files that require a password to open. Unscannable files are files that have a file type that cannot be identified by the scan engine. Because these files cannot be scanned, Symantec Brightmail Gateway considers them a potential security threat.

You can specify whether to scan files that are sent in the following ways:

- **Inbound**
Files that are sent from external IM users

- Outbound
  Files that are sent by your internal IM users

- Both inbound and outbound

You can generate a report that details file transfer activity.
See “Report types” on page 359.

---

**Note:** If you allow file transfers, and use a load balancer to distribute traffic to multiple Scanners, you must configure your load balancer for single affinity mode. In this mode, all TCP/IP requests that originate from the same client (IP address) are routed to the same Scanner.

---

**Note:** Before you create an IM virus policy, you must first create any notifications that you want to select for that policy.
See “Adding notifications” on page 295.

---

**To add an instant messaging virus policy**

1. In the Control Center, click **Virus > Policies > Instant Messaging**.
2. Click **Add**.
3. In the Policy name box, type a name for this policy.
   This name appears on the Instant Messaging Virus Policies page, and on the **Virus** tab when you configure a group. Compliance, spam, and virus policy names must be unique. For example, you cannot have both a spam policy and a virus policy called XYZ.
4. Under Conditions, from the **Apply to** drop-down list, select the file transfers to which this policy applies:
   - Inbound file transfers
   - Outbound file transfers
   - All file transfers
5. From the **If the following condition is met** drop-down list, select the type of threat to which this policy applies:
   - Contains an encrypted file
   - Contains a virus
   - Is unscannable for viruses
6 Under Actions, from the **Perform the following action** drop-down list, select the action that this policy should take when a threat is detected:

- **Allow file transfer**
- **Block file transfer**
- **Send notification**

You can select more than one action provided the actions are not contradictory. For example, you can block a file transfer as well as send a notification. However, you cannot both allow and block a file transfer within the same policy.

If you select **Send notification**, you must select a notification from the **Notification** drop-down list.

7 Click **Add Action**.

8 (Optional) If desired, add more actions.

The actions that you add appear in the Actions list in the order in which you added them.

9 Under Apply to the following groups, do one of the following:

- Check each group to which this policy applies
- Check **Groups** to apply this policy to all of your groups

10 Click **Save**.

---

**Creating IM spim policies**

You can add, edit, copy, delete, and enable or disable IM spim policies.

You can create IM spim policies to detect whether IM messages contain known or heuristic-based spim.

See “About how spim works” on page 256.

You can configure your IM spim policies to perform one or more of the following actions when spim is detected:

- **Add annotation**
  Prepends the IM message with a customized annotation so that the recipient is alerted.

- **Delete the message**
  Deletes the IM message so that the recipient does not receive it.
Delivers the IM message to the recipient even though the message was detected as spim.

Send notification

Sends a customized notification to the sender of the IM message, the recipient of the IM message, or both.

When you create an IM spim policy, you can select more than one action for that policy. For example, you can select Delete the message and Send Notification if you want to inform the sender that the message was deleted. Or, you can select Deliver message normally and Add annotation if you want to alert the recipient that the message contains spim. However, you cannot select actions that do not logically work together within the same policy. For example, you cannot select both Delete the message and Deliver message normally; or Delete the message and Add annotation.

You can specify the IM messages to which you want your IM spim policy to apply:

- **Inbound instant messaging spim**
  Applies to IM messages that are received from an internal or external IM user. IM messages, including those that are sent by your internal IM users, are sent to their IM network servers over the Internet before they are delivered to their recipients. This means that all IM messages are subject to any inbound IM spim policies that you create.

- **Outbound instant messaging spim**
  Applies to IM messages that are sent from an internal IM user.

- **Inbound and outbound instant messaging spim**
  Applies to IM messages that are sent from an internal IM user, or received from another internal IM user or an external IM user.

Symantec Brightmail Gateway is installed with the default IM spim policies that are listed in Table 11-3. These policies are automatically enabled and assigned to the default group. However, if you create or make precedent another IM spim policy for a group, that policy overrides the default policy.

If you upgraded from an earlier version of Symantec Brightmail Gateway, the settings for your default IM spim policies are based on your previous settings. As a result, the settings of your default policies may differ from those listed in Table 11-3.
Note: Before you create an IM spim policy, you must first create any notifications or annotations that you want to select for that policy.

See “Adding notifications” on page 295.

See “Annotating messages” on page 292.

Table 11-3 Default IM Spim Policies

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming spim</td>
<td>Deletes inbound IM messages that contain known or suspected as spim.</td>
</tr>
<tr>
<td>Outgoing spim</td>
<td>Deletes outbound IM messages that contain known or suspected spim, and sends the default spim notification to the senders of those messages.</td>
</tr>
</tbody>
</table>

To add an instant messaging policy

1. In the Control Center, click **Spam > Policies > Instant Messaging**.
2. Click **Add**.
3. In the Policy name box, type a name for this policy.
4. Under Conditions, from the Apply to drop-down list, select one of the following:
   - Inbound instant messaging spim
   - Outbound instant messaging spim
   - Inbound and outbound instant messaging spim
5. Under Actions, from the Perform the following action drop-down list, select one of the following as it applies to this policy:
   - Add annotation
   - Delete the message
   - Deliver message normally
   - Send notification

   You can select more than one action. For example, you can delete the message as well as send a notification. However, you cannot both delete and deliver the IM message within the same policy. In addition, you cannot add an annotation and delete the IM message within the same policy.
6. Do one of the following:
If you selected Add annotation, select an annotation from the Prepend Annotation drop-down list.

If you selected Send notification, select a notification from the Notification drop-down list.

7 Click **Add Action**.

8 (Optional) If desired, add more actions.

   The actions that you add appear in the Actions list in the order in which you add them.

9 Under Apply to the following groups, do one of the following:

   ■ Check each group to which this policy applies

   ■ Check **Groups** to apply this policy to all of your groups

10 Click **Save**.
Creating IM spam policies
This chapter includes the following topics:

- About content filtering
- About regulatory compliance
- About configuring compliance policies
- About compliance policy conditions
- About compliance policy actions
- About using compliance policy resources
- About Vontu Network Prevent integration

### About content filtering

A content compliance policy is a set of simple and complex conditions and actions that determine how email message content and attributes are evaluated and how the email is handled as a result of that evaluation.

You can configure compliance policies to filter content:

- Block email from marketing lists that generate user complaints or use up excessive bandwidth.
- Block or redirect messages or attachments with specific content or specific file attachment types or filenames.
- Control message volume and preserve disk space by filtering out oversized messages.
- Prevent confidential or sensitive information from being sent to competitors.
- Limit ability of email users to communicate language or conduct activities contrary to your organization's values and policies.

See “About configuring compliance policies” on page 280.

About regulatory compliance

In addition to configuring policies that filter message content, you can configure compliance policies to enforce regulatory compliance of incoming or outgoing messages, allowing compliance officers or an incident response team manage these policy violations.

You can use compliance policies to:
- Ensure that employees do not send or receive messages that violate state and federal regulations, for example, a message from a call center user, containing a credit card number, sent to a recipient who is not a valid partner, that violates the California State Data Privacy regulation.
- Protect sensitive customer and employee data from being sent to unauthorized individuals and organizations.

See “About configuring compliance policies” on page 280.

About configuring compliance policies

When you create a content compliance policy, you define conditions and actions. Symantec Brightmail Gateway scans message content for specified conditions, determine the appropriate actions for messages that meet those conditions, and applies those actions to appropriate groups.

Symantec Brightmail Gateway provides you with a set of preconfigured compliance resources, such as dictionaries, patterns, and policy templates, with which to create compliance policies.

See “About using compliance policy resources” on page 300.

A content compliance policy can be as simple as a single "if = then" statement, or can be more complex, describing multiple dependent conditions and resulting actions.

You can create a new policy, use a preconfigured policy provided by Symantec Brightmail Gateway, or edit an existing policy to suit your needs. A content compliance policy might be:
One condition/one action – Using a blank policy template, the user provides a keyword, term or regular expression and selects one action to be taken if that keyword, term, or regular expression is detected in a message.

Compound condition/one action – User enters more than one condition, at least one of which references a policy resource (dictionary, pattern, etc.), and selects one action that is triggered by meeting all or any of the specified conditions.

Described Content policy template – Using a policy template, the user configures several nested compound conditions (some referencing a policy resource), and several actions (including Create an incident so the policy violations can be monitored in a policy folder).

Structured Data policy template – Using a compound condition that references at least one record, the user first adds a record, configures a view, and defines at least one condition that references that view. The user selects multiple actions (including Create an incident/Hold for Review), which may include a Message Review Approved Action or Message Review Rejected Action. Message Review actions defer configured actions until a compliance policy officer reviews and approves or rejects the message held in a compliance folder.

Once you have created compliance policies, you can further manage content compliance:

- Create compliance folders to collect and monitor incidents of noncompliance. See “About compliance folders” on page 346.

- Manage incidents of noncompliance by deferring actions and holding messages for review. See “About incident management” on page 351.

Compliance policies are configured using the Email Content Compliance Policies page.

See “Creating compliance policies” on page 282.

The process of creating compliance policies consists of the following steps:

- Setting conditions by which messages are filtered.
  Conditions are based on the content of messages using key words, regular expressions, patterns (such as credit card numbers) found in specific areas of a message, and on frequency of occurrence, and whether they apply to inbound, outbound, or both inbound and outbound messages.
  Symantec Brightmail Gateway provides some resources, such as a dictionary of profanity and a credit card regular-expression pattern, for use in creating conditions as well as templates that help you to define the conditions and actions of a policy and apply them to groups.
Specifying the actions that are to be taken on messages that meet specified conditions.
You can enable a wide variety of actions for messages that match the conditions in a compliance policy.
By selecting the Create an incident action, you can organize messages that violate a policy into folders for monitoring purposes.
See “About compliance policy actions” on page 290.

Designating groups to which a given policy applies.
See “About assigning filter policies to groups” on page 68.

Messages that meet similar conditions but require separate actions for different groups constitute separate policies. For example, separate actions may be required to route email containing sensitive human resource data depending on whether messages are destined for executives or departmental managers. Although the same conditions apply to both executives and managers, your HR policy may require that messages sent to executives not include attachments and that email sent to managers be held for review. Similarly, inbound messages may be treated differently from outbound messages that otherwise meet the same conditions for a group.

When you add a condition to a content compliance policy, you can group similar policies that prescribe different actions into policy folders by selecting the Create an incident action. You can then check the Hold message for review box, select a compliance folder, and indicate whether actions should be added to the list of approved or rejected actions that are invoked after a message is reviewed.
See “About monitoring compliance policies” on page 345.
See “About incident management” on page 351.

Creating compliance policies

If you edit an existing policy, any changes made to the conditions and actions of the policy override the existing policy. If you wish to create a similar policy without changing the existing one, check the box next to the policy and click 'Copy' and give the new policy a different name before making any changes. Once you save those changes, the newly-created policy will be added to the list of policies on the Email Content Compliance Policies page.

To add a compliance policy

1 In the Control Center, click Compliance > Policies > Email.
2 Click Add.
3 On the Add Content Compliance Policy page, you can either choose a template or choose Blank.

To use a policy template, you must have the Premium Content Control module enabled.

4 If you are choosing a template, select whether the policy applies to Described Content or Structured Data.

Described content refers to content that matches the conditions that you define. Structured data refers to comma-, tab-, and pipe-delimited data records whose columns you have mapped and uploaded as a Record resource. Symantec Brightmail Gateway compares email content with entries in the data file and filters messages with content that matches any data entries in the mapped columns.

5 Click Select.

The Email Content Compliance Policy page is displayed.

6 In the Policy name text box, type a name for the compliance policy.

This name appears on the Email Content Compliance Policies page, and on the Compliance tab when configuring a group. Compliance, spam, and virus policy names must be unique. For example, if you have a compliance policy called XYZ, you cannot name a spam or virus policy XYZ.

Note: To avoid confusion among similarly named policies, the policy name should reflect not only the conditions but the actions invoked and the group to which they apply.

7 If you want the results of this policy to be included in the statistics shown on the dashboard and in reports, check the Track violations of this policy in the dashboard and reports checkbox.

8 Under Apply to, choose where this compliance policy should be available:
- Inbound messages
- Outbound messages
- Inbound and Outbound messages

9 Under Which of the following conditions must be met, choose Any or All.

This determines the overall grouping of conditions as AND or OR. You can also link conditions together using AND or OR within the list.
10 Under Conditions, add a condition, or retain the existing list of conditions. If you chose a template on the Add Content Compliance Policy page, the conditions for that template appear in the list. You can examine or change any of the listed conditions by checking the box to the left of that condition and clicking Edit.

11 To add a condition, click Add. See “Adding conditions to compliance policies” on page 289.

12 To create a compound condition, check the conditions in the list and click (X & Y).

If you want to replace a compound condition with its constituent conditions, then click (X), (Y).

13 Under Perform the following action, select an action. For some actions you need to specify additional information in fields that appear below the action.

14 Click Add Action. Add additional compatible actions if desired.

If you want to monitor violations to this policy, select Create an incident, and click Hold message for review. Select a compliance folder from In the compliance folder drop-down list. Add deliver, delete, forward, or archive actions as appropriate by clicking Add to Approved Action to add the action to the list of Message Review Approved Actions. Click Add to Rejected Action to add the action to the list of Message Review Rejected Actions. These actions are initiated once a compliance officer approves or rejects a message from the compliance folder's Incident Management page.

Select Send notification if you want to send a message indicating that an email has triggered the policy. Select a notification from the Notification drop-down menu that appears when you select this action. You must have already created a notification for it to appear in the list of available notifications.

Note: If a message triggers a compliance policy that is configured to the Treat as Good Sender action, then the message is not scanned for spam.
15 Under Groups, check one or more groups to which this policy should apply.

You can also add a compliance policy to a group on the Compliance tab from the Edit Group page. You must have already configured the compliance policy for it to appear on this page. Previously checked groups continue to use this compliance policy although they are displayed unchecked upon loading this page. See the Compliance tab of the Edit Group page to verify which compliance policies a group is using.

16 Click Save.

See “About configuring compliance policies” on page 280.

Enabling and disabling compliance policies

After you create compliance policies, they are automatically enabled, unless they are incomplete or restricted.

On the Email Content Compliance Policies page, the Enabled column indicates one of the following policy statuses:

- **Enabled**, indicated by a green check.
- **Incomplete**, indicated by a page icon. To enable the policy you must complete the resource on which it is dependent. For example, a specific dictionary may be empty. When you add the missing data, the policy is automatically enabled.
- **Restricted**, indicated by a red circle with a line in the middle. The policy uses a premium dictionary or pattern. To enable this policy, renew your Premium Content Compliance license.
- **Disabled**, indicated by a black dash. To enable this policy, check it and click Enable.

To enable or disable a compliance policy

1. In the Control Center, click **Compliance > Policies > Email**.
2. Check the box next to a compliance policy.
3. Click **Enable** or **Disable**.

See “About configuring compliance policies” on page 280.
See “Creating compliance policies” on page 282.
See “About using compliance policy resources” on page 300.
Determining compliance policy order

You can change the order in which compliance policies are checked against messages. Changing the order in which the compliance policies are evaluated allows you to prioritize actions.

For example, you may have two policies that overlap for a message:

- One policy, Sexual Language, evaluates messages for predefined sexual language with an action to create an incident in a compliance folder for any message that triggers the policy.
- One policy, Security Violations, evaluates messages for security violations, with an action to forward a copy of the message to an administrator.

If you are tracking security violations, you may want to ensure that an incident of the message is not first filed in a compliance folder by the Sexual Language policy where it might be approved and released for delivery.

To set compliance policy order

1. In the Control Center, click Compliance > Policies > Email.
2. Check the box next to a compliance policy.
3. Click Move Up or Move Down.

See “About configuring compliance policies” on page 280.

See “Setting the compliance folder storage threshold” on page 351.

See “Creating compliance policies” on page 282.

See “Editing compliance folders” on page 350.

See “Enabling and disabling compliance policies” on page 285.

About compliance policy conditions

A policy condition is a statement that the system uses to evaluate messages. For each condition or set of conditions, you define actions to be taken. When a particular condition is met, the system takes the defined actions for that statement.

When you define policy conditions you can use the following types of information:

- Literal expressions — words, phrases, file names, and file extensions against which a policy matches message content.
  See “Adding conditions to compliance policies” on page 289.

- PERL-compatible regular expressions — pattern matching strings consisting of variables in the syntax of the PERL programming language.
  See “Using Perl-compatible regular expressions in conditions” on page 329.
File type — true file types or common file extensions that identify the program in which an attachment was created.
See “Configuring attachment list resources” on page 312.

Structured data — customer, employee, and other proprietary data sets that contain organization-specific entries, such as social security numbers. Policies that reference structured-data files match message content against entries contained in the originating data set, thus reducing false positives generated by policies that filter messages using regular expression patterns.
See “Defining a record resource View” on page 325.

In addition, you can configure conditions that reference policy resources. For example, a policy defined to filter messages for offensive language can reference words and phrases listed in several keyword dictionaries, including Profanity, Racist Language, Sex, or Explicit Words. Such a policy matches message content against entries in any of the dictionaries specified in a condition.
See “About configuring compliance policies” on page 280.

Keep in mind the following suggestions and requirements as you create the conditions for a compliance policy:

- Initially, you may want to set your policies so that messages that match compliance policy conditions are quarantined or modified instead of deleted. When you are sure the compliance policies are working correctly, you can adjust the actions accordingly.

- Sieve scripts cannot be imported, including those created in previous versions of Symantec or Brightmail software.

- There is no limit to the number of conditions per compliance policy.

- You can create a set of compound conditions. Each compound condition contains conditions linked by AND. You can then link the compound conditions using ALL or ANY.

- You can use keywords or a regular expression in a compliance policy to strip attachments. However, you cannot specify that only attachments containing the keyword or regular expression are stripped. All attachments to the message will be stripped if any of the attachments contain the keyword or regular expression.

- The order of conditions in a filter does not matter as to whether a filter matches a message. However, if a filter has Body filter tests, you can optimize the filter by positioning them as the final conditions in a filter.

- Spammers usually "spoof" or forge some of the visible headers and the usually invisible envelope information. Sometimes they forge header information
using actual email addresses or domains of innocent people or companies. Use care when creating filters against spam that you have received.

- A policy condition that limits an attachment file size should allow for the fact that a compressed file attachment that falls under the limit set for the condition may, as an uncompressed file, exceed the configured size limit. For example, a policy that is configured to strip messages of attachment files over 10 MB strips a 5-MB compressed attachment file from a message if the attachment expands to 35 MB when opened, even though the size of the compressed file is under the 10-MB limit.

- A compressed file attachment is not scanned if the uncompressed attachment exceeds the file size set for Container Settings on the Scanning Settings page (Protocols > SMTP > Scanning Settings). Make sure that any limit you set on attachment file size for your policy does not exceed the limit for uncompressed files specified on the Scanning Settings page. See “Configuring container settings” on page 189.

- If you want a policy condition to reference a structured data record, you must already have defined at least one view (data subset) for that record. Select a view from those available in the View drop-down list after you have selected the Record resource on the Content Compliance Policy Condition page. See “About creating a record resource for compliance policies” on page 318.

- The following considerations apply to keyword text string searches.

  - All tests for words and phrases are case-insensitive, meaning that lowercase letters in your conditions match both lower- and uppercase letters in messages, and uppercase letters in your conditions match lower- and uppercase letters in messages.

    If you tested that the subject contains this string "inkjet"

    Then any message subject containing these strings would be matched "inkjet" "Inkjet" "INKJET"

    If you tested that a subject contains this string "INKJET"

    Then any message subject containing these strings would be matched "inkjet" "Inkjet" "INKJET"
Multiple white spaces in an email header or body are treated as a single space character.

If you tested that a subject contains this string
Then any message subject containing these strings would be matched

If you tested that a subject contains this string
Then any message subject containing these strings would be matched

If you tested that a subject contains this string
Then any message subject containing these strings would not be matched

For details on regular expression searches:
See “Using Perl-compatible regular expressions in conditions” on page 329.

Refer to the following tables when creating your compliance policy.
See Table B-20 on page 581.

Adding conditions to compliance policies

If you intend to create a condition using a regular expression that is defined as a condition in a premium policy template, you must first open the policy template. Then either copy the regular expression into the text box adjacent to the matches regular expression field or use it to create a custom pattern.

See “About using regular expressions in conditions” on page 327.
About compliance policy actions

When you create a compliance policy, you define conditions and the actions to be taken when a message meets those conditions. You select the actions, including
those that reference policy resources, that you want the policy to take and the
groups to which you want them to apply.

See “Creating compliance policies” on page 282.

Symantec Brightmail Gateway provides the following tools that you can use to
help configure actions:

■ Optional archive tags allow you to specify an X-archive: header to add to
messages that meet a policy's conditions for archiving. This can enable you
to sort archived mail.
See “Archiving messages” on page 299.

■ Annotation templates allow you to configure standard comments that are
added to emails that meet a policy's conditions.
See “Annotating messages” on page 292.

■ Notification templates allow you to configure email messages that automatically
notify senders, recipients, or others of messages that meet a policy's conditions.
You can choose to attach the original email or not. Notification templates can
include variables that Symantec Brightmail Gateway automatically replaces
with message-specific information whenever a message triggers a policy that
is configured to send a notification.
See “About notifications” on page 294.

About annotating messages

Annotations are phrases or paragraphs appended to the body of an email or IM
message when you choose the action Add annotation. For example, an annotation
for email may be a legal disclaimer that is used to comply with a government or
corporate policy. An annotation for IM may be text that is used to alert the
recipient of an IM message that the message contains suspected spim.

When specifying an annotation for email, a plain text version is required, and an
HTML version is optional. In nearly all cases, you should type the same message
for both the plain text and HTML versions. If desired, you can use HTML formatting
tags in the HTML version, such as <b>bold text here</b>, but do not use HTML
structure tags, such as <body> or <html>.

When specifying an annotation for IM, only a plain text version is required. The
annotation is prepended to the IM message that is delivered to the recipient.

If the text cannot be converted to the original message's character set value, then
a "wrapper" is created whereby multipart annotation with both plain text and
HTML is added to the original message. Messages that contain a digital signature
or do not contain plain text or HTML would also use multipart annotation.
Table 12-1 describes the annotation behavior for email when the annotation text can be converted to the original message's character set value.

**Table 12-1**  Inline annotation behavior for email

<table>
<thead>
<tr>
<th>If these MIME parts are found...</th>
<th>And annotations have been specified...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text only</td>
<td>Plain text only</td>
<td>Plain text annotation is added to the message</td>
</tr>
<tr>
<td>Text only</td>
<td>Plain text and HTML</td>
<td>Plain text annotation is added to the message; HTML annotation is not used</td>
</tr>
<tr>
<td>Text and HTML</td>
<td>Plain text only</td>
<td>Plain-text annotation is added to the plain text part, and added to the HTML part by enclosing it in a <code>&lt;p&gt;</code> tag</td>
</tr>
</tbody>
</table>
| Text and HTML                   | Plain text and HTML                   | Plain text annotation is added to the plain text part, and HTML annotation is added to the HTML part.  
**Note:** If you define an annotation in plain text and HTML, only the HTML version appears in the resulting email message.  

See “Annotating messages” on page 292.

See “Editing an annotation” on page 293.

**Annotating messages**

Symantec recommends that annotations not exceed 1,000 characters for email, and 128 characters for IM. Do not use HTML structure tags such as `<body>` or `<html>` in the HTML box.

For email, when you specify the action to add an annotation in a policy, you can choose to prepend the annotation to the beginning of the message body, or append the annotation to the end of the message body. If you prepend, you may want to end your annotation text with a blank line or a line of dashes to provide a clear boundary before the beginning of the message body. For IM, the annotation is automatically prepended to the message.

**To add a new annotation**

1. In the Control Center, click **Compliance > Resources > Annotations**.
2. Click **Add**.
3 In the **Annotation description** box, type a name for the annotation. This is the name that appears on the Annotations page and in the annotations list in the Actions section when configuring a policy.

4 Under Protocol, click **Email** or **Instant Messaging**.

5 In the **Plain text** box, type the annotation text.
   
   If you are creating an annotation for instant messaging, go to Step 9.

6 Choose a character encoding for the plain text annotation.
   
   The following encodings are available: Western European (ISO-8859-1), Unicode (UTF-8) Japanese (ISO-2022-JP, EUC-JP or Shift_JIS), Simplified Chinese (GB2312 or GB18030), Traditional Chinese (Big5), and Korean (KS_C_5601-1987).

7 If desired, type annotation text in the **HTML** box.
   
   You can use HTML formatting tags, if desired.

8 Choose a character encoding for the HTML annotation, if you have specified an HTML annotation.
   
   The following encodings are available: Western European (ISO-8859-1), Unicode (UTF-8) Japanese (ISO-2022-JP, EUC-JP or Shift_JIS), Simplified Chinese (GB2312 or GB18030), Traditional Chinese (Big5), and Korean (KS_C_5601-1987).

9 Click **Save**.

See “About annotating messages” on page 291.

See “Editing an annotation” on page 293.

**Editing an annotation**

You can edit an existing annotation to change the wording. Symantec recommends that annotations not exceed 1,000 characters for email, and 128 characters for IM. Do not use HTML structure tags such as `<body>` or `<html>` in the HTML box.

Use the following procedure to edit an annotation.

**To edit an annotation**

1 In the Control Center, click **Compliance > Resources > Annotations**.

2 Click the annotation that you want to edit.

3 Change the annotation text as desired.

4 Click **Save**.

See “About annotating messages” on page 291.
About notifications

Notifications are preset messages that get sent when an email or instant message meets conditions specified in a policy. Use the Add Notification page to configure the notification message content and the message recipients.

Notifications are different from alerts. Alerts are sent automatically when certain system problems occur, such as low disk space.

Once you have configured a notification, you select the Send notification action on the Add Spam, Virus, or Compliance policy page and choose the notification that you want to send when an email meets the conditions for the policy.

Note that the original message is delivered to the original recipients unless you specify an additional action that prevents this.

Using the Add Notification page, you can configure the notification so that it is sent to the sender and recipients of the original message. You can also send a notification to other email addresses that you specify. For example, if you have a compliance policy that strips .exe attachments from incoming email messages, you may want to notify the sender and the recipient that the attachment has been stripped. Or you may want to notify an administrator that an email with an .exe attachment was sent to its recipient without its attachment.

You can also customize the Subject and Body fields of a notification message by inserting variables into the template. Symantec Brightmail Gateway replaces these variables with information that is specific to the message that triggered the policy. For example, by inserting the $attachments$ variable into the notification template, you configure the notification message to include the names of any attachments that the policy stripped from the original email.

You can further customize the Subject and Body fields of a notification message by inserting identifying or explanatory text around the variables. For example,

The message concerning $subject$ sent by $sender$ to $recipients$ was stripped of $attachments$.

Symantec Brightmail Gateway replaces the variables with the appropriate values in the notification message that it sends to the addresses designated in the Send to option on the Add Notification page.

**Note:** The Add and Edit Notifications pages may also be used to create and edit notifications for virus and spam policies.

See “Adding notifications” on page 295.
Adding notifications
Notifications are preset messages that are sent when an email or instant message meets conditions specified in a policy.

See “About notifications” on page 294.

Use the Add Notification page to configure the notification message content and the message recipients.

**Note:** The Add and Edit Notifications pages may also be used to create and edit notifications for both virus and spam policies.

To add a new notification

1. In the Control Center, click **Compliance > Resources > Notifications**.
2. Click **Add**.
3. In the **Notification description** box, type a name for the notification.
   This is the name that appears on the Notifications page and in the **Notification** list when you choose the **Send notification** action when configuring a policy.
4. Select the **Protocol** you want to use.
   If you want the notification to be applied to email messages, click the **Email** radio button.
   If you want to apply the notification to instant messages, click the **Instant Messaging** radio button.
5. In the **Send from** box, enter an email address that will appear in the **From:** header in the email containing the notification message. Specify the full email address including the domain name, such as admin@example.com.
   Since recipients can reply to the email address supplied, type an address where you can monitor responses to the notifications. Alternatively, include a statement in the notification that responses are not be monitored.
6 Under **Send to**, check one or more of the following:

- **Sender**: Check this box to send the notification to the sender listed in the message envelope (not the sender listed in the `From:` header).
- **Recipients**: Check this box to send the notification to the recipients listed in the message envelope (not the recipients listed in the `To:` header).
- **Others**: Check this box to send the notification to one or more complete email addresses that you specify. Separate multiple email addresses with a comma, semicolon, or space.

7 Choose a character encoding for the notification subject line.


8 Select the variables you want to include in the subject line of your notifications by using the **Include message attribute** drop-down list, then click the **Add** button.

   When you select attributes from this list and click **Add**, a corresponding variable is inserted into the **Subject** text box. For example, to include the subject line for the message that triggered the notification, you select **Subject** from the drop-down list.

   See Table B-19 on page 580.

9 In the **Subject** box, type the text for the subject header of the notification message.

   Incorporate any variables by typing text before and after the variables. For example, if you added the variable `$subject$`, you can create the following subject line text: "The message $subject$ could not be delivered." When the system delivers the message to the specified recipient(s), the system will insert the applicable subject line text.

10 Choose a character encoding for the notification message body.

11 Select the variables you want to include in the message body of your notifications by using the **Include message attribute** drop-down list, then click the **Add** button.

When you select attributes from this list and click **Add**, a corresponding variable is inserted into the **Message body** text box as a variable. For example, if you want the body text of your notification message to include the name of an attachment that has been stripped from the email, you select **Attachment names** from the drop-down list.

See Table B-19 on page 580.

12 In the **Message body** box, type the text for the body of the notification message.

Incorporate any variables by typing text before and after the variables. For example, if you added the variables `$subject$`$`attachments$`, you might create the following message: "The file $attachments$ exceeded maximum file size and had been stripped from the message $subject$." When the system delivers the message to the specified recipient(s) the system will insert the applicable attachment name and subject line text.

13 Optionally, check **Attach the original message** to attach the original message to the notification message.

14 Click **Save** to list the notification in the available notifications list whenever you choose to send a notification as a policy action.

See “Editing notification templates for compliance folders” on page 297.

**Editing notification templates for compliance folders**

Access the Incident Notification Template from the Compliance Folder Settings page to view or modify the template used to create incident notifications from this compliance folder.

See Table B-15 on page 574.

**To edit the notification template for a compliance folder**

1 In the Control Center, click **Compliance > Settings > Compliance Folders**.

2 Click the name of a compliance folder that you want to modify in the **Compliance Folders** list.

   Alternatively, check the box next to the name of the compliance folder and click **Edit**.
3 On the Add Compliance Folder Settings page click Edit next to Notification template.

The Compliance Folder Settings page refreshes to display the Notification Template frame, showing existing values for notifications sent from this folder.

4 Choose the character encoding for the notification message from the Encoding drop-down list.


5 To alter the address of the From header displayed in incident notification messages, change the email address displayed in the Send from field.

6 To alter the Subject header displayed in incident notification messages, change the contents of the Subject field.

7 Edit the text show in the Notification text box.

Symantec Brightmail Gateway will replace the 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, or you can delete the variable if desired. For example, you could type the following text to precede variable, replacing Name with the folder name:

A new incident has been created. Please access the Name Compliance Folder for incident details.

See “About notifications” on page 294.

See “Adding notifications” on page 295.

About archiving messages

By archiving messages, you can have a message copied and sent to a specified email address, as well as an archive server host. The copy is delivered by SMTP email to the specified email address and can be accessed as email by the email address owner. Ensure that the email address that you specify is valid and that the messages delivered to the address are managed appropriately. For example, you may want to add the archived messages to your backup scheme.

Note the following additional information about the Archive action:

- Only one global email address is supported. You can’t supply different archive email addresses for different policies.
The specified archive email address replaces the original message recipients in the message envelope. The To: header is not changed.

When adding the archive action to a policy, you can optionally specify an archive tag. Specifying an archive tag adds an X-archive: header to archived messages followed by your text. The X-archive: header may be useful to sort archived messages when viewing them with an email client.

See “Archiving messages” on page 299.

See “Configuring optional archive tags for archive actions” on page 299.

Archiving messages

The archive action creates a copy of a message and sends it to an email address, and, optionally, an archive server host. If no additional action is specified, the original message is delivered normally as well. Only one global email address is supported. You can't supply different archive email addresses for different policies.

To set the archive email address destination

1. In the Control Center, click Compliance > Settings > Archive.

2. In the Archive email address box, type a complete email address, such as kyi@example.com.

3. Optionally, specify a computer to which to relay archived messages in the Archive server host box.

4. Optionally, specify a port for the archive server host in the Archive server port box.

   Port 25, the usual port for SMTP messages, is the default.

5. Check or uncheck Enable MX Lookup to enable or disable MX lookup for the archive server host.

   If enabled, archive messages are routed using the MX information corresponding to the archive server host. If disabled, archive messages are always routed to the specified archive server host.

6. Click Save.

See “Configuring optional archive tags for archive actions” on page 299.

See “About incident management” on page 351.

Configuring optional archive tags for archive actions

Specifying an archive tag adds an X-archive: header to archived messages followed by your text. The X-archive: header may be useful to sort archived messages when viewing them with an email client. However, Symantec Brightmail Gateway itself
does not use the X-archive: header. If multiple policies result in archiving the same message, each unique X-archive: header is added to the message. For example, the following archive tag:

Docket 53745

adds the following header to the message when it is archived:

X-archive: Docket 53745

To specify an archive tag

1. When configuring a virus, spam, or compliance policy, select Archive the message from the drop-down list.

2. In the Optional archive tag box, type the text that should occur after the X-archive header.
   Type any character except carriage return, line feed, or semicolon.

3. Choose encoding for the archive tag.

4. Click Add Action.

5. Finish configuring the policy.

See “Archiving messages” on page 299.
See “About incident management” on page 351.

About using compliance policy resources

When you create policy conditions that leverage existing resources, you can:

- Annotate messages – You can create boiler-plate text to append to a message that a compliance policy has identified. The text you choose will depend on the policy and may advise the recipient that the accompanying email violates company norms and policies for corporate governance.
  See “Annotating messages” on page 292.

- Archive messages – Some regulations may require that you archive messages that may be in violation of corporate policies. You can send copies to an archive server, regardless of what actions are carried out on the original message.
  See “Archiving messages” on page 299.
Configure resources, such as dictionaries, attachment lists, and patterns – You can customize these resources to suit your organizational needs by adding to them or disabling pre-defined entries.
See “Creating compliance policies” on page 282.

Adding and editing notifications – You can instruct Symantec Brightmail Gateway to send customized notifications to the sender or recipients of an email whenever a policy’s conditions are met without having to deliver the actual message. You can also configure the policy to notify the compliance officer, manager, or administrator charged with enforcing the policy.
See “Adding notifications” on page 295.

Symantec Brightmail Gateway provides templates that you can use to create your compliance policies.

Templates
Policy templates are preconfigured conditions that use existing resources. You can add a template to your policy as a condition and modify that template to suit your needs.
See “About compliance policy templates” on page 302.

Symantec provides the following resources that you can use with template resources to create your compliance policies:

Basic and premium dictionaries
Dictionaries provide lists of predefined words that you can use when creating new policy conditions for evaluating message content. For example, you may wish to screen outgoing messages for certain vulgar language, or language that might suggest a job search. You can leverage a dictionary, disabling and enabling individual words in that dictionary to suit your needs.
See “About dictionary resources” on page 305.

Basic and premium attachment lists
Attachment lists are predefined lists of attachment types that you can use when screening messages. Attachment list file metadata allows you to filter messages based on an attachment's true file type, MIME-type, or file name extension.
For example, you can use an attachment list to screen out any executable type files to protect your system from viruses.
See “About attachment list resources” on page 311.

Patterns
Patterns are predefined lists of character patterns that are associated with an object or data type that you may want to restrict. For example, you can use patterns to screen outgoing messages for credit card numbers or Social Security by screening for the standard credit card patterns.
About compliance policy templates

Policy templates are prebuilt conditions that reference existing resources. You can use these resources as is, or edit them to suit your needs. You can add conditions that reference other resources than those referenced in a policy template's prebuilt conditions.

There are two types of pre-built policy templates:

- Described Content templates provide pre-built conditions that reference existing premium policy resources, such as dictionaries.
Pre-built conditions can be logically combined in different ways to create new policies that are based on the template. For example, you can use a described content template when you need to create variable conditions for a policy depending on who is authorized to review messages that meet those conditions. See Table B-1 on page 517.

Structured Data policy templates allow you to create policy conditions that reference proprietary data sets that you upload to Symantec Brightmail Gateway as a record resource. Properly configured policies based on Structured Data templates filter message content for proprietary data that you want to protect against data loss. You must create Views (data subsets) to designate the columns that a condition can reference in a record resource. Using a Structured Data policy that references a record can virtually eliminate the number of false positives returned by a similarly configured Described Content policy that relies solely on matching regular expression patterns. See “Structured Data Compliance policy templates” on page 522.

**Note:** Some policy templates provide both Described Content and Structured Data versions. Select the Structured Data version of a policy template only if you have access to and permissions for the relevant data source. If you use the Structured Data version of a policy template, you do not need to configure and enable the Described Content version of the same policy template.

See “About using compliance policy resources” on page 300.

When you change the conditions or actions of a template, you should give the policy a different name from the policy template. That way the policy template will not be confused with the policies based on it. The new policy that you have created appears in the Content Compliance Policies list.

There are two kinds of policy templates: Described Content and Structured Data. Some templates are offered in both versions while other templates only come in one version or the other.

The Described Content and Structured Data versions of the same policy template define different condition and rely on different resources to filter message contents.

**Note:** In general you should not need to create described content and structured data versions of the same policy.

The following table describes the policy templates you can use to leverage the basic resources of your choice.
Table 12-2  Basic policy resources

<table>
<thead>
<tr>
<th>Basic resource</th>
<th>Associated policy template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionaries</td>
<td>Profanity, Profanity (Ambiguous)</td>
</tr>
<tr>
<td></td>
<td>Racial, Racial (Ambiguous)</td>
</tr>
<tr>
<td></td>
<td>Sexual, Sexual (Ambiguous), Sexual Slang</td>
</tr>
<tr>
<td>Attachment Lists</td>
<td>Archive Files</td>
</tr>
<tr>
<td></td>
<td>Document Files</td>
</tr>
<tr>
<td></td>
<td>Executable Files</td>
</tr>
<tr>
<td></td>
<td>Image Files</td>
</tr>
<tr>
<td></td>
<td>Multimedia Files</td>
</tr>
<tr>
<td>Patterns</td>
<td>Credit Card</td>
</tr>
<tr>
<td></td>
<td>Email Address</td>
</tr>
<tr>
<td></td>
<td>Social Security Number</td>
</tr>
<tr>
<td></td>
<td>U.S. Phone Number</td>
</tr>
<tr>
<td></td>
<td>U.S. Zip Code</td>
</tr>
</tbody>
</table>

When using the premium pre-built templates, there are some general best practices to follow:

- Review dictionaries and determine if their contents are adequate for your environment as delivered. Some dictionaries used by templates are delivered without content. For these dictionaries, it is mandatory that you populate them with your site-specific information. If these dictionaries are not populated, the policy using them is not deployed and instead appears in a dependent state.

- Add keywords or keyword phrases to dictionaries and save.

- To prevent false positives, disable commonly used words in a dictionary that is used for your specific business environment. For example, a pharmaceutical company that distributes Allegra would probably want to disable Allegra from drug names used in a HIPAA policy.

- Review the template conditions to ensure that they are satisfactory for your business conditions.

- Add conditions to the template and save the policy.

See “About creating a record resource for compliance policies” on page 318.
See Table B-1 on page 517.

Symantec Brightmail Gateway provides a number of regulatory policies:

See “U.S. regulatory policy templates” on page 542.

See “Confidential data-protection policy templates” on page 552.

See “Acceptable use policy templates” on page 558.

See “Customer and employee data-protection templates” on page 562.

See “Network security policy templates” on page 568.

See “UK and international regulatory policy templates” on page 569.

### Viewing policy templates

You can select from the list of pre-built basic and premium compliance policy templates to create policies on the Add Content Compliance Policy page. The policy templates enable you to construct a policy using Described Content or Structured Data.

**To view content compliance policy templates**

1. In the Control Center, click **Compliance > Policies > Email**.
2. Click **Add**.

   The Blank compliance policy template with Any Resource Type is selected by default.

See “About compliance policy templates” on page 302.

See “Described Content Compliance policy templates” on page 516.

### About dictionary resources

A dictionary is a list of keywords, keyphrases, filenames, and file name extensions against which messages and attachments are checked. Content-compliance policies evaluate matches to a referenced dictionary using substring text analysis, not regular expression analysis. When a substring in a scanned message matches a dictionary entry and meets the conditions of a policy that references that dictionary, Symantec Brightmail Gateway takes the actions that are defined in the policy.

Symantec Brightmail Gateway includes a number of predefined case insensitive dictionaries available for use with the basic and premium dictionaries.

Basic dictionaries can be used with basic policy templates and provide a number of commonly used dictionaries as follows:
Note: The dictionaries marked as ambiguous contain terms that can be legitimate when used in certain contexts.

- Profanity
- Profanity, Ambiguous
- Racial
- Racial, Ambiguous
- Sexual
- Sexual, Ambiguous
- Sexual, Slang

Premium dictionaries are referenced by premium policy templates and offer the ability to configure more in-depth regulatory compliance policies. You can configure conditions in other policies to reference these dictionaries. Various pre-built conditions in premium policy templates reference premium dictionaries. Except where noted, premium pre-built dictionaries are delivered with some keywords, keyphrases, or characters and can be used as is. You can view the contents of the premium dictionaries, enable and disable existing keywords, and add keywords, keyword phrases, or characters of your choosing. Symantec recommends that you examine the contents of the premium dictionaries that you decide to use and determine if the pre-populated keyword, keyphrases, and characters meet your site-specific and business needs and then edit the dictionary as necessary. Where noted, some dictionaries are delivered empty and require that you populate them with keywords or keyphrases before they can be referenced by compliance policy conditions.

You can add new words to a dictionary or delete words previously added. Although you cannot delete predefined keywords or phrases that are already part of a pre-built dictionary, you can disable any pre-built keywords or phrases that you do not want a policy to match.

See “Editing dictionaries” on page 309.

You can also import keywords and keyphrases from a newline-delimited text file into a new, empty dictionary, or into an existing dictionary.

See “Adding a new dictionary” on page 308.

If you want to match dictionary entries against words in attachments, such as word-processing files, that are not in plain text format, you must first configure content filtering on the Scanning Settings page to Enable scanning of non-plain text attachments for words in dictionaries.
See “Scanning non-plain text file attachments for content compliance” on page 474. Symantec Brightmail Gateway provides a set of premium dictionary resources. See “Premium dictionary resources” on page 537.

In addition to editing existing dictionaries, you may create custom dictionaries. You populate custom dictionaries to suit a site-specific or business need. These dictionaries must contain at least one keyword or keyphrase. You may add or delete keywords or keyphrases from custom dictionaries.

See “Adding a new dictionary” on page 308.

Note the following additional information about dictionaries:

- Dictionaries cannot be deleted if they are used in any policy conditions or referenced by any policy template. If deletion is attempted on a dictionary that is used in a policy condition or referenced by a policy template, an error message explains that the dictionary cannot be deleted until the references are removed from the policies that reference the dictionary.

- Keywords in a dictionary are either predefined or user-defined. Predefined words are those that are delivered with the dictionary. These words can be either enabled or disabled and cannot be deleted.
  User-defined words are words you add to a dictionary. All words in custom dictionaries are user defined. User-defined words cannot be disabled. If you select multiple words of different types, and attempt to disable or enable them, that action is applied to the predefined words and not the user-defined words.

- Tests against dictionaries only match the exact word listed but not variations such as verb tenses.

- Wildcards are not supported in dictionaries.

- You can enter multiple keywords as one phrase. This is called a keyphrase. Separate the keywords with spaces.

- Up to 100 dictionaries are supported, and each dictionary can contain up to 10,000 words.

- Individual words in a dictionary cannot be set to be more or less important than other dictionary words.

- A dictionary can be used in multiple compliance policies.

- When adding words to a dictionary, keep in mind that some words can be considered both profane and legitimate, depending on the context.

- Symantec Brightmail Gateway does not search for dictionary matches in the HTML headers or tags of HTML messages or HTML attachments.

- Keywords are case insensitive.
Punctuation characters are not allowed as the first character of a keyword.

**Adding a new dictionary**

Symantec Brightmail Gateway provides set of basic and premium dictionaries that you can use for your compliance policies.

See “About dictionary resources” on page 305.

See “Premium dictionary resources” on page 537.

Additionally, you can create a new, custom dictionary to suit your specific needs.

**To add a new dictionary**

1. In the Control Center, click **Compliance > Resources > Dictionaries**.
2. Click **Add**.
3. In the **Dictionary name** field, type a name for the dictionary.
   
   This is the name that appears on the Dictionaries page and in the first drop-down list on the Content Compliance Policy Condition page when configuring a compliance policy.

4. In the **Optional description** field, type a description of the dictionary.
   
   Any dictionary that requires customer edits to populate it with site-specific keywords or keyphrases should include a description that explains what the user should provide.

5. Type a keyword or keyphrase in the **Enter a word or phrase** field.
6. Click **Add** to add the keyword or keyphrase to the Word or Phrase list.
7. Repeat these steps to add more keywords as desired.
8. Click **Save**.

See “Importing dictionary keywords” on page 308.

See “Editing dictionaries” on page 309.

See “Disabling and enabling predefined dictionary entries” on page 310.

**Importing dictionary keywords**

You can import dictionary keywords or keyphrases from a newline-delimited text file in UTF-8 format. Each keyword or keyword phrase should be on a separate line. Keywords or keyphrases can be imported into a new, empty dictionary, or into an existing dictionary.

See “Premium dictionary resources” on page 537.
You cannot import a file with extended ASCII or non-ASCII characters. The file must be accessible to your local machine.

See “About dictionary resources” on page 305.

**To import dictionary keywords**

1. In the Control Center, click **Compliance > Resources > Dictionaries**.
2. Click the dictionary that you want to import keywords into or create a new dictionary by clicking **Add**.
3. Click **Import**.
4. Enter the name of the text file you want to import or click **Browse** to locate the file.

   The dictionary keywords or keyphrases in the text file should be newline delimited—each keyword or keyphrase should be on a separate line. Keywords or keyphrases are enabled by default.

5. Click **Save**.

See “Adding a new dictionary” on page 308.

See “Editing dictionaries” on page 309.

See “Disabling and enabling predefined dictionary entries” on page 310.

**Editing dictionaries**

Symantec Brightmail Gateway provides set of basic and premium dictionaries that you can use for your compliance policies.

See “About dictionary resources” on page 305.

See “Premium dictionary resources” on page 537.

Additionally, you can customize an existing dictionary by adding or deleting keywords.

**To edit a dictionary**

1. In the Control Center, click **Compliance > Resources > Dictionaries**.
2. Click the dictionary that you want to edit.
3. Change the description as needed.
4. Enter new keywords or keyphrases in the text box provided.
5. Click **Add**.

   User-defined entries are automatically enabled so that policy conditions that reference the dictionary can search email messages for matches.
6 Select the number of keywords that you want displayed at any one time from the Entries per page drop-down menu.

7 Select the range of dictionary entries that you want to view from the Display drop-down menu.

   Use the navigation arrows to view the previous or next page of entries or to navigate to the first or last page of entries.

8 Select any user-defined keywords or phrases that you want to delete by checking the adjacent box and clicking Delete.

   You cannot delete a predefined word or phrase from a dictionary. You can only disable a predefined word or phrase so that policy conditions that reference the dictionary do not search email for matching text strings.

   See “Disabling and enabling predefined dictionary entries” on page 310.

9 Click Save.

   See “Adding a new dictionary” on page 308.

   See “Importing dictionary keywords” on page 308.

Disabling and enabling predefined dictionary entries

Symantec Brightmail Gateway provides set of basic and premium dictionaries that you can use for your compliance policies.

See “About dictionary resources” on page 305.

See “Premium dictionary resources” on page 537.

To help better meet your particular business needs, you can disable predefined dictionary entries in the dictionaries that you use for your compliance policies. You can also enable any entries that were previously disabled.

**To disable or enable dictionary entries**

1 In the Control Center, click Compliance > Resources > Dictionaries.

2 Click the dictionary in which you want to disable or enable predefined entries.

3 Select the number of keywords that you want displayed at any one time from the Entries per page drop-down menu.

4 Select the range of dictionary entries that you want to view from the Display drop-down menu.

   Use the navigation arrows to view the previous or next page of entries or to navigate to the first or last page of entries.

5 Click the box opposite the predefined keyword or keyphrase that you want to disable or enable.
6 Click **Disable** to prevent policy conditions that reference the dictionary from matching against email text strings.

You cannot disable user-defined words and phrases. You can only delete them.

Click **Enable** to allow policy conditions to search for matches against a previously disabled predefined keyword or phrase in the dictionary.

7 Click **Save**.

See “Adding a new dictionary” on page 308.

See “Editing dictionaries” on page 309.

See “Importing dictionary keywords” on page 308.

### About attachment list resources

Symantec Brightmail Gateway provides a number of basic attachment lists that allow you to identify types of email attachments that you want the system to act upon. For example, you can create an attachment list that acts upon messages with .exe files. By adding that attachment list to a policy, you can strip attachments from those messages, insert an annotation for the recipients, and notify the senders.

The following basic attachment lists have been predefined and can be edited:

- Archive Files
- Document Files
- Executable Files
- Image Files
- Multimedia Files

Additionally, Symantec Brightmail Gateway provides a library of premium attachment list resources that you can use with the premium policy templates.

See “Premium attachment list resources” on page 529.

In addition to commonly used file extensions, these resources also contain identifying information that makes it possible for Symantec Brightmail Gateway to match an email attachment based on the application in which it was created, regardless of its file extension. Since file extensions can easily be altered to disguise the identity of the originating application, the ability to recognize an email attachment by its true file type can help protect against intrusions by different types of malware.

In addition to true file types, the Attachment Types list includes common file extensions and MIME-types that a policy referencing an attachment list uses to
identify file attachments of interest. This feature can be useful, for example, if you want to filter out all .jpeg file attachments, regardless of the application that created it.

**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.

See “Configuring attachment list resources” on page 312.

**Configuring attachment list resources**

Each of the attachment list resources has been prepopulated with many of the more common true file types. To view the file types that make up the attachment list, go to the Attachment Lists page by clicking Compliance > Resources > Attachment Lists, check the attachment list that you want to view and click Edit (or click the link), then scroll down the page to the Attachment Types list.

**Note:** You can view other available true file types by opening an Attachment List and clicking one of the true file classes in the left-hand File classes list. After you choose a file class, the true file types belonging to it appear in the right-hand File types list. Select the true file type and click Add to add it to the list of file types that a policy referencing that Attachment List will search for. You can also select any of the true file types already listed in the Attachment Types list and delete those that you do not want a policy referencing the Attachment List to search for.

To configure an attachment list, choose a true file type or class from the pull-down lists or enter a file name, extension, or MIME type on the Add Attachment List page. For the last three choices, all characters are interpreted literally; wildcards are not allowed (see the table below).

See “Premium attachment list resources” on page 529.

For a technical description of MIME, see the following RFC:

http://www.ietf.org/rfc/rfc2045.txt

**To add an attachment list**

1. In the Control Center, click **Compliance > Resources > Attachment Lists**.
2. Click **Add**.
3. In the **Attachment list name** box, type a name for the attachment list. This is the name that appears on the Attachment Lists page and as the **Attachment List** in the Conditions section when configuring a policy.
4. In the **Add Attachment Types** box, perform one of the following tasks:
Choose True file class or True file type from the drop-down list. Then click on the classes or classes and types that you want to match. Press and hold Ctrl while clicking to select more than one file class or file type.

Click the second radio button to match files based on their file names, extensions, or MIME types. Select File name, Extension, or MIME-type from the drop-down menu. Then select is, contains, begins with, or ends with from the adjoining drop-down menu. Then type the text that you want the attachment file to match.

Type only one file name, extension, or MIME type in the box. Type the MIME type completely, such as image or image/gif.

---

**Note:** MIME-type and file extension-based attachment lists are not effective for stripping attachments that are not described in the MIME header, such as in the case of some forwarded messages. If you want to make sure that you strip all possible instances of a particular attachment file type, Symantec recommends that you configure your attachment lists to use True file type whenever possible.

---

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.

See “About attachment list resources” on page 311.
See “Editing attachment list resources” on page 313.
See “Premium attachment list resources” on page 529.

**Editing attachment list resources**

Use the Premium attachment list resources table to make valid choices for attachment list properties.

Premium attachment list resources

For a technical description of MIME, see the following RFC:

http://www.ietf.org/rfc/rfc2045.txt

**To edit an attachment list**

1. In the Control center, check the box next to the Attachment List name and click Edit or click on the name itself.
2. In the **Add Attachment Types** box, perform one of the following tasks:
Choose **True file class** or **True file type** from the drop-down list. Then click on the classes or classes and types that you want to match. Press and hold **Ctrl** while clicking to select more than one file class or file type.

Click the second radio button to match files based on their file names, extensions, or MIME types. Choose **File name**, **Extension**, or **MIME-type** from the drop-down menu. Then choose **is**, **contains**, **begins with**, or **ends with** from the adjoining drop-down menu. Then type the text that you want the attachment file to match.

Type only one filename, extension, or MIME type in the box. Type the MIME type completely, such as image or image/gif.

3. Click **Add** to add the attachment type to the attachment list.
4. Repeat steps 2 and 3 to add more attachment types to the attachment list.
5. If needed, select an attachment type check box in the **Attachment Types** list and click **Delete** to delete that attachment type from the list.
6. Click **Save**.

See “About attachment list resources” on page 311.

See “Configuring attachment list resources” on page 312.

See “Premium attachment list resources” on page 529.

### About pattern policy resources

Patterns are named regular expressions or system patterns that describe a commonly known data object, such as a common pattern used for credit card numbers. Symantec Brightmail Gateway provides basic and premium patterns to let you filter email for strings in outbound or inbound email that match the described pattern.

Symantec provides you with the ability create resources that contain regular expressions or system patterns that can be reused in policy creation.

Basic patterns are predefined for the basic license and cannot be edited. These are known and performance tested regular expressions which can be used as examples and in creating policies. Basic patterns must be used with basic templates.

<table>
<thead>
<tr>
<th>Basic pattern name</th>
<th>Regular expression syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card</td>
<td>\b(?&lt;!-)((4\d{3})</td>
</tr>
</tbody>
</table>
Basic pattern name | Regular expression syntax
--- | ---
Social Security Number | \b(?<!-)(\d{3})([-]?)\d{2}(\d{4})(?!-)\b
US Phone Number | \b(?<!-)((\d{5})|\d{5}\-\d{4})(?!-)\b
US Zipcode | \b(?<!-)(([\d{5}])(\d{4})(?!-))\b

Premium patterns are available to you when you define a policy condition using the Matches pattern/does not match pattern drop-down list on the Content Compliance Policy Conditions page. Premium patterns perform additional checking and validation (such as Luhn checking) beyond regular expression definitions to reduce false positives. These patterns cannot be edited or deleted.

Premium patterns may only be used with premium templates.

The list of premium patterns delivered includes:
- Valid Credit Card
- Valid IP Address
- Valid Social Security Number

See “Creating custom patterns” on page 315.

See “Creating compliance policies” on page 282.

See “Editing custom patterns” on page 316.

See “Premium pattern resources” on page 536.

See “Deleting custom patterns” on page 317.

Creating custom patterns

Symantec Brightmail Gateway provides basic and premium patterns that you can reference in your policy conditions. These patterns let the system search your messages for character patterns that indicate certain types of data that you may wish to restrict, such as credit card numbers.

See “Premium pattern resources” on page 536.

You cannot edit basic and premium patterns, however, you can create and edit custom patterns to suit your unique needs.

To add a custom pattern

1. In the Control Center, click **Compliance > 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.
   
   You can copy a regular expression from a policy template condition and paste it into the Regular Expression text box here. Doing so will make the regular expression available to other policies as a named pattern from the matches pattern drop-down list on the Content Compliance Policy Condition page.

6  Click **Save**.
   
   The system verifies that the pattern name is unique. If the pattern name is not unique, you are prompted to enter a (case insensitive) name.

   After clicking **Save**, the regular expression is stored and is available to use when building compliance policy conditions.

See “About pattern policy resources” on page 314.

See “Editing custom patterns” on page 316.

See “Deleting custom patterns” on page 317.

**Editing custom patterns**

You cannot edit the basic and premium patterns provided by Symantec Brightmail Gateway, however, you can create and edit custom patterns to suit your unique needs.

To edit a custom pattern

1  In the Control Center, click **Compliance > Resources > Patterns**.

2  Click the **Custom** tab.

3  Click the underlined custom pattern. Or, click the check box opposite the pattern and then click **Edit**.

   If you select more than one custom pattern and click **Edit**, you receive an error message indicating that editing more than one custom pattern at a time is not allowed.

4  In the **Pattern name**: field, edit the pattern name.

   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.

6  Click **Save**.

See “About pattern policy resources” on page 314.
See “Creating custom patterns” on page 315.
See “Deleting custom patterns” on page 317.

Deleting custom patterns

You cannot edit the basic and premium pattern resources provided by Symantec Brightmail Gateway. You can, however, create, edit or delete custom patterns to suit your unique needs.

To delete a custom pattern

1. In the Control Center, click Compliance > Resources > Patterns.
2. Click the Custom tab.
3. Click the checkbox opposite the pattern(s) you want to delete. Or, you may select all the patterns for deletion by clicking the checkbox opposite Patterns.
4. Click Delete.

If a custom pattern is referenced in a policy, it cannot be deleted. An error message lists the patterns used and the policies that reference them.

See “About pattern policy resources” on page 314.
See “Creating custom patterns” on page 315.
See “Editing custom patterns” on page 316.

About using structured data records in policy conditions

When creating a policy using premium resources, you can include customer data supplied by your organization. A record lets you create policy conditions that reference proprietary data in filtering messages for content compliance. By using a record as a policy resource, you can identify or protect specific customer, employee, patient, or other data that cannot be identified using regular expressions or keywords.

For example, the Gramm-Leach Bliley Act recommends a combination of name, social security number, and address data that would protect against identity theft. You can upload a company-specific record resource of those data sets to use as part of a structured data Gramm-Leach Bliley compliance policy to protect against data loss.

Record resources use Structured Data detection. You use a data source file provided by your company to create a record that includes rows of company-specific delimited data that you want to protect. You map your data source fields to a set of Symantec Brightmail Gateway fields. Once uploaded, subsets (views) of these fields are then referenced by policy conditions in your structured data policy.
See “Record system patterns” on page 583.

Consider the following if you choose to use a Structured Data premium template:

- By using a company-specific data source file, you can reduce the incidents of false positives. You match only the data that you want to protect.

- Structured data records are typically used in policies for data loss prevention. For example, you might use structured data to filter outbound email for sensitive proprietary customer or employee data.

- Creating a structured data record depends on having access to a data source file. Consider whether or not you have access to a data source file and if it contains the appropriate data for your filtering needs.

- Structured data detection requires a greater degree of resource consumption than the Described Content policy template. Uploading a large data source file can be processing-intensive.

Once the record has been defined as a resource and replicated to all enabled and attached Scanners, you define one or more views, or data subsets of the record. A view is used to identify a subset of fields from the associated record and is used by a structured data policy to match a condition against message content.

On the Add Content Compliance Policy page, you can choose a template by clicking in either the Described Content column or the Structured Data column. To use a record as a resource in a policy, you must click in the Structured Data column when creating the policy.

See “About creating a record resource for compliance policies” on page 318.

**Note:** You cannot enable a policy with a structured data condition until a required record and one or more views have been defined, uploaded, indexed, and replicated as a resource to all enabled Scanners. Structured data conditions are designated as required in premium Structured Data policy templates by the words "Not Defined" highlighted in red text.

---

**About creating a record resource for compliance policies**

If you plan to configure a policy with conditions that reference customer data, such as employee social security numbers, that your organization supplies, you need to create at least one record as a policy resource. You create a record when you upload a text file containing rows of delimited data (the data source file), whose columns you have mapped to predefined or custom field names, as a Symantec Brightmail Gateway resource. To make the record available as a compliance policy resource, you replicate the record to Scanners and create
individual views (data subsets) that different policy conditions can reference when scanning email.

Before you can create a record resource, you must first obtain a text-only delimited file of the data source that you want a Structured Data policy to reference as a Record resource. You then map the columns in your data file to the field names that define a Record resource. Structured Data policy templates require that you provide data files with the columns required by a given policy. For instance, if you use the Price Information Structured Data policy template, your data file must include columns that correspond to the SKU number for the item and its price. Check the policy template before obtaining the database file to make sure that your database administrator can provide data for the fields that are required by the Structured Data policy that you are creating. If your data file does not contain all the fields required by the policy template, you need to modify the conditions specified in the template accordingly.

You map each column in your data source file to a Record resource field name in either one of two ways:

- As a customized field name – In this case, a Structured Data policy references the Record resource field by its column heading in the delimited data source text file. Check the box under Data Source Attributes to indicate that the data source file contains a header row. Data in columns identified by a customized field name are treated as of type WORD and are not validated when the index is created.

- As a system pattern field – In this case, Symantec Brightmail Gateway matches data in a Record-resource field against a system pattern defined by a set of regular expressions. Data in your data source file must conform to one of the regular expressions for a data file to be successfully uploaded and indexed. You do not need to check that the Data source file contains a header row box if you define all fields as system patterns.

When mapping columns in your data file to the Record resource definition, make sure that the following conditions are met:

- Symantec recommends that you use customized field names in the Record-resource definition that are similar to the field names used by the Structured Data policy template to identify matches. For example, if you use the Resumes template, you should map the first_name and last_name columns in your data source file to similarly named customized fields in the Record resource definition.
  See “About compliance policy templates” on page 302.

- The system-pattern fields must correspond to the data types used by the Structured Data policy template to identify matches. For example, if you use
the Customer Data Protection template, you should use system pattern fields that correspond to SSN, CCN, Phone, and Email columns.

- The data used in the data file should match the type of system pattern selected for the field name.
- Make sure that your data source file contains the minimum number of columns that you will use to define a Record resource view. For example, a Structured Data policy that calls for a minimum of three fields to trigger a rule must be able to reference at least those three fields, which must be mapped to the Record resource. For example, when using the EU Data Protection Directives policy template, any view that accesses the EU Data Protection Directives rule should be configured to match entries in at least 4 of 5 fields: Last name, email, phone, account number, and username.

- The size of the data file should not exceed 1.5GB. Larger files sizes cannot be indexed when uploaded as a Record resource.
- Set Maximum Allowable Errors to a percentage of the total rows that can safely return errors and continue processing. Setting too low of a percentage may make it difficult to complete processing an otherwise useful data source file. Setting the percentage too high may hide the fact that the record file is partially corrupted, and should be repaired or recreated before continuing.

Keep in mind the following issues when mapping data file columns to a Record resource system patterns:

- 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.

- If your data source contains adjacent fields you map as number patterns, Symantec recommends that you use a tab or pipe instead of a comma as your field delimiter. Otherwise, the Record resource validator may interpret two numbers from adjacent fields as a single number belonging to the first field, with digits offset by commas, and return an error. For example, the Record resource validator can interpret two adjacent, comma-delimited fields—Age and Weight—in one row as 25,150 under one column rather than as 25, 150 under separate Age and Weight columns, respectively.

- Symantec Brightmail Gateway does not match rows occurring more than 99 times.

- Symantec Brightmail Gateway cannot match entries consisting of a single character. Each entry must contain at least two alphanumeric characters.

Creating a record requires the following steps:

- Obtain a comma-separated values (CSV) data source file in UTF-8 format that contains the specific values for the data you want to protect. Other supported
delimiter characters for the data source file can be tab (tab key) and pipe (|). Optionally, this file can have a header row at the beginning. The data source file should not exceed 1.5GB. Files larger than 1.5 GB cannot be indexed when they are uploaded as a record.

- Define the record by mapping data source columns to predefined or custom record-resource field names.
- Upload the data source file and replicate the generated record to attached and enabled Scanners.
  See “Defining data for a record resource” on page 322.
- Define views.
  A view identifies the set or a subset of fields named in a record. A compliance policy condition references a view when Symantec Brightmail Gateway scans messages for matches to structured-data content.
  See “Defining a record resource View” on page 325.

**Note:** Compliance policy conditions do not reference a record resource directly. Before you can add or edit a policy condition that references data that has been mapped to a record, you must define at least one view for that record. A view can consist of the set of fields mapped to a record or, more usefully, a subset of those fields. You can define more than one view per record, and different policies can reference the same view.

Note the following additional information about records:

- If you change the name of a record, all conditions that reference views of that record reflect the name change.
- You can edit and update a record definition provided that no upload of the record is in progress or pending. You must, however, remember to upload and replicate the updated record definition.
- While an existing record is being updated and uploaded, any policies that reference a view of the record continue to implement the older definition of the record until the updated record has been successfully uploaded and replicated to attached and enabled Scanners.
- You can modify a record definition by mapping additional data source columns to record field names. Any existing views referenced by policy conditions remain valid during the update. After the updated record is uploaded to the Control Center and replicated to enabled Scanners, all previously defined policies remain valid and all new column fields made available for use in creating additional views.
You cannot delete a named field from a record resource definition if it is part of any existing view, whether or not a policy condition references that view. Attempting to delete such a field generates an error message at the top of the Edit Record Resource page.

■ When you construct an EDM data source it must be well formed for successful matching. Use or create a data source that has a single word (or character depending on the language) per delimited field. For example, if you want to match the data "1st Street", you should place "1st" in one delimited field and "Street" in a separate (but following) field.

If you place the string "1st street" in a single delimited field, you have placed multiple "words" in the same cell, since the words are separated by white space, and a match is then unlikely since the only match expected would be when the data being examined is in a tabular format.

Similar behaviors exist when trying to match languages that recognize white spaces differently, such as Korean or Chinese.

■ Symantec Brightmail Gateway recognizes only certain separator characters when it attempts to match Record entries in Credit Card and Number pattern fields. Recognized separator characters (other than space) are tab, comma (,), pound sign (#), hyphen (-), plus sign (+), pipe (|), semicolon (;), and colon (:). Symantec Brightmail Gateway interprets numbers or credit card numbers that use other separators as belonging to type WORD. For example, 4123*6666*7777*8888 would not return a valid match against a credit card number field that included that sequence of digits in a record view.

See “Defining a record resource View” on page 325.

See “Editing a record resource View” on page 326.

See “Defining data for a record resource” on page 322.

See “Record system patterns” on page 583.

**Defining data for a record resource**

If you plan to configure a policy with conditions that reference specific data that your organization supplies, you must create at least one record as a policy resource.

See “About creating a record resource for compliance policies” on page 318.

Before you create a record resource, you must first obtain a text-only delimited file of the data source that you want a Structured Data policy to reference as a Record resource.

When you construct an EDM data source it must be well formed for successful matching. Use or create a data source that has a single word (or character, depending on the language) per delimited field. For example, if you want to match
the data "1st Street", you should place "1st" in one delimited field and "Street" in a separate (but following) field.

If you place the string "1st street" in a single delimited field, you have placed multiple "words" in the same cell, since the words are separated by white space, and a match is then unlikely since the only match expected would be when the data being examined is in a tabular format.

Similar behaviors exist when trying to match languages that recognize white spaces differently, such as Korean or Chinese.

**To define a record resource**

1. In the Control Center, click **Compliance > Resources > Record**.
2. Click **Add**.
3. Specify a Record resource name.
4. Specify an optional description
5. Under Data Source Attributes select the appropriate delimiter character for your data source file.
   
   The supported delimiter characters are Tab (Tab key), Comma (",") or Pipe ("|").
6. Check the **Data source file contains a header row** checkbox if your data source file contains a header row.

A header row is neither processed nor included in the Record resource.

---

**Note:** CRLF line breaks that precede rows in a data set are included in the row count. Instead of skipping the actual header row as it would for a data set without CRLFs, Symantec Brightmail Gateway treats the first CRLF as the header row and returns the values from subsequent rows, including those for the actual header row. If system mappings do not match the columns in the header row, Symantec Brightmail Gateway counts the actual header row as invalid because the header row returns values other than those expected. For example, if one column is mapped to recognize the US Zip code pattern and one or more CRLFs begin the data set, Symantec Brightmail Gateway counts the actual header row as a normal row that is expected 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 Brightmail Gateway counts it as an invalid row. Symantec Brightmail Gateway ignores CRLFs that occur within a data set or at the end of a data set. Such CRLFs are not counted as rows.
7 Under **Error Threshold** indicate the maximum allowable percentage of errors that occur before processing is halted.

8 Under **Mapping** indicate the field names to associate with the columns in the data source file.

   You can select the field name from the drop-down list or you may enter custom field names for your Record resource by selecting **Customize...** from the drop-down list.

   Once you select **Customize...** from the drop-down list, an adjacent blank text field is available to enter a unique custom field name. These custom field names cannot be the same as any of the pre-defined list of Field Names and cannot be the same as any other custom field name in the Record resource. These custom fields are then available to use when creating a View that references the Record resource.

9 Change the order of one or more columns and associated Field Names by clicking the check box opposite the Field Names and then clicking **Move Up** or **Move Down**.

   Use **Move Up** and **Move Down** when you want to modify the mappings for the Record resource without having to delete all the mappings and then recreate them. For example, a new version of the data in your Record resource might have columns 2 and 3 interchanged. You can move up the mapping for column 3 to interchange the mapping for column 3 and column 2.

10 Click **Next** to locate the data-source file on your computer and upload it to Symantec Brightmail Gateway as a structured-data resource.

   After the Record resource has been defined, you must upload the data source file that contains the structured data that you want to a policy to reference.

**Warning:** Symantec Brightmail Gateway does not support indexing of data-source files larger that 1.5GB for upload as a Record resource. Attempts to upload a larger-size file will cause Symantec Brightmail Gateway to return an error message suggesting that you split the file into smaller segments.

**To upload a data-source file and replicate a Record resource**

1 In the Control Center, click **Compliance > Resources > Records**.

2 Click on the Record resource you want to edit.

   The Edit Record Resource page appears. This is the same page you see when you Add a record resource.

3 Under Record Resource Data Source, click **Browse** to locate the data source file on your file system.
4 Click **Upload**.

When you click **Upload**, the file is uploaded and processed. This upload process can be a long-running process and you may want to schedule it at off-peak times if the data source file is very large.

After the Record Resource Status page appears, you can view the status of the upload under Processing Status. Possible statuses for a Record resource are:

- Complete
- Failed
- In Progress

In addition, Processing Status displays the time the upload and processing started, ended, and the number of rows either uploaded or processed.

5 If the Record Resource Status page shows that the data-source file has completed uploading, click **Replicate Now** under **Replication Status** on the Record Resource Status page.

6 Click **OK**.

To cancel the replication of a Record resource to all enabled Scanners, click **Cancel Replication**.

7 Refresh the Record Resource Status page to display the status, start, and end of the replication process, and the size of the Record resource replicated.

See “About creating a record resource for compliance policies” on page 318.

See “Editing a record resource View” on page 326.

See “Defining a record resource View” on page 325.

See “Record system patterns” on page 583.

**Defining a record resource View**

Symantec Brightmail Gateway uses regular expression system patterns to find data in a Record resource.

After the Record resource has been replicated to the Scanner, you define a View. A View is used to identify sets of fields from the associated record resource and is used in a policy condition to identify a match set from the associated Record resource. A Record resource is not directly usable from within a policy until you create a View.

See “About creating a record resource for compliance policies” on page 318.
To add a Record resource View

1. In the Control Center, click **Compliance > Resources > Records**.
2. On the Records page, check the box next to the Record resource for which you want to create a View.
3. Click **Views**. The Record Resource Views page appears.
4. Under Customer Data Views, click **Add**.
5. Specify a View name that is unique within the Record resource.
6. Under Field Selection, select any combination of custom or pre-defined fields which when matched are used to define an occurrence of this View.
7. Specify the number of fields that must be matched to trigger a Record resource rule in this View.
   A number of Structured Data policy templates require more than one field to trigger a rule.
   See “Structured Data Compliance policy templates” on page 522.
8. Under **Exception Combinations**, select the combination of fields that you do not want to trigger the policy condition.
9. Click **Save**.

Some Structured Data policy templates except certain combinations of fields from triggering a rule. For example, a View might include any of the following fields: Last Name, Social Security Number, Credit Card Number, Phone Number. An exception combination might consist of fields for First Name, Last Name, and Phone Number. A message that contained a person’s first and last names and phone number would not trigger a policy even if it contained information that matched the other fields in the View.

To configure an exception combination, you need to edit the existing View.

See “Editing a record resource View” on page 326.
See “Defining data for a record resource” on page 322.
See “Record system patterns” on page 583.

**Editing a record resource View**

A View is used to identify sets of fields from the associated record resource and is used in a policy condition to identify a match set from the associated Record resource.

See “About creating a record resource for compliance policies” on page 318.

Once a view has been created, it can be edited.
To edit a Record resource view

1. In the Control Center, click **Compliance > Resources > Records**.
2. On the Records page, check the box next to the Record resource for which you want to edit a View.
3. Click **Views**.
4. On the Record Resource Views page, click the name of the View that you want to edit.
5. Select the fields that you want to add to an exception combination. Deselect any fields that you do not want as part of an exception combination.
6. Click **Add**.
7. On the Edit Exception Combinations page, select the fields that you want as part of an exception combination.
8. Click **Save**.

You cannot save the configuration if you selected the full set of fields or if the number of selected fields does not equal the minimum number of matched selected fields that are required for an occurrence.

See “Defining a record resource View” on page 325.
See “Defining data for a record resource” on page 322.
See “Record system patterns” on page 583.

About using regular expressions in conditions

In addition to the named regular expressions (Patterns) that Symantec Brightmail Gateway provides as basic and premium Pattern resources, it also delivers predefined regular expressions as part of the premium policy template definitions. Besides providing predefined conditions for policy templates, these regular expressions can be used to create additional content filtering conditions in policies you create.

Regular expressions are designed to match on a line-by-line basis when configured to match against a message subject line, but only match against the entire body text when configured to match against the message body. Regular expressions will not match on a line-by-line basis when configured to match against a message body.

Unlike a Pattern resource, regular expressions do not appear as resources in the Control Center. They cannot be directly accessed from the Content Compliance Policy Condition page when you add a condition to a policy. They can only be
viewed from an existing premium policy template or policy derived from such a template.

See “Regular expressions for context-filtering conditions” on page 525.

See “Using Perl-compatible regular expressions in conditions” on page 329.

To use any of the regular expressions that come with the Premium Content Control module, keep in mind the following precepts:

■ You are not limited to using the regular expressions supplied in the policy templates. You can write your own Perl-compatible regular expressions. See “Using Perl-compatible regular expressions in conditions” on page 329.

■ You must first identify the policy template in which the regular expression that you want to use appears as a condition. Regular expressions are not identified by name in these conditions. See “Premium pattern resources” on page 536.

■ In policy templates where more than one regular expression appears, you must also identify which regular expression is the appropriate one for the condition that you want to define. If you are in doubt about which regular expression to use, check the conditions listed under the particular policy template in which the regular expression appears. See “Premium regular-expression resources keyed to policy templates” on page 541.

Once you have located the policy template and identified the regular expression that you want to use in a policy, you can copy the regular expression from the policy template and paste it in either of two places:

■ The Regular Expression text box under Add Patterns on the Custom tab of the Patterns page. This procedure makes the regular expression available as a custom pattern resource when you select Matches pattern or Does not match pattern on the Content Compliance Policy Condition page. Symantec recommends that you create custom patterns for regular expressions you intend to use in more than one policy.

■ The text box adjacent to the regular expression drop-down menu on the Content Compliance Policy Condition page. Use this procedure if you only need to use the regular expression for a condition once. The regular expression will be saved as a condition of the policy you create but does not appear as a pattern resource for use in other policies. See “Adding conditions to compliance policies” on page 289.
Using Perl-compatible regular expressions in conditions

When creating conditions, you can use regular expressions that behave like Perl regular expressions. To do this, click “matches regular expression” or “does not match regular expression” in the Content Compliance Policy Condition page for either of the condition options that offer you that choice. Symantec Brightmail Gateway wraps your regular expression in two forward slashes. Symantec Brightmail Gateway supports PCRE version 6.6.

Regular expressions are designed to match on a line-by-line basis when configured to match against a message headers, but only match against the entire body text when configured to match against the message body or attachments.

See “Creating compliance policies” on page 282.

To use a pattern to match certain special characters, including forward slashes, you must escape each with \ as shown in the table.

See “Perl-compatible regular expressions” on page 587.

---

**Note:** Symantec Brightmail Gateway uses two different types of analysis in scanning for messages that match your criteria. If you specify a condition using a regular expression, a regular expression analysis is performed. If you specify a condition using a keyword or dictionary, a text search is performed.

See “About using regular expressions in conditions” on page 327.

See “Regular expressions for context-filtering conditions” on page 525.

---

About Vontu Network Prevent integration

Symantec Brightmail Gateway integrates with Vontu Network Prevent to deliver, route, hold, or block email traffic. Vontu Network Prevent is a component of Vontu Data Loss Prevention, which discovers, monitors, and protects confidential data wherever it is stored or used. With Vontu Data Loss Prevention, you can create policies that extend across endpoint, network, and storage systems. You install Vontu Network Prevent on a separate server. You must have a Scanner configured for outbound mail filtering to route email to Vontu Network Prevent.

You can configure Vontu Network Prevent policies to perform the following actions on messages depending on the type of data 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 Vontu Network Prevent, you can also configure policies on Symantec Brightmail 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 compliance folder and review them before they are delivered. You can optionally configure notification for messages routed to compliance folders.

Encrypt

Government regulations or your own policies may require that you encrypt sensitive messages.

See “Common Vontu Network Prevent actions” on page 331.

**Note:** You cannot route inbound mail through Vontu Network Prevent.

---

**How Symantec Brightmail Gateway and Vontu Network Prevent interact**

If you configure Symantec Brightmail Gateway to route email to Vontu Network Prevent, email is typically routed in the following order:

- Symantec Brightmail Gateway accepts outbound messages at the gateway on port 25, by default.
- Symantec Brightmail Gateway passes outbound messages to Vontu Network Prevent on port 10025, by default.
- Vontu Network Prevent scans messages and blocks, redirects, or tags messages for further action by the MTA.
- See “Common Vontu Network Prevent actions” on page 331.
- Vontu Network Prevent passes messages back to Symantec Brightmail Gateway on port 25 (default) unless the Vontu Network Prevent rejects the message. In that case, Symantec Brightmail Gateway returns the message back to the sender with an SMTP 5xx failure response code including text that you specify.
- Symantec Brightmail Gateway processes messages as configured. Symantec Brightmail Gateway can process messages based on subject or header markup of messages by Vontu 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.
If you have multiple Scanners, the Vontu Data Loss Prevention Setup settings in the Control Center apply to all Scanners. Each Scanner routes email to all configured Vontu Network Prevent servers according to the preference order. If Vontu Network Prevent is configured in reflecting mode then each Vontu Network Prevent server returns each message to the Scanner from which it received the message. If Vontu Network Prevent is configured in forwarding mode then Vontu Network Prevent servers pass messages to the next destination.

See “About Vontu Network Prevent preference order” on page 333.


## Ports used for Vontu Network Prevent integration

Table 12-3 describes the default ports used if you route email to one or more Vontu 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>Vontu Network Prevent</td>
<td>Outbound email for processing by Vontu Network Prevent</td>
<td>—</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Vontu Network Prevent</td>
<td>Scanners</td>
<td>Outbound email that was processed by Vontu Network Prevent</td>
<td>By default, Vontu Network Prevent returns email to port 10026. You may need to change the Remote SMTP Listener Port setting on Vontu Network Prevent to match the port that Symantec Brightmail Gateway expects, such as port 25.</td>
</tr>
</tbody>
</table>

## Common Vontu Network Prevent actions

Symantec Brightmail Gateway and Vontu Network Prevent interoperate by exchanging SMTP messages. Using response rules and policies, Vontu Network Prevent can modify, reroute, and reject messages. Some actions that you configure Vontu Network Prevent to take on email require no further action by Symantec Brightmail Gateway. Other actions require you to configure Symantec Brightmail Gateway.
Table 12-4  Common Vontu 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 Vontu 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 Brightmail Gateway to search for the custom header and act on the message. Symantec Brightmail Gateway can delete, archive, create an incident and hold the message for review, etc.</td>
</tr>
<tr>
<td></td>
<td>You can also run reports on the actions that Symantec Brightmail Gateway takes on matching messages.</td>
</tr>
<tr>
<td></td>
<td>See “Creating an incident based on Vontu Network Prevent header markup” on page 336.</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 Brightmail Gateway to search for the specific text in the subject line and act on matching messages.</td>
</tr>
</tbody>
</table>

Supported Vontu Network Prevent delivery modes

You can integrate Vontu Network Prevent into your network architecture using two methods. For both methods, Vontu 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.

- Reflecting: After processing messages, Vontu Network Prevent returns the message to the Scanner from which it came.
- Forwarding: After processing messages, Vontu Network Prevent passes messages to the MTA that you specify.

The method you choose depends on the particular requirements at your site.
About performance implications for Vontu Network Prevent integration

Due to the additional processing involved, integrating with Vontu 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 Vontu Network Prevent
- Message content and size
- The number of Vontu Network Prevent servers compared to the volume of mail

You may be able to decrease latency and increase throughput by:

- Adding additional Vontu Network Prevent servers.
- Tuning the maximum number of connections and maximum number of connections from a single IP address settings for outbound SMTP and SMTP delivery. This is a Symantec Brightmail Gateway Scanner setting. See “Configuring SMTP Advanced Settings” on page 118.
- Tuning the NumThreads setting on the Vontu Network Prevent server to optimize throughput depending on the volume of outbound email at your site.

About Vontu Network Prevent preference order

If you have multiple Vontu Network Prevent servers, you can configure the order in which Vontu Network Prevent servers are employed by Symantec Brightmail Gateway. You can use the preference order for server priority, server load balancing, or failover. You set the preference either in the Control Center or in MX records as described in Table 12-5.

<table>
<thead>
<tr>
<th>Preference type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preference on Vontu Data Loss Prevention Setup page</td>
<td>You configure this type of preference on the Vontu Data Loss Prevention Setup page in the Control Center. You must specify a preference value for every Vontu Network Prevent server that you specify. The valid preference range is 1 - 100.</td>
</tr>
</tbody>
</table>
Table 12-5  Available preference types (continued)

<table>
<thead>
<tr>
<th>Preference type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX record preference</td>
<td>You configure MX record preference in the DNS records for Vontu Network Prevent using your DNS software. You must configure MX record preference if the host name you specify routes to more than one Vontu 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>

For both types of preference, lower numbers are attempted before higher numbers. For example, a Vontu Network Prevent server with a preference of 1 is tried before a Vontu Network Prevent server with a preference of 2.

You can use both types of preference in combination. The preference settings on the Vontu Data Loss Prevention Setup page are compared before the preference is checked in the MX record for the chosen host name.

Table 12-6  Uses for preference

<table>
<thead>
<tr>
<th>Preference use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server priority and server failover</td>
<td>Choose a lower preference number for Vontu Network Prevent servers that are running on high network bandwidth computers with ample CPU and hard disk resources. Choose a higher preference number for Vontu Network Prevent servers that are running on lower network bandwidth computers with fewer CPU and hard disk resources. In case a Vontu Network Prevent server is unreachable, the server with the next higher preference number is tried.</td>
</tr>
<tr>
<td>Load balancing</td>
<td>If Vontu Network Prevent servers have the same preference number, Symantec Brightmail Gateway randomly chooses a Vontu Network Prevent server for each outbound message. This random selection of Vontu Network Prevent servers creates load balancing among the Vontu Network Prevent servers.</td>
</tr>
</tbody>
</table>

Configuring Vontu Network Prevent to return email to Symantec Brightmail Gateway

You must configure Vontu Network Prevent server to return email to Symantec Brightmail Gateway on the expected port. On Symantec Brightmail Gateway, the default outbound email port is 25. On Vontu Network Prevent, the default Remote
SMTP Listener Port is 10026. It should be changed to match the Symantec Brightmail Gateway outbound email port.

Table 12-7

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Check the default outbound email port on Symantec Brightmail Gateway</td>
<td>The outbound mail IP address port is shown on the SMTP tab of the Host Configuration page in the Control Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set the Remote SMTP Listener Port for Vontu Network Prevent</td>
<td>Set the Remote SMTP Listener Port for Vontu Network Prevent to the outbound email port used on Symantec Brightmail Gateway. See the Vontu Network Prevent documentation for configuration details.</td>
</tr>
</tbody>
</table>

Configuring email connections to and from Vontu Network Prevent

If you have one or more Vontu Network Prevent servers, you can route email to them from Symantec Brightmail Gateway. Follow these steps to configure Symantec Brightmail Gateway to route email to Vontu Network Prevent. You also must configure Vontu Network Prevent to route email back to Symantec Brightmail Gateway.

See “Configuring Vontu Network Prevent to return email to Symantec Brightmail Gateway” on page 334.

To configure email connections to and from Vontu Network Prevent

1. In the Control Center, click **Compliance > Settings > Vontu DLP Connect**.
2. Check **Enable** to route email to Vontu Network Prevent.
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 Vontu 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 Vontu Network Prevent server.
5. Under Port, specify the port number on the Vontu 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 Vontu Network Prevent server is set to the same port number.
Check **MX Lookup** to enable MX lookup for the Vontu 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.

Under Preference (1 - 100), specify the preference of this Vontu Network Prevent server as compared to all the defined Vontu Network Prevent servers.

See “About Vontu Network Prevent preference order” on page 333.

**Enable bypass when all DLP servers are unreachable** is described in another section.

See “Enabling or disabling bypass for Vontu Network Prevent” on page 340.

8 Under Accept Scanned Mail from DLP servers, click **Add** to add a blank row.

9 Specify an IP address from which Symantec Brightmail Gateway should expect email from Vontu Network Prevent.

Add additional rows to specify the IP addresses of all Vontu Network Prevent servers from which Symantec Brightmail 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 Vontu Network Prevent servers, add the IP addresses of all of those servers.

10 Click **Save**.

Creating an incident based on Vontu Network Prevent header markup

This section describes a sample method to handle any sensitive data that Vontu Network Prevent detects. This method requires configuring both Vontu Network Prevent and Symantec Brightmail Gateway.

In this sample, Vontu Network Prevent adds a custom header to matching messages. Symantec Brightmail 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 compliance folder on Symantec Brightmail Gateway. An administrator can approve, reject, forward, archive, delete, and manage the messages in the compliance folder.

Creating an incident based on Vontu Network Prevent header markup involves the following tasks:

- Configure Vontu Network Prevent to add a custom header to messages it detects with sensitive data. On Create a Modify SMTP Message response rule on the Add/Edit Response Rule screen. You can add up to three RFC 2822 header lines. Symantec recommends using the header **X-Cfilter:** with different values depending upon the wanted action on Symantec Brightmail Gateway.
or scan verdict. For example, you can specify X-Cfilter: Vontu Incident to mark messages for a compliance folder or X-Cfilter: SSN for any messages that contain social security numbers.

■ In Symantec Brightmail Gateway, create a compliance folder, such as "Vontu Incidents". You may want to enable email notification for the compliance folder.

■ In Symantec Brightmail Gateway, create an email compliance 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: Vontu Incident
Condition - The message header: exists
Perform the following action: Create an incident. Add additional actions for approved and rejected.
In compliance folder: The folder you created
Hold message for review checked

About failure behavior with Vontu Network Prevent

If Vontu Network Prevent is unreachable, email may bypass Vontu Network Prevent or wait in a mail queue. The behavior depends on how many Vontu Network Prevent servers are unreachable and whether bypass is enabled. By default, bypass is enabled.

See “Enabling or disabling bypass for Vontu Network Prevent” on page 340.

Vontu Network Prevent servers may be unreachable because of the following reasons:

■ Failures in the network
■ Failures on the hardware on which Vontu Network Prevent is running
■ The network bandwidth, hardware speed, or number of Vontu Network Prevent servers are not adequate for the mail flow
Table 12-8  Failure behavior with Vontu Network Prevent

<table>
<thead>
<tr>
<th>Bypass status</th>
<th>Vontu 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 Vontu Network Prevent server is bypassed. Email is routed to the next Vontu Network Prevent server according to the preference list, MX record, or both.</td>
</tr>
</tbody>
</table>
| Bypass disabled             | All unreachable                     | Email is stored in the delivery queue of Symantec Brightmail Gateway. No outbound email is delivered. If the Vontu Network Prevent servers continue to be unavailable, the delivery queue grows larger as time passes. Messages can get stuck in Symantec Brightmail Gateway if the following conditions are met:  
  - The Maximum number of messages in the delivery queue limit is reached.  
  - "Defer new connections when delivery queue is full" is enabled. 
New inbound and outbound connections are deferred when the delivery queue becomes full. 
See “Correcting a delivery queue backup to Vontu Network Prevent” on page 338. 
See “Configuring SMTP Advanced Settings” on page 118. |
| Bypass enabled (default)    | All unreachable                     | Email is not routed to Vontu Network Prevent servers, but Symantec Brightmail Gateway does process it. Sensitive data can leave your site unscanned unless you configure Symantec Brightmail Gateway appropriately. 
See “Managing unscanned email if bypass is enabled for Vontu Network Prevent” on page 340. |

Correcting a delivery queue backup to Vontu Network Prevent

If you have disabled bypass to the Vontu Network Prevent servers and the servers are unreachable, messages back up in the delivery queue. Normally when the Vontu 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 Brightmail Gateway is too low.

The amount of free memory on Symantec Brightmail Gateway is too low.

The following conditions on Symantec Brightmail Gateway are met:

- The Maximum number of messages in the delivery queue limit is reached.
- "Defer new connections when delivery queue is full" is enabled.

See “About failure behavior with Vontu Network Prevent” on page 337.

If Vontu Network Prevent servers continue to be unavailable, the queue may grow to a large size and consume large amounts of disk space. Low disk space can cause problems on Symantec Brightmail Gateway, including the inability to deliver messages.

 Attempt the following tasks in this order to clear the delivery message queue:

- Correct the issue with the Vontu Network Prevent servers by confirming that the Vontu Network Prevent servers are running, have sufficient capacity for processing the given email volumes, and network paths are reachable.

- If disk space is low on the Symantec Brightmail Gateway Scanners, free disk space such as by deleting report data or logs. See “clear” on page 595.

- Temporarily or permanently enable bypass. Sensitive data can leave your site unscanned unless you configure Symantec Brightmail Gateway appropriately. See “Managing unscanned email if bypass is enabled for Vontu Network Prevent” on page 340. See “Enabling or disabling bypass for Vontu Network Prevent” on page 340.

- Halt message flow to Scanners by changing the MTA operation to "Do not accept incoming messages." See “Managing services, Scanner replication, and MTA operations” on page 108.

- 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 118.
Optionally, in the Control Center, access the Status > SMTP > Messages Queues page and flush all queues. The MTA flushes queues automatically, but this manual action expedites queue processing.

Enabling or disabling bypass for Vontu Network Prevent

By default, outbound email bypasses Vontu Network Prevent if all Vontu Network Prevent servers are unavailable. Bypass is triggered only if a connection cannot be established with the Vontu Network Prevent servers. Bypass is not triggered in the following cases:

- The connection to Vontu Network Prevent server is established but the connection is deferred.
- The email results in an SMTP 4xx temporary failure. The Symantec Brightmail Gateway MTA attempts to redeliver the message later.
- The email results in an SMTP 5xx permanent failure. The Symantec Brightmail Gateway MTA sends a bounce message to the sender.
- The Vontu Network Prevent server is just slow in processing the SMTP connection. However, if the SMTP connection times out, bypass is triggered if no other Vontu Network Prevent servers are available.

Sensitive data can leave your site unscanned if Vontu Network Prevent servers are unreachable. If you disable bypass and Vontu Network Prevent is unavailable, all outbound email waits in the delivery queue which prevents timely delivery.

See “About failure behavior with Vontu Network Prevent” on page 337.

See “Managing unscanned email if bypass is enabled for Vontu Network Prevent” on page 340.

To enable or disable bypass for Vontu Network Prevent

1. In the Control Center, click Compliance > Settings > Vontu DLP Connect.
2. To enable bypass, check Enable bypass when all DLP servers are unreachable.
   To disable bypass, uncheck Enable bypass when all DLP servers are unreachable.
3. Click Save.

Managing unscanned email if bypass is enabled for Vontu Network Prevent

By default, outbound email bypasses Vontu Network Prevent if Vontu Network Prevent is unavailable. Sensitive data can leave your site unscanned if Vontu Network Prevent servers are unreachable. However, you can configure a policy
on Symantec Brightmail Gateway to prevent unscanned messages from leaving your site. You can use a variety of policy configurations to prevent unscanned messages from leaving your site. The following outline describes how to prevent unscanned messages from leaving your site by creating an incident for unscanned messages. In this policy configuration, the administrator of the compliance folder receives notification if an unscanned message is detected. Unscanned messages are held in the compliance folder for review.

- Ensure that the Vontu Network Prevent server adds a header to messages it processes. By default, Vontu Network Prevent adds the header X-CFilter-Loop: to messages it processes.

- In Symantec Brightmail Gateway, create a compliance folder for unscanned messages and configure email notification for the compliance folder.

- In Symantec Brightmail Gateway, create an email compliance 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 compliance folder: The folder you created
  Hold message for review checked

Alternatively, you may not need to store unscanned messages but want to be notified if messages are unscanned. You can create an email compliance policy on Symantec Brightmail Gateway to send an email notification if unscanned messages are detected.

See “About notifications” on page 294.

About Vontu Network Prevent reports

Symantec Brightmail Gateway does not provide reports specifically for Vontu Network Prevent activity. Use Vontu Network Prevent for reports on its activity.
Some activity that is related to Vontu Network Prevent may be part of reports on Symantec Brightmail Gateway. For example, you could create a compliance incident for the messages that are marked up by Vontu Network Prevent. That compliance incident activity is reflected in some compliance reports.

See “About working with reports” on page 356.

**Troubleshooting Vontu Network Prevent integration: messages bounce**

If you have recently enabled routing to Vontu Network Prevent and email messages bounce, check the following:

- Accept Scanned Mail from DLP Servers IP address is configured correctly on Symantec Brightmail Gateway.
- The Prevent Server is correctly configured with the reflected port setting that points to the Scanner port.

**Troubleshooting Vontu Network Prevent integration: deferred messages**

If outbound email is returned containing the following error:

421 Forwarding agent unavailable. Closing connection.

the Remote SMTP Listener Port for Vontu Network Prevent does not match the inbound email port on Symantec Brightmail Gateway.

See “Configuring Vontu Network Prevent to return email to Symantec Brightmail Gateway” on page 334.

This describes the error seen in Vontu Data Loss Prevention from Symantec Version 8.1. Future versions may produce different errors.

**Taking Vontu Network Prevent servers offline for maintenance**

Occasionally you may need to take one or more Vontu Network Prevent servers offline to perform maintenance, such as to install a new software release. Table 12-9 describes the effect on mail flow for the options available.
### Table 12-9  Options for taking Vontu Network Prevent servers offline

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| If you have multiple Vontu 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 are true:  
■ You have configured multiple Vontu Network Prevent servers in Symantec Brightmail Gateway  
■ The address you specify for Vontu Network Prevent in Symantec Brightmail Gateway resolves to multiple Vontu Network Prevent servers using MX records  
The Vontu Network Prevent server that is not available is ignored and the next available Vontu Network Prevent server in the preference list is used. |
| Disable routing to Vontu Network Prevent    | Outbound email bypasses Vontu Network Prevent servers. You must manually re-enable routing to Vontu Network Prevent servers when they become available again. Sensitive data can leave your site unscanned by Vontu Network Prevent servers. |
| Enable bypass                               | Outbound email bypasses Vontu Network Prevent servers if none are available. Sensitive data can leave your site unscanned by Vontu Network Prevent servers. When Vontu Network Prevent servers are available again, Symantec Brightmail Gateway automatically routes outbound email to them.  
Bypass is enabled by default. |
| Stop outbound message queue                | No outbound messages are delivered while the queue is stopped. Vontu Network Prevent servers and Symantec Brightmail Gateway eventually scan all outbound messages. You must manually reenable the outbound message queue when Vontu Network Prevent servers become available again.  
See “MTA and message queue behavior " on page 111. |
| Enable routing to Vontu Network Prevent but disable bypass | Outbound messages back up in the delivery queue. |

Bypass is enabled by default. When bypass is enabled, messages are not scanned for sensitive data while the servers are down. If you disable bypass, outbound email remains in the delivery queue. When you later activate Vontu 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 being bounced.

If bypass is disabled, you can perform maintenance on Vontu Network Prevent servers by enabling bypass:

■ Enable bypass in the Control Center of Symantec Brightmail Gateway.
■ Perform maintenance on the Vontu Network Prevent servers.
■ When work on the servers is complete, bring the Vontu Network Prevent servers online again.
■ Disable bypass in the Control Center of Symantec Brightmail Gateway.

Ensure that your organization's policies allow you to enable bypass temporarily.
Monitoring and managing compliance

This chapter includes the following topics:

- About monitoring compliance policies
- About compliance folders
- About incident management

About monitoring compliance policies

You can use a compliance folder to monitor incidents of messages that meet a policy's conditions. Monitoring enables you to understand, prevent, respond to, and audit potential violations of regulatory compliance and internal-governance policies. For example, you can use a compliance folder to monitor the scale of compliance violations at your company before adopting a more permanent compliance policy. You can also have your compliance policy statistics tracked in your dashboard.

You can also use one of the premium templates to create and monitor a policy that facilitates specific kinds of regulatory compliance or other common compliance goals. You should create a specific compliance folder for the type of policy you are creating. If a compliance folder does not exist for a policy, incidents of messages that meet its conditions are logged in the default folder.

See “About compliance folders” on page 346.

When you use the Create an incident action, you can specify the compliance folder in which incidents that meet the conditions of a given policy are held for review before further processing. You can grant or deny administrators and compliance officers access to the compliance folder.
When creating a compliance policy that you want to monitor, in addition to choosing a compliance folder and specifying the Create an incident action, you can also include at least one of the following actions:

- Deliver message normally
- Delete the message
- Forward a copy of the message
- Archive the message

You can add other actions to the policy provided that they are compatible with each other. If you only specify the Create an incident action, the message is copied to the compliance folder you chose for that policy.

Messages that meet the conditions of a policy can be held for later review by selecting the Create an incident action when creating a policy. An incident is recorded in the appropriate compliance policy folder.

You can also configure the actions that you want a policy to take and defer executing them until someone has approved or rejected an incident that has been held for review in a compliance policy folder. When you select the Create an incident action and check Hold for review, you can add any compatible actions to the list of Message Review Approved Actions or the list of Message Review Rejected Actions. These actions take effect after a compliance officer approves or rejects the message.

See “About incident management” on page 351.

About compliance folders

Compliance folders serve as containers that allow you to organize, monitor, and manage incidents generated by compliance policies.

See “Creating compliance policies” on page 282.

You should create a compliance folder for each type of policy that you intend to create before you create actual policies. If you are working with policies that use premium templates, create a compliance folder corresponding to each premium template that you use. For example, you can create a HIPAA compliance folder and a Sarbanes-Oxley compliance folder to monitor any incidents generated by policies that you create based on those premium templates.
Note: If you have not created a compliance folder for a policy that generates an incident action, incidents generated by that policy are filed in the Default compliance folder. You can view a list of these incidents by clicking Compliance > Default folder.

To monitor outgoing email messages to competitors, you can create a policy using the Competitor Communications premium template to catch incidents of outgoing email messages to competitor domains and create a Competitor Incidents compliance folder to monitor those incidents.

For each compliance folder that you create, you can specify archive settings and notification settings. For example, you may want to archive all HIPAA incidents with a special archive tag and special character encoding, and notify a set of HIPAA Compliance Officers as well as an administrators of each incident. You can specify all these settings on the Add Compliance Folder page.

Additionally, you can use compliance folders to manage incidents that defer actions on messages matching the conditions of a given policy. By checking Hold for review when you select the Create an incident action on the Email Content Compliance Policy page, any other actions that you have selected for that particular policy are deferred until a compliance officer or administrator has reviewed incidents logged in that policy's compliance folder. For example, you may want to log all incidents of messages to and from competitors in a Competitor Communications folder (based on the premium template). The actions of one policy for inbound communications would log an incident but deliver mail to the recipient normally. The actions of another policy would hold outgoing communications for review until an administrator or compliance officer reviews message content for proprietary information. The policy for outbound mail might include actions that, if the incident is approved, would forward the message for delivery or, if the incident is rejected, delete the message and notify the sender.

The Compliance Folder Overview page shows the status of incidents in your compliance folders. Except for the new and unknown statuses, the status reported on this page reflects determinations made on incidents by compliance officers at your site. Table 13-1 describes the values displayed on the page.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance folder</td>
<td>Compliance folder for which to display status</td>
</tr>
<tr>
<td>Display</td>
<td>Displays status summary for selected folder.</td>
</tr>
<tr>
<td>Status</td>
<td>Status (new, active, confirmed, false positives) of incidents in compliance folder</td>
</tr>
</tbody>
</table>


### Table 13-1  Compliance folder overview (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Severity</td>
<td>A compliance officer determined that the incident is of low severity.</td>
</tr>
<tr>
<td>Medium Severity</td>
<td>A compliance officer determined that the incident is of medium severity.</td>
</tr>
<tr>
<td>High Severity</td>
<td>A compliance officer determined that the incident is of high severity.</td>
</tr>
<tr>
<td>Unknown Severity</td>
<td>New incidents that haven't been prioritized by a compliance officer</td>
</tr>
<tr>
<td>Total</td>
<td>The total number of incidents for the particular row</td>
</tr>
<tr>
<td>New</td>
<td>New incidents that haven't been categorized</td>
</tr>
<tr>
<td>Active</td>
<td>A compliance officer set the status to active. The incident is under review.</td>
</tr>
<tr>
<td>Confirmed</td>
<td>A compliance officer set the status to confirmed. The incident is valid.</td>
</tr>
<tr>
<td>False Positives</td>
<td>A compliance officer set the status to false positive. The incident is not valid.</td>
</tr>
<tr>
<td>Total Incidents</td>
<td>The total number of low, medium, high severity and unknown incidents, and the sum of those incidents</td>
</tr>
</tbody>
</table>

See “Adding compliance folders” on page 348.

### Adding compliance folders

Once you have created a compliance folder, the name of the folder appears in the drop-down list of available folders when you select the Create an incident action on the Email Content Compliance Policy page.

To create a compliance folder, you need the appropriate administrative rights.

See “Adding administrators” on page 439.

**To add a compliance folder**

1. In the Control Center, click **Compliance > Settings > Compliance Folders**. The Compliance Folders Settings page appears.

2. Click **Add**.
In the Content compliance folder name field, type a name for the compliance folder that you want to use to manage incidents generated by a content-filtering policy.

This name will appear in the Compliance Folder drop-down list on the Compliance Folder Overview page, in the list of available compliance folders when adding the Create an incident action to a policy, and on the left menu of the Control Center under Compliance > Incident Management.

In the Optional incident archive tag field, you can type identifying text for incidents in this folder.

When you specify an archive action on an incident in this compliance folder on the Incident Management page, the text you enter in this field will accompany the incident.

If you specified an incident archive tag, you can choose a character encoding set to use for the tag in the Encoding drop-down list.


In the Notification format drop-down list, you can choose a format for incident notifications, either Multipart (HTML and text), HTML only or text only.

Click Edit to view or edit the incident notification template.

See “Editing notification templates for compliance folders” on page 297.

In the Notification recipient addresses field, type the email addresses of the compliance officers who should be notified of incidents in this folder.

You can add multiple email addresses, separated by commas, semicolons, or spaces.

In the Administrator Notifications list, check the names of administrators whom you want to be notified of incidents in this folder.

After the compliance folder is added, you can also specify administrators to notify on the Edit Administrator or Add Administrator pages. Changes made on any of these three pages are reflected on all of them.

Click Save to save your changes, add this compliance folder, and return to the main Compliance Folder Settings page.

Click Cancel to cancel your changes and return to the main Compliance Folder Settings page.

See “About compliance folders” on page 346.
Editing compliance folders

Once you have created a compliance folder, you may edit or delete it. You can add or edit these folders as you create and modify your compliance policies, to ensure that the folders accurately collect the incidents created by the related policy.

To edit a compliance folder, you need the appropriate administrative rights.

See “Adding administrators” on page 439.

To edit a compliance folder

1. In the Control Center, click **Compliance > Settings > Compliance Folders**.
   
   A list of existing compliance policy folders appears in the Compliance Folder Settings page.

2. Click on the linked name of a compliance folder in the Compliance Folders list or check the adjacent box and click **Edit**.

   The **Edit Compliance Folder** page appears.

3. Edit the compliance folder settings as necessary.

   You can change the compliance folder name, archive tag, and encoding, modify notification settings, and indicate administrators whom you want to notify of incidents.

4. Click **Save** to save the new settings or **Cancel** to return to the Compliance Folder Settings page without saving changes.

Deleting compliance folders

Compliance folders serve as containers that allow you to organize, monitor, and manage incidents generated by compliance policies.

To delete a compliance folder you need the appropriate administrative rights.

See “Adding administrators” on page 439.
To delete compliance folders

1. In the Control Center, click Compliance > Settings > Compliance Folders.
2. Check the compliance folders you want to delete.
3. Click Delete.

See “About compliance folders” on page 346.
See “Editing compliance folders” on page 350.
See “Setting the compliance folder storage threshold” on page 351.

Setting the compliance folder storage threshold

Once you create a compliance folder, you must configure the maximum allowable storage size for all compliance folders.

To set a compliance folder threshold, you need the appropriate administrative rights.

See “Adding administrators” on page 439.

To set the compliance folder storage threshold

1. In the Control Center, click Compliance > Settings > Compliance Folders.
2. Under Threshold, check Maximum size for all Compliance Folders (combined) to enable this setting.
3. Type an integer.
   This value must be less than the amount of available storage.
4. Choose KB, MB, or GB.
5. Click Save.

See “About compliance folders” on page 346.
See “Adding compliance folders” on page 348.
See “Setting the compliance folder storage threshold” on page 351.
See “Deleting compliance folders” on page 350.

About incident management

Once you filter incidents into compliance folders, you can then initiate various actions on selected incidents.

If you want to monitor violations, do the following before creating your compliance policy:
Create a compliance folder to track messages that meet the conditions of this policy, and specify whom to notify of a potential violation of company policy. See “About compliance folders” on page 346.

If necessary, add entries to dictionaries that are to be referenced by the policy. For example, for a Competitor Communications policy you will want to add the domain names of competitors to the Competitor Domains dictionary. See “About dictionary resources” on page 305.

If you intend to reference a record resource, make sure that you have obtained any necessary permissions, mapped and uploaded a delimited text version of your data source to the Control Center, created the necessary Views, and replicated the Record resource to the appropriate Scanners. See “About creating a record resource for compliance policies” on page 318.

After configuring one or more compliance policies to create an incident, you can monitor and manage the incidents on the Incident Management page for the compliance folder in which incidents for a particular policy are logged. See “Acting upon incidents” on page 352.

See “Forwarding and tracking incidents” on page 353.

**Acting upon incidents**

Once your compliance folders begin collecting incidents that match conditions specified in your compliance policies, you can use the Incident management page to take specific actions for each incident.

For more information about creating compliance folders that collect incidents, see “About compliance folders” on page 346.

**To archive, delete, approve or reject, or update single incidents**

1. In the Control Center, click **Compliance** and then click a compliance folder. An administrator must have given you modify permission for the folder to categorize incidents.

2. Specify the type of incident to view by setting the search filters. Click the subject of a message to display it.

3. In the details panel of the Incident Management page, archive, delete, forward, or update the status, severity, or review action of an incident as appropriate. You can also add a comment.

4. If you have updated the status, severity, or review action of an incident or added a comment, click **Update**.

See “About incident management” on page 351.
See “Forwarding and tracking incidents” on page 353.

Forwarding and tracking incidents

In addition to taking specific actions upon an incident collected in your compliance policy folders, you can also forward the incident for further review and export the incident history information.

For more information about creating the compliance folders that collect these incidents, see “About compliance folders” on page 346.

To forward an incident or export an incident history

1. In the Control Center, click **Compliance** and then click a compliance folder.
2. Select the compliance folder whose content you wish to review.
3. Click on the message title in the **Subject** column to review the contents.
4. Click **Back to Compliance Folder** to return to the incidents listed for that folder.
5. Check the box of the incident you want to forward under the **Incident ID** column.
6. Select an **Encoding** from the drop-down list.
7. Click **Forward Incident** to forward the incident or skip to 11 if you want to export an incident history.
8. In the **Forward to** text box, enter the email address.
9. In the **Subject** text box, enter a subject name.
10. In the **Comments** text box, type a message that you want to accompany the incident email.
11. If you want to export a message incident history, select the type of delimiter from the **Delimiter** drop-down list to use in a comma-separated values (CSV) text file.
12. Click **Export Incident History** to export an incident history.

See “About incident management” on page 351.
See “Acting upon incidents” on page 352.
Working with reports

This chapter includes the following topics:

■ About working with reports
■ Selecting the data to track for reports
■ Creating and configuring reports
■ Saving favorite reports
■ Editing a favorite report's filter options
■ Editing a favorite report's schedule
■ Copying favorite reports
■ Deleting favorite reports
■ About generated reports layout and data
■ Running reports on demand
■ Generating reports automatically
■ Canceling scheduled reports
■ Emailing generated reports
■ Printing generated reports
■ Saving generated reports
■ About purging report data
■ Troubleshooting report generation
About working with reports

Symantec Brightmail Gateway reporting capabilities provide you with information about filtering activity at your site. You can analyze consolidated filtering performance for all Scanners and investigate the spam attacks and virus attacks that target your organization.

See “Report types” on page 359.

You can create the following reports:

One-time reports  Create reports to run one-time on an as-needed basis.
You can print, save, or email one-time the reports that you generate on demand.

Favorite reports  When you save reports to your Favorite Reports page, you can generate them on demand or schedule them to run automatically.
You can print, save, or email the favorite reports that you generate on demand. However, automatically generated reports can only be emailed.

See “Creating and configuring reports” on page 357.
See “Saving favorite reports” on page 370.
See “Running reports on demand” on page 377.
See “Generating reports automatically” on page 377.
See “Saving generated reports” on page 382.
See “Printing generated reports” on page 381.
See “Emailing generated reports” on page 379.

Symantec Brightmail Gateway tracks some of the data that is included in reports automatically. You must specify the additional data that you want Symantec Brightmail Gateway to track and maintain.

See “Report types” on page 359.
See “Selecting the data to track for reports” on page 357.

Symantec Brightmail Gateway contains a utility that runs periodically to purge old report data and Dashboard data. You can specify how often and when data is automatically purged.

See “About purging report data” on page 383.
Selecting the data to track for reports

Symantec Brightmail Gateway automatically tracks data that is used to create several predefined reports. However, some reports require that you specify the appropriate data to track for the report. For information about which reports require that you configure the product to track data and what data needs to be tracked to create that report, see “Report types” on page 359.

Note: Because the data storage requirements for some reports can be high, choose an appropriate length of time to store report data. In particular, the sender statistics usually consume a large amount of disk space.

See “Specifying how long report data is retained” on page 383.

See “About generated reports layout and data” on page 372.

To select the data to track for reports

1. In the Control Center, click Administration > Settings > Reports.
2. Under Email Reports Data, check the box beside the report data that you want to track.
   
   Extended statistics (such as Top Senders and Top Sender Domains) are only collected when the appropriate options are selected. To track extended statistics, ensure that all of the Sender-related check boxes are selected.

3. Click Save.

Creating and configuring reports

You can create and configure a report from the available report types. Then you can customize the report configuration to filter the data to include in the report. For example, you can specify time ranges and message flow direction. You must have at least full administration rights or rights to view or modify reports to create reports.

See “Report types” on page 359.

Before you create a report, ensure that you configure Symantec Brightmail Gateway to track the appropriate data for the report.

See “Selecting the data to track for reports” on page 357.

After you create the report, you can save it or run it.

See “Saving favorite reports” on page 370.

See “Running reports on demand” on page 377.
To create and configure reports

1. In the Control Center, click **Reports > View > Create a Report**.
2. In the Report type drop-down list, select a report category.
3. In a drop-down list beside Report type, select a specific report.
   This step does not apply to the Executive Summary report.
4. If applicable, for the reports that filter on specific elements, click the drop-down menu to select the criteria.
   For certain reports, you can filter by Sender name. You can use the null sender address <> to filter for messages that do not contain Sender names.
5. If applicable, in the Direction drop-down list, select the message directions to include in the report.
6. For IM reports, in the Network drop-down list, select the network.
7. In the Time range drop-down list, do one of the following:
   - Select a preset range.
     - Past Hour
     - Past 24 hours
     - Past 7 days
     - Past 30 days
   - Specify a custom time range.
     - Click **Customize**.
     - Click in the Start Date field, then click the pop-up calendar and select the start date.
     - Click in the End Date field, then click the pop-up calendar and select the end date.
     You must enable JavaScript in your browser to use the pop-up calendar.
8. In the Group By drop-down list, select one of the following:
   - Hour
   - Day
   - Week
Month

9 Select one or more of the following:

■ Graph
■ Table

See “About generated reports layout and data” on page 372.

10 For the reports that rank results, in the Top Entries box, type the maximum number for each time range that is specified in the Group by drop-down list.

11 Select the columns that you want to display in the report table.

This option is only available for certain reports.

Report types

Symantec Brightmail Gateway contains predefined report types. When you configure a report, you specify the report type that you want to use. The tables in this section show the report types that you can choose. The last column in each table lists the reporting data that you must instruct Symantec Brightmail Gateway to track before you can generate that report.

See “Selecting the data to track for reports” on page 357.

The categories of reports that you can generate are as follows:

■ Summary
   See Table 14-1 on page 360.

■ Content compliance
   See Table 14-2 on page 360.

■ Email message
   See Table 14-3 on page 362.

■ Instant messaging
   See Table 14-4 on page 364.

■ IP connection
   See Table 14-5 on page 365.

■ Spam
   See Table 14-6 on page 365.

■ Virus
   See Table 14-7 on page 368.

See “About generated reports layout and data” on page 372.

Table 14-1 describes the summary reports.
### Table 14-1  Summary reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive</td>
<td>Overview of your security profile, which includes total messages and threats processed, and virus and compliance summaries.</td>
<td>None</td>
</tr>
<tr>
<td>Compliance</td>
<td>Overview of the compliance violations and trends affecting your organization. Includes 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>Instant Messages</td>
<td>There is no Summary report for Instant Messages.</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</td>
<td>Overview of the email message spam.</td>
<td>None</td>
</tr>
<tr>
<td>Virus</td>
<td>Overview of the current viral threats to your organization. Includes a message summary, virus summary, suspect virus outcomes, and separate tables showing stats for known and potential viral threats.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 14-2 describes the available content compliance reports.

### Table 14-2  Compliance 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 compliance violations.</td>
<td>None</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most compliance matches have been detected. For each domain, the total messages processed and number and percentage of content-compliance policies triggered are listed.</td>
<td>Sender domains</td>
</tr>
</tbody>
</table>
Table 14-2  Compliance reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Senders</td>
<td>Email addresses from which the most compliance matches have been detected. For each email address, the total messages processed and number and percentage of content-compliance 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 compliance matches have been detected. For each HELO domain, the total messages processed and number and percentage of content-compliance 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 compliance matches have been detected. For each IP address, the total messages processed and number and percentage of content-compliance 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 compliance matches have been detected. For each recipient domain, the total messages processed and number and percentage of content-compliance 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 compliance matches have been detected. For each email address, the total messages processed and number and percentage of content-compliance 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 compliance policies triggered from a sender email address that you specify. For each grouping, the total messages processed and number and percentage of content-compliance policies triggered are listed.</td>
<td>Senders, Sender domains</td>
</tr>
</tbody>
</table>
Table 14-2  Compliance 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 compliance policies triggered for a recipient email address that you specify. For each grouping, the total messages processed and number and percentage of content-compliance policies triggered are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Top Policies</td>
<td>Names of the most common compliance matches, number of policies triggered, and percentage of policies triggered versus total processed messages. Optionally, you can limit the report to a particular compliance folder.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 14-3 describes the available email messages reports.

Table 14-3  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>Summary of total messages and messages that matched filters for spam, suspected spam, attacks, bad sender groups, good sender groups, viruses, suspicious attachments, worms, unscannable messages, malware (spyware/adware), encrypted attachments, and content compliance.</td>
<td>None</td>
</tr>
<tr>
<td>Average Message Size</td>
<td>The average size of messages in KB.</td>
<td>None</td>
</tr>
<tr>
<td>Total Message Size</td>
<td>Total size in KB of all messages in the report, and total size of each grouping.</td>
<td>None</td>
</tr>
<tr>
<td>Number of Messages</td>
<td>Number of all messages in the report, and number for each grouping.</td>
<td>None</td>
</tr>
<tr>
<td>Number of Recipients</td>
<td>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.</td>
<td>None</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 Domains</td>
<td>Domains from which the most messages have been processed. For each domain, the total processed and number of virus and spam messages 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 virus and spam messages 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 virus and spam 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 messages have been processed. For each IP address, the total processed and number of virus and spam 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 messages have been processed. For each recipient domain, the total processed and number of virus and spam 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 messages have been processed. For each email address, the total processed and number of virus and spam 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 messages that were processed for a sender email address that you specify. For each grouping, the total processed and number of virus and spam messages are listed.</td>
<td>Senders, Sender domains</td>
</tr>
</tbody>
</table>
Table 14-3  Email messages reports *(continued)*

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 virus and spam messages are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
</tbody>
</table>

Table 14-4 describes the available instant messages reports.

Table 14-4  Instant messages reports

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Total number of IM messages, messages sent, messages received, number and percentage of messages that were spim, number and percentage of messages blocked due to spim.</td>
<td>None</td>
</tr>
<tr>
<td>Top SPIM Senders</td>
<td>Screen names from which the most IM messages have been sent. For each screen name, the report lists the total IM messages sent, the number of spim messages sent, the number of spim messages blocked, and the percentages of each.</td>
<td>Senders</td>
</tr>
<tr>
<td>Top SPIM Recipients</td>
<td>Screen names for which the most IM messages have been received. For each screen name, the report lists the total IM messages received, the number of spim messages received, the number of spim messages blocked, and the percentages of each.</td>
<td>Recipients</td>
</tr>
<tr>
<td>File Transfers</td>
<td>The total number of files transferred, and number and percentage of files that contained a virus, were blocked, could not be scanned, had a scanner error, contained malware, or were encrypted.</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 14-5 describes the available IP connection-related reports.
### Table 14-5  
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>
</tbody>
</table>
| Connection Classification Summary | Summary of connections based on their connection class.  
See “About managing connection load at the gateway” on page 134. | Sender IP connections         |
| Top Accepted Connections    | IP addresses from which the most successful SMTP connections were detected.  | Sender IP connections         |
| Top Deferred Connections    | IP addresses from which the most failed SMTP connections were detected.      | Sender IP connections         |
| Top Rejected Connections    | IP addresses from which the most rejected SMTP connections were detected.    | Sender IP connections         |
| Top Virus Attacks           | IP addresses from which the most virus attacks have been detected. For each IP address, the total messages that were processed and number and percentage of virus attacks are listed. | Sender IP connections         |
| Top Directory Harvest Attacks | 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. | Sender IP connections         |

Table 14-6 describes the available spam reports.

### Table 14-6  
Available spam 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 messages (spam, bad senders, and suspected spam messages).</td>
<td>None</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 Domains</td>
<td>Domains from which the most spam messages have been detected. For each domain, the spam-to-total-processed percentage, total processed, and the number of spam, suspected spam, and bad sender 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 spam messages have been detected. For each email address, the spam-to-total-processed percentage, total processed, and the number of spam, suspected spam, and bad sender messages 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 spam messages have been detected. For each HELO domain, the spam-to-total-processed percentage, total processed, and the number of spam, suspected spam, and bad sender 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 spam messages have been detected. For each IP address, the spam-to-total-processed percentage, total processed, and the number of spam, suspected spam, and bad sender 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 spam messages have been detected. For each recipient domain, the spam-to-total-processed percentage, total processed, and the number of spam, suspected spam, and bad sender 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>Report</td>
<td>Description</td>
<td>Required data storage options</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Top Recipients</td>
<td>Email addresses for which the most spam messages have been detected. For each email address, the spam-to-total-processed percentage, total processed, and the number of spam, suspected spam, and bad sender 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 spam messages 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 spam, suspected spam, and bad sender messages are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of spam messages 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 spam, suspected spam, and bad sender messages are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
<tr>
<td>Sender Authentication Overview</td>
<td>Total 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>
</tbody>
</table>
### Table 14-6  
Available spam reports (continued)

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
<th>Required data storage options</th>
</tr>
</thead>
<tbody>
<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 14-7 describes the available virus reports.

### Table 14-7  
Available virus 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 viruses detected.</td>
<td>None</td>
</tr>
<tr>
<td>Top Sender Domains</td>
<td>Domains from which the most virus messages have been detected. For each domain, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and 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 virus messages have been detected. For each email address, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and 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>
<tr>
<td>Top Sender HELO Domains</td>
<td>SMTP HELO domain names from which the most virus messages have been detected. For each HELO domain, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and 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>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 virus messages have been detected. For each IP address, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and 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 virus messages have been detected. For each recipient domain, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and 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 virus messages have been detected. For each email address, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and 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>Top Virus and Worms</td>
<td>Names of the most common viruses detected. For each grouping, the virus-to-total-processed percentage, virus to total virus and worm percentage, and last occurrence of the virus are listed.</td>
<td>None</td>
</tr>
<tr>
<td>Specific Senders</td>
<td>Number of virus messages that were detected from a sender email address that you specify. For each grouping, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and unscannable messages are listed.</td>
<td>Senders, Sender domains</td>
</tr>
<tr>
<td>Specific Recipients</td>
<td>Number of virus messages that were detected for a recipient email address that you specify. For each grouping, the virus-to-total-processed percentage, total processed, and the number of viruses, worms, and unscannable messages are listed.</td>
<td>Recipients, Recipient domains</td>
</tr>
</tbody>
</table>
Saving favorite reports

When you create a report, you can specify a name for the report and save it on your Favorite Reports page in the Control Center. You can run saved reports on demand. You can also schedule generating the report automatically.

You must have at least full administration rights or rights to view or modify reports to save reports.

See “Generating reports automatically” on page 377.

See “Deleting favorite reports” on page 372.

You must create and configure a report before you can save it.

See “Creating and configuring reports” on page 357.

To save a favorite report

1. On the Report Filter page, under Report Options, in the Report name box, type the name of the favorite report.
2. Click Save to Favorites.

Editing a favorite report's filter options

You may want to modify a favorite report to expand or condense the information that it provides. You can modify the schedule in which reports are automatically generated and the report's filter options.

You must have full administration rights or rights to view or modify reports to edit reports.

See “Editing a favorite report's schedule” on page 371.

See “Creating and configuring reports” on page 357.

To edit a favorite report's filter options

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.
Editing a favorite report's schedule

You may want to modify a favorite report's schedule to expand or condense the information that it provides. You must have full administration rights or rights to view or modify reports to edit reports.

See “Editing a favorite report's filter options” on page 370.

To edit a favorite report's schedule
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.

Copying favorite reports

You may have instances in which you create a favorite report and want to create a similar report with only a few variances. Symantec Brightmail Gateway lets you copy favorite reports.

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.

See “Saving favorite reports” on page 370.

You must have full administration rights or rights to view or modify reports to copy favorite reports.

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.
Deleting favorite reports

You can delete the favorite reports that you no longer need. However, when you delete a report, the report configuration cannot be retrieved.

You must have full administration rights or rights to view or modify reports to delete a favorite report.

See “Editing a favorite report's filter options” on page 370.

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.

About 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.

See “Report types” on page 359.

Table 14-8 provides information about how reports are displayed.
Table 14-8  Report layout

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Graphs and tables        | 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:  
  ■ Graph—overview  
    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.  
  ■ 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.  
  ■ Table  
    Creates numeric a representation of the report data.  
    For all reports, a table report can list more than 20 items.  

The method to save graphs and tables to files depends on the report, its format, and whether you save or email the report.  
See “Saving generated reports” on page 382.  
See “Emailing generated reports” on page 379.  

| Number of rows           | 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).  
  **Note:** This limitation is not configurable.  

### Table 14-8  Report layout (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Extra bars in report graphs   | 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:  
  ■ You run a report for the past hour at 2:22 P.M. Tuesday:  
    ■ The resulting data set is from 1:00 P.M. until 2:22 P.M.  
    ■ The data appears by hour, spread across two bars.  
  ■ You run a report for the past 24 hours at 2:22 P.M. Tuesday:  
    ■ The resulting data is from 2:00 P.M. Monday until 2:22 P.M. Tuesday.  
    ■ The data appears by hour, spread across 25 bars. |
| Time ranges                   | 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 P.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. |

Table 14-9 provides the information to help you interpret the information in reports.

### Table 14-9  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, viruses, and compliance policy violations. Similar message verdicts are grouped into threat categories. Table 15-3 lists the verdicts in each category.</td>
</tr>
</tbody>
</table>
### Table 14-9  Report data details *(continued)*

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 a virus is a multiple threat message. Clean messages contain no known threats.</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 viruses 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 quarantined suspect viruses were deleted, determined to be viruses or not, or are still in the Suspect Virus Quarantine.</td>
</tr>
</tbody>
</table>
| Sender HELO domain or IP connection shows gateway information | If any Scanners accept relayed messages from a gateway computer, the SMTP HELO name or IP connection address is the name or connection of the gateway computer. Affected reports are as follows:  
   - Top Sender HELO Domains  
     All Top Sender HELO Domain reports are affected  
   - Top Sender IP Connections  
     All Top Sender IP Connections reports are affected  
   - Top Succeeded Connections SMTP report  
   - Top Failed Connections SMTP report  
   - Top Rejected Connections SMTP report  
| 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. |
### Table 14-9: Report data details (continued)

<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 groups. For example, recipients in group A may have content compliance 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 virus count increases by two. The message is considered a multiple threat message. The following verdicts have unique names:  ■ Content compliance 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 virus threat count for the message is one (encrypted content counts as a virus 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 391.</td>
</tr>
<tr>
<td>IM message count</td>
<td>IM messages between users within your site are counted twice in the reports. See “Creating and configuring reports” on page 357.</td>
</tr>
</tbody>
</table>
Running reports on demand

You can run reports as needed. You can run the on-demand reports that you create and the reports that are saved on your Favorite Reports page. You can even run scheduled reports whenever you want.

After you run the report, if there is data available, the report appears in a new browser window. Based on how much data is available for that report, this process may take several minutes.

You must have full administration rights or rights to view or modify reports to run reports.

See “Troubleshooting report generation” on page 385.

To run reports on demand
1. Create a report.
   See “Creating and configuring reports” on page 357.
2. Click Run.
3. If a "Pop-up blocked" message appears in the Control Center, click the message and permit pop-ups from Symantec Brightmail Gateway Control Center.
   The report appears in a separate browser window.

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.
4. If a "Pop-up blocked" message appears in the Control Center, click the message and permit pop-ups from Symantec Brightmail Gateway Control Center.
   The report appears in a separate browser window.

Generating reports 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. Recipients of the email report can manually save the report on their local computer.

See “Saving generated reports” on page 382.
See “Printing generated reports” on page 381.
You must have full administration rights or rights to view or modify reports to create automatically generated reports.

**To generate reports 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.**
3. On the Schedule tab under Report Schedule, in the Generate report at drop-down lists, set the time of day to generate the report.
4. Specify when you want the report to be generated as follows:

   **Daily**
   - Click **Daily** and specify whether you want the report every day or only weekdays.

   **Weekly**
   - Click **Weekly** and check the boxes for the days of the week that you want to generate the report.
   - You can select multiple days.

   **Monthly**
   - Click **Monthly** and specify whether you want the report to be created on the same day of each month or the last day of every month.
   - If you specify 29, 30, or 31 in the Day of every month box, and a month does not have one of those days, the report is not sent. Instead, click **Last day of every month** to avoid this problem.

5. Click the **Export** tab.
6. Under Report Format, select one of the following to specify the format:
   - HTML
   - PDF
   - CSV (this file format is not available for the Executive Summary report)
     - In the CSV Delimiter drop-down list, select a delimiter.
     - In the File Encoding drop-down list, select an encoding for the CSV file.
7. Under Report Sender and Destination Addresses, in the Send from the following email address box, type the email address.
   
   For example, r1b3s@symantecexample.com.
   
   Separate multiple email addresses with a space, comma, or semi-colon.
8 In the Send to the following email addresses box, type at least one email address.
For example, r1b3s@symantecexample.com.
Separate multiple email addresses with a space, comma, or semi-colon.
9 In the Character Set drop-down list, select a character set appropriate for the recipient of the email message.
10 Click **Save**.

**Canceling scheduled reports**

You can cancel a scheduled report from being automatically generated without deleting the report. You can still manually generate the report at any time or modify the report later to set up a new schedule.

You must have full administration rights or rights to view or modify reports to cancel automatically generated reports.

See “Generating reports automatically” on page 377.

To **cancel scheduled reports**

1 In the Control Center, click **Reports > View > Favorite Reports**.
2 Check the box beside the report that you no longer want scheduled, and then click **Clear Schedule**.

**Emailing generated reports**

You can email the reports that you generate on demand to one or more recipients. Reports that you generate on demand are attached to an email message in a compressed file. The compressed file contains an HTML file and graphic files. When recipients open the HTML file, the report appears as it did in the Web browser when you generated it.

See “Running reports on demand” on page 377.

Scheduled reports must be emailed to at least one recipient, and you must specify the recipient when you create the scheduled report. For more information about how to create scheduled reports, see “Generating reports automatically” on page 377.

Ensure that you have configured from whom the email report is sent. You can also customize the subject line.

See “Specifying the report email notification sender and subject line” on page 380.
You must create and run a report before you can email it. You must have full administration rights or rights to view or modify reports to create and email reports.

See “Creating and configuring reports” on page 357.

See “Running reports on demand” on page 377.

To email generated reports

1. In the browser window in the box next to Email, type the address of the person to whom you want the report emailed.
   For example, r1b3s@symantecexample.com.
   Separate multiple email addresses with a comma, semi-colon, or space.

2. Select an appropriate encoding for the message from the Character Set drop-down list.
   The following options are available:
   ■ Western European (ISO-8859-1)
   ■ Unicode (UTF-8)
   ■ Simplified Chinese (GB2312 or GB18030)
   ■ Traditional Chinese (Big5)
   ■ Korean (KS_C_5601-1987)

3. Click Email.

Specifying the report email notification sender and subject line

Symantec Brightmail Gateway can email reports to the recipients that you specify. However, you must specify from whom the email notification is sent. You can also customize the subject line of the email notice. The email address that you specify must be a valid email address for your domain.

When you install the product, the default email address is ReportAdmin@yourcompany.com. If you do not change the default email address and users reply to the notification email, the reply message is undeliverable.

See “Emailing generated reports” on page 379.

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% (\{MMM d, yyyy hh:mm a\} to \{MMM d, yyyy hh:mm a\})

For example:


Report by week or month

%TITLE% (\{MMM d, yyyy\} to \{MMM d, yyyy\})

For example:

MonthlyReport (December 1, 2008 to January 1, 2009 PST)

For more information about Java SimpleDateFormat, see
http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html

You must have full administration rights or rights to view or modify reports to
modify report settings.

To specify the report email notification sender and subject line

1 In the Control Center, click Administration > Settings > Reports.

2 Under Report Export Settings, 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, if needed.

5 Click Save.

Printing generated reports

When you generate a report, if there is data available, the report appears in a new
browser window. You can print the report from your browser. You must have full
administration rights or rights to view reports.

You must generate a report before you can print it.

See “Creating and configuring reports” on page 357.

See “Running reports on demand” on page 377.
To print generated reports
1. In the Report browser window, click **Print**.
2. Choose the appropriate options in your print dialog box to print the report.

**Saving generated reports**

When you generate a report, if there is data available, the report appears in a new browser window. You can save the report from your browser.

Table 14-10 lists the report file formats that you can use.

**Table 14-10 Report file formats**

<table>
<thead>
<tr>
<th>Report file format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>Save the report as a compressed file that contains an HTML file and graphic files. When you unzip the file and open it in a Web browser, the HTML file appears as it appeared originally, with the graphics inline.</td>
</tr>
<tr>
<td>CSV</td>
<td>You can save the report as a .csv text file with comma, semicolon, or tab-delimited data. After you save the report as a .csv file, you can import it into a spreadsheet. The report is saved as a delimited text file no matter which Table box or Graph box is checked. 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 and save the CSV file as Unicode. This file format is not available for the Executive Summary report.</td>
</tr>
<tr>
<td>PDF</td>
<td>You can save the report as an Adobe Acrobat .pdf file. The PDF file looks similar to the HTML version of the file, though the sections are broken into pages. You can view the saved PDF file in a PDF reader such as Adobe Acrobat Reader.</td>
</tr>
</tbody>
</table>

You must generate a report before you can save it.

See “Running reports on demand” on page 377.
To save generated reports

1. On the browser window, select the report file format that you want to use.
   
   See Table 14-10 on page 382.

   Before you click Save as CSV, click the **Delimiter** drop-down list. Delimiters include the comma, semicolon, or tab character.

2. Choose the appropriate options in your browser dialog box to save the report.

**About purging report data**

Symantec Brightmail Gateway contains a utility (Expunger) that purges old report data and Dashboard data. You can configure the amount of time report data is kept before it is purged, the frequency data is purged, and the Expunger start time.

Symantec Brightmail Gateway performs better when you configure it to store less report data. Try to balance your reporting needs against the performance of Symantec Brightmail Gateway. You can accomplish this balance by adjusting the retention period and the types of report data to store.

See “Specifying how long report data is retained” on page 383.

See “Specifying when and how often report data is purged” on page 384.

**Specifying how long report data is retained**

By default, report and Dashboard data is retained for seven days. If Symantec Brightmail Gateway already has seven days of data, the oldest hour of data is deleted as each new hour of data is stored. Based on your organization's size and message volume, the disk storage requirements for report data can become quite large. You can modify how long Symantec Brightmail Gateway maintains report data.

You must have full administration rights or rights to view or modify reports to modify report settings.

See “Deleting all report data at one time” on page 384.

See “About purging report data” on page 383.

See “Specifying when and how often report data is purged” on page 384.
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 Symantec Brightmail Gateway keeps your report data.
3. Click **Save**.

### Specifying when and how often report data is purged

You can specify when the Expunger utility begins the purge process and how frequently the purge process occurs. The Expunger lets you keep the report data that is maintained at a manageable size. Because it is resource intensive, you may want to configure the Expunger to run at off hours. Report data that is purged cannot be retrieved.

You must have full administration rights or rights to view or modify reports to modify report settings.

See “About purging report data” on page 383.

See “Deleting all report data at one time” on page 384.

See “Specifying how long report data is retained” on page 383.

### 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 start time.
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**.

### Deleting all report data at one time

Based on your organization's size and message volume, the disk storage requirements for reports data can become quite large. You can delete all of the report data that Symantec Brightmail Gateway has retained at one time. Once the data is deleted, it cannot be retrieved. If you are unsure about deleting all of the report data, you can delete data based on a specified time range.

See “Specifying how long report data is retained” on page 383.
See “About purging report data” on page 383.
You must have full administration rights or rights to view or modify reports to modify report settings.

**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*.

### Troubleshooting report generation

Table 14-11 lists issues you might encounter when you generate reports.

**Table 14-11 Report generation issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>No data available for the report type specified</td>
<td>Instead of displaying the expected reports, Symantec Brightmail Gateway might display the following message:</td>
</tr>
<tr>
<td></td>
<td><em>No data is available for the report type and time range specified.</em></td>
</tr>
<tr>
<td></td>
<td>If you receive this message, verify the following:</td>
</tr>
<tr>
<td></td>
<td>■ Data exists for the filter you specified.</td>
</tr>
<tr>
<td></td>
<td>For example, perhaps you specified a recipient address that received no mail during the specified period for a Specific Recipients report.</td>
</tr>
<tr>
<td></td>
<td>■ Symantec Brightmail Gateway is configured to keep data for that report type.</td>
</tr>
<tr>
<td></td>
<td>Some reports require that you enable report data before those reports can be run.</td>
</tr>
<tr>
<td></td>
<td>See “Selecting the data to track for reports” on page 357.</td>
</tr>
<tr>
<td></td>
<td>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 &quot;Delete data older than&quot; setting on the Report Settings page controls this retention period.</td>
</tr>
</tbody>
</table>
Table 14-11  Report generation issues (continued)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrepancies in Suspect Virus Outcomes</td>
<td>The graph part of the Virus 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.</td>
</tr>
<tr>
<td></td>
<td>The reasons for this difference include the following:</td>
</tr>
<tr>
<td></td>
<td>- The suspect virus outcomes are counted for 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.”</td>
</tr>
<tr>
<td></td>
<td>- 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, if a message contains a virus and a suspect virus and the matching virus policy is &quot;Delete message&quot; and the matching suspect virus policy is &quot;Hold message in Suspect Virus Quarantine,&quot; the message is deleted. The message is deleted because deletion takes precedence over &quot;Hold message in Suspect Virus Quarantine.&quot;</td>
</tr>
<tr>
<td>Data in Compliance Summary report can look inconsistent</td>
<td>By default, the bottom of the Compliance Summary report contains a table of the top compliance policies 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>

See “About working with reports” on page 356.
This chapter includes the following topics:

- About monitoring the status of your product
- About the Dashboard
- Viewing the status of your hardware
- Viewing information about your hardware
- Viewing the status of software and services
- About LDAP synchronization and Control Center replication
- About logs
- About message audit logging
- About message queues
- Viewing IM users that are signed on
- Viewing the connection status of your IM networks

About monitoring the status of your product

You can monitor the status of Symantec Brightmail 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 15-1 describes the items that you can monitor.
### Table 15-1  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 timeframes.  
|          |     See “About the Dashboard” on page 389.  
|          |     See “Viewing the Dashboard” on page 390.  
|          |  ■ 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 393.  
|          |     See “Viewing the status of software and services” on page 394.  
|          |     See “Viewing the status of your hardware” on page 392.  
|          |     See “Monitoring message queue size and volume” on page 428.  
|          |  ■ LDAP Synchronization  
|          |     You can monitor LDAP synchronization and Control Center replication statuses and perform manual synchronizations and replications.  
|          |     See “About LDAP synchronization and Control Center replication” on page 395.  
|          |  ■ Logs  
|          |     Symantec Brightmail Gateway logs information about the Control Center, Spam Quarantine, and each Scanner (local and remote). You can view these logs to monitor the status of your product and troubleshoot issues.  
|          |     See “About logs” on page 403.  
| SMTP     | You can monitor the following SMTP statuses:  |
|          |  ■ Message audit logs  
|          |     Symantec Brightmail 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.  
|          |     See “About message audit logging” on page 418.  
|          |  ■ 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 424.  |
Table 15-1 Status items that you can monitor (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant messaging</td>
<td>You can monitor the following instant message statuses:</td>
</tr>
<tr>
<td></td>
<td>■ Active users</td>
</tr>
<tr>
<td></td>
<td>You can view all of the registered and unregistered IM users that are currently signed on.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing IM users that are signed on” on page 429.</td>
</tr>
<tr>
<td></td>
<td>■ Network status</td>
</tr>
<tr>
<td></td>
<td>You can view the connection status of each IM network that you support from each Scanner that is in your corporate network.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing the connection status of your IM networks” on page 432.</td>
</tr>
</tbody>
</table>

About the Dashboard

Table 15-2 describes the information that appears on the Dashboard.

Table 15-2 Dashboard contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages graph</td>
<td>Shows the single threats, multiple threats, and clean messages in proportion to the total message volume for the specified timeframe.</td>
</tr>
<tr>
<td>Messages table</td>
<td>Lists the individual counts for single threat, multiple threat, and clean messages. Also lists each type's percentage of total message volume for the specified timeframe.</td>
</tr>
<tr>
<td>Threats graph</td>
<td>Shows all known threats for a specified timeframe.</td>
</tr>
<tr>
<td>Threats table</td>
<td>Lists the individual counts for common message verdicts as well as each type's percentage of total message volume for the specified timeframe.</td>
</tr>
<tr>
<td></td>
<td>See “Threat category components” on page 391.</td>
</tr>
<tr>
<td>Top 5 Named Viruses</td>
<td>Lists the most prevalent viruses and worms for the specified timeframe, ranked by the number of times they were detected. The Details link takes you to the Virus Summary.</td>
</tr>
<tr>
<td>Top 5 Compliance Policies</td>
<td>Lists the most prevalent types of Compliance Policy violations for the specified timeframe, ranked by the number of times they were detected. The Details link takes you to the Compliance Summary.</td>
</tr>
</tbody>
</table>
Table 15-2  Dashboard contents *(continued)*

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Status</td>
<td>This pane displays the following information:</td>
</tr>
<tr>
<td>■ System</td>
<td>Status of the hardware components and software components in your system.</td>
</tr>
<tr>
<td></td>
<td>If available, the link that is adjacent the component provides a more detailed status.</td>
</tr>
<tr>
<td>■ Definitions</td>
<td>Status of spam, spim, and virus definitions available through LiveUpdate.</td>
</tr>
<tr>
<td></td>
<td>If available, the date that is adjacent to the Virus definitions field links to the LiveUpdate Settings page.</td>
</tr>
<tr>
<td></td>
<td>If IM is not enabled, &quot;IM filtering not enabled&quot; appears as a link that is adjacent to the Spim definitions field.</td>
</tr>
<tr>
<td></td>
<td>This link provides information about how to enable IM and configure IM-related policies.</td>
</tr>
<tr>
<td>■ Licenses</td>
<td>Status of the licenses you purchased from Symantec.</td>
</tr>
<tr>
<td><strong>Note:</strong> The Definitions column and License column show the oldest definition or license across all Scanners that are licensed for that feature.</td>
<td></td>
</tr>
</tbody>
</table>

Symantec ThreatCon level | To the left of the Dashboard is Symantec ThreatCon. This rating is a measurement of the global threat exposure that is delivered as part of Symantec DeepSight Threat Management System. |

See “Viewing the Dashboard” on page 390.

**Viewing the Dashboard**

The Dashboard provides a dynamic view of your appliance's status and filtering activity for various timeframes. Color-coded graphs show the total volume of processed email and detected threats, sub-divided by message category and verdict, respectively. Accompanying tables present the same data numerically. You can tailor the display to show data according to the direction of email through your system: inbound mail, outbound mail, or both. You can also drill down to more detailed data on viral threats and compliance policy violations.
**Note:** Some statistics are relevant only to one direction of the mail stream. For example, the Invalid recipients verdict applies only to inbound mail.

You must have Full Administration rights or Manage Status and Log view or modify rights to view the Dashboard.

See “About the Dashboard” on page 389.

**To view the Dashboard**

1. Do one of the following actions:
   - Log onto Symantec Brightmail Gateway. When you log onto the product, the Dashboard is the first page that appears.
   - In the Control Center, click **Status > System > Dashboard**.

2. Select an email message processing direction from the drop-down list: inbound, outbound, or both.

3. Select a timeframe from the adjacent drop-down list. When the screen refreshes, the specified timeframe appears in the top-right corner.

**Threat category components**

The Dashboard contains data for several threat categories.

Table 15-3 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>Compliance</td>
<td>■ 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>
</tbody>
</table>

Content compliance policies count as threats if “Track violations of this policy in the dashboard and reports” is checked.
### Table 15-3 Threat category components (continued)

<table>
<thead>
<tr>
<th>Threat category</th>
<th>Verdicts that make up the threat category</th>
</tr>
</thead>
</table>
| Virus                    | Virus threat category components are as follows:  
  ■ Viruses  
  ■ Worms  
  ■ Malware  
  Potential Virus threat category components are as follows:  
  ■ Suspect Virus  
  ■ Unscannable Attachments  
  ■ Encrypted Attachment |
| Invalid recipients       | Invalid recipients                       |
| Bad reputation           | Bad reputation threat category components are as follows:  
  ■ Directory Harvest Attacks  
  ■ Virus Attacks  
  ■ Bad IPs  
  ■ Connection Class  
  ■ Symantec Global Bad Senders  
  Good reputation threat category components are as follows:  
  ■ Symantec Global Good Senders  
  ■ Good IPs  
  ■ Fastpass |
| Spam                     | Sender authentication failure  
  ■ Spam  
  ■ Suspected spam  
  ■ Bounce attack |

See “About the Dashboard” on page 389.

See “Viewing the Dashboard” on page 390.

### 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.

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 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.

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 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. Available details vary depending on how each appliance is configured: as a Control Center, a Scanner, or both.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view information about your software and services.

The information that appears is as follows:

<table>
<thead>
<tr>
<th>Scanners</th>
<th>The status information is as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Scanner</td>
</tr>
<tr>
<td></td>
<td>The name that you assigned to the Scanner</td>
</tr>
<tr>
<td></td>
<td>■ Version</td>
</tr>
<tr>
<td></td>
<td>The version number of the software that you are running on the Scanner</td>
</tr>
<tr>
<td></td>
<td>■ Virus Definitions</td>
</tr>
<tr>
<td></td>
<td>The date of the virus definitions that Symantec Brightmail Gateway uses to scan messages</td>
</tr>
<tr>
<td></td>
<td>■ Scanner</td>
</tr>
<tr>
<td></td>
<td>Whether the Scanner is enabled or disabled</td>
</tr>
<tr>
<td></td>
<td>■ Agent</td>
</tr>
<tr>
<td></td>
<td>Whether the Agent is enabled or disabled</td>
</tr>
<tr>
<td></td>
<td>■ Conduit</td>
</tr>
<tr>
<td></td>
<td>Whether the Conduit service is running</td>
</tr>
<tr>
<td></td>
<td>■ LiveUpdate</td>
</tr>
<tr>
<td></td>
<td>Whether the LiveUpdate service is running</td>
</tr>
<tr>
<td></td>
<td>■ Brightmail Engine</td>
</tr>
<tr>
<td></td>
<td>Whether the Brightmail Engine service is running</td>
</tr>
<tr>
<td></td>
<td>■ MTA</td>
</tr>
<tr>
<td></td>
<td>Whether the MTA service is running</td>
</tr>
<tr>
<td></td>
<td>■ IM Relay</td>
</tr>
<tr>
<td></td>
<td>Whether the IM relay service is running</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Center</th>
<th>The status information is as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Version</td>
</tr>
<tr>
<td></td>
<td>The version number of the software that you are running on the Control Center</td>
</tr>
<tr>
<td></td>
<td>■ Spam Quarantine</td>
</tr>
<tr>
<td></td>
<td>Whether the Spam Quarantine is running</td>
</tr>
<tr>
<td></td>
<td>■ LDAP Synchronization</td>
</tr>
<tr>
<td></td>
<td>Whether the most recent LDAP Synchronization was successful</td>
</tr>
</tbody>
</table>
If you want to make any modifications, you can do the following from the same page that you view the status:

- Modify a Scanner.
  
  See “Modifying Scanners” on page 126.

- Enable or disable a service.
  
  See “Working with Services” on page 107.

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. 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.

To modify a Scanner

- On the Software and Services tab, click any linked word to modify a Scanner.

  The Edit Host Configuration page appears.

To enable or disable a service

1. On the Software and Services tab, click on a host.
2. On the Services page, click the linked word that follows Status next to the component.

   The linked word is either Running or Stopped. The Services tab of the Edit Host Configuration page appears.
3. On the Edit Host Configuration page on the Services tab, check the service that you want to enable or disable, and click Start or Stop.

About LDAP synchronization and Control Center replication

When you install and configure Symantec Brightmail Gateway, you configure an LDAP synchronization and Control Center replication schedule. These processes run automatically at the schedule that you specify.

See “About LDAP synchronization” on page 481.

However, you may have an occasion when you want to perform a manual synchronization and replication. For instance, assume that you schedule synchronization and replication to occur daily at 2:00 A.M. Assume that your organization has hired several new employees. You might want to perform a
one-time synchronization and replication rather than wait until the regularly scheduled synchronization and replication process. After you perform the on-demand synchronization and replication, your new employees can immediately receive emails. You can create or modify policies to include the new employees immediately rather than waiting until after the regularly scheduled process runs. You can also update user, alias, group, and distribution list data rather than waiting until after the regularly scheduled process runs.

You must have Full Administration rights or Manage Status and Logs modify rights to synchronize LDAP and replicate the Control Center data to your Scanners. Perform the LDAP synchronization before you perform the Control Center replication.

See “Synchronizing LDAP servers manually” on page 398.

See “Replicating the Control Center database manually” on page 402.

### Viewing LDAP synchronization status

Symantec Brightmail Gateway generates synchronization status information for each LDAP server. The information that appears consists of either the synchronization process that is occurring or the most recent synchronization process that completed.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view the LDAP synchronization status.

See “Synchronizing LDAP servers manually” on page 398.

See “Synchronization status information” on page 396.

To refresh the status view, perform the steps to view LDAP synchronization status again.

**To view LDAP synchronization status**

1. In the Control Center, click **Status > System > LDAP Synchronization**.
2. Click the **LDAP to CC** tab.

### Synchronization status information

Symantec Brightmail Gateway generates synchronization status information for each LDAP server. The information that appears consists of either the synchronization process that is occurring or the most recent synchronization process that completed.

Table 15-4 describes the information that appears for the synchronization status.
Table 15-4  LDAP synchronization

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Servers</td>
<td>List of the LDAP sources that are configured for synchronization with the Control Center.</td>
</tr>
<tr>
<td>Status</td>
<td>Information about synchronization activity.</td>
</tr>
<tr>
<td></td>
<td>The Status can indicate any of the following states:</td>
</tr>
<tr>
<td></td>
<td>■ Idle</td>
</tr>
<tr>
<td></td>
<td>Nothing is happening.</td>
</tr>
<tr>
<td></td>
<td>■ Starting</td>
</tr>
<tr>
<td></td>
<td>LDAP synchronization is about to start.</td>
</tr>
<tr>
<td></td>
<td>This status lasts about a minute.</td>
</tr>
<tr>
<td></td>
<td>■ Canceled</td>
</tr>
<tr>
<td></td>
<td>LDAP synchronization has been canceled.</td>
</tr>
<tr>
<td></td>
<td>This status can also occur if a scheduled LDAP synchronization interrupts a replication in progress or a scheduled replication interrupts an LDAP synchronization in progress.</td>
</tr>
<tr>
<td></td>
<td>■ In Progress</td>
</tr>
<tr>
<td></td>
<td>The server has acknowledged the synchronization and the process is under way.</td>
</tr>
<tr>
<td></td>
<td>■ Success</td>
</tr>
<tr>
<td></td>
<td>Synchronization has completed successfully.</td>
</tr>
<tr>
<td></td>
<td>■ Failed</td>
</tr>
<tr>
<td></td>
<td>The synchronization has failed.</td>
</tr>
<tr>
<td></td>
<td>Consult your logs to identify possible causes.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing log files” on page 406.</td>
</tr>
<tr>
<td></td>
<td>■ Complete</td>
</tr>
<tr>
<td></td>
<td>The synchronization completed successfully.</td>
</tr>
<tr>
<td>Started</td>
<td>The time at which the most recent synchronization began.</td>
</tr>
<tr>
<td>Ended</td>
<td>The time at which the most recent synchronization finished.</td>
</tr>
<tr>
<td>Read</td>
<td>The number of directory entries read from the synchronization server.</td>
</tr>
<tr>
<td></td>
<td>For a full synchronization, this number is equal to the total number of records from the LDAP source.</td>
</tr>
<tr>
<td>Added</td>
<td>The number of directory entries that are added from the synchronization server to the Control Center.</td>
</tr>
<tr>
<td>Modified</td>
<td>The number of records that are modified in the Control Center based on synchronization server information.</td>
</tr>
</tbody>
</table>
Table 15-4  LDAP synchronization (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleted</td>
<td>The number of entries that are deleted from the Control Center based on synchronization server information.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The number of directory entries from the LDAP source that the synchronization server rejects.</td>
</tr>
</tbody>
</table>

See “Viewing LDAP synchronization status” on page 396.
See “Synchronizing LDAP servers manually” on page 398.
See “Troubleshooting LDAP synchronization rejection entries” on page 400.

Synchronizing LDAP servers manually

You can configure Symantec Brightmail Gateway to synchronize your LDAP servers with the Control Center database according to the schedule that you specify. However, you can perform a manual synchronization as needed. You must have Full Administration rights or Manage Status and Logs modify rights to perform a manual synchronization.

See “About LDAP synchronization and Control Center replication” on page 395.

You can perform the following types of synchronization:

- **Synchronize Changes**
  Select this option to synchronize modifications of LDAP data from the selected LDAP source with the Control Center.
  Use this option if there are fewer than approximately 1,000 entries to update.

- **Full Synchronization**
  Select this option to synchronize all data entries from the selected LDAP source with the Control Center.
  Use this option if there are approximately 1,000 or more entries to update. When a full synchronization is performed, all LDAP source records are erased from the Control Center and replaced with new LDAP source records.
  *Note:* Full synchronization between an LDAP source and the Control Center can take up to several hours to perform. The amount of time depends on the number of records that need to be synchronized.

If you initiate a manual replication and want to stop it, you can cancel it.

See “Canceling an LDAP synchronization in progress” on page 399.
Perform a manual synchronization before a manual replication or scheduled replication. If a replication begins while synchronization is occurring, the synchronization process stops.

See “Replication status information” on page 401.

See “Canceling a Control Center replication in progress” on page 402.

**To synchronize LDAP servers manually**

1. In the Control Center, click **Status > System > LDAP Synchronization**.
2. Click the **LDAP to CC** tab.
3. Check the box that is beside the LDAP source with which you want the Control Center to synchronize directory data.
4. Click the option for the type of synchronization that you want to perform as follows:
   - Synchronize Changes
   - Full Synchronization
5. In the navigation pane under System, click **LDAP Synchronization** again to refresh the page to view the status of a synchronization in progress.

See “Synchronization status information” on page 396.

**Canceling an LDAP synchronization in progress**

You can cancel a manual LDAP synchronization or scheduled LDAP synchronization at any time. If you cancel a synchronization, you cannot reinitialize it at a later time. You can either perform a manual synchronization or wait until the next scheduled synchronization.

You must have Full Administration rights or Manage Status and Logs modify rights to cancel an LDAP synchronization.

See “Synchronizing LDAP servers manually” on page 398.

**To cancel an LDAP synchronization in progress**

1. In the Control Center, click **Status > System > LDAP Synchronization**.
2. Click the **LDAP to CC** tab.
3. Check the box beside the LDAP source that is synchronizing and that that you want to cancel.
4. Click **Cancel Synchronization**.
Troubleshooting LDAP synchronization rejection entries

If you continually see the same number of rejected entries for an LDAP source, use the log to troubleshoot the issue.

To troubleshoot LDAP synchronization rejection entries

1. Modify the LDAP server synchronization audit level to Low or Verbose.
   See “About LDAP synchronization” on page 481.
2. Manually initiate an LDAP synchronization.
   See “Synchronizing LDAP servers manually” on page 398.
3. Once synchronization is complete, in the Control Center, click Status > System > Logs.
4. Under Filter, in the Components drop-down list, click Control Center.
5. In the Log type drop-down list, click LDAP Logs.
6. Click Display.
7. Examine the information to determine why the entries are repeatedly rejected.
   Pay particular attention to the file error.log.X, where X is a number, and the newly created log files that end in rejects_forward.xml.

Viewing Control Center replication status

Symantec Brightmail Gateway generates replication status information for each Scanner. The information that appears consists of either the replication process that is occurring or the most recent replication process that was completed.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view the Control Center replication status.

See “Replicating the Control Center database manually” on page 402.
See “Replication status information” on page 401.
To refresh the status view, perform the steps to view Control Center replication status again.

To view Control Center replication status

1. In the Control Center, click Status > System > LDAP Synchronization.
2. Click the CC to Scanners tab.
Replication status information

Symantec Brightmail Gateway generates replication status information for each Scanner. The information that appears consists of either the replication process that is occurring or the most recent replication process that was completed.

Table 15-5 describes the information that appears for the replication status.

Table 15-5  Control Center replication status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanners</td>
<td>List of attached Scanners that are enabled for replication.</td>
</tr>
<tr>
<td>Status</td>
<td>The status can indicate any of the following states:</td>
</tr>
<tr>
<td></td>
<td>- Idle</td>
</tr>
<tr>
<td></td>
<td>Nothing is happening.</td>
</tr>
<tr>
<td></td>
<td>- Started</td>
</tr>
<tr>
<td></td>
<td>A replication request has been issued.</td>
</tr>
<tr>
<td></td>
<td>- Canceled</td>
</tr>
<tr>
<td></td>
<td>Either replication was canceled manually or an LDAP synchronization was</td>
</tr>
<tr>
<td></td>
<td>in progress when a scheduled replication or manual replication was</td>
</tr>
<tr>
<td></td>
<td>initiated.</td>
</tr>
<tr>
<td></td>
<td>- In Progress</td>
</tr>
<tr>
<td></td>
<td>The Control Center has acknowledged a replication request and the</td>
</tr>
<tr>
<td></td>
<td>process is under way.</td>
</tr>
<tr>
<td></td>
<td>- Success</td>
</tr>
<tr>
<td></td>
<td>Replication has completed successfully.</td>
</tr>
<tr>
<td></td>
<td>- Failed</td>
</tr>
<tr>
<td></td>
<td>The replication failed. Consult your logs to identify possible causes.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing log files” on page 406.</td>
</tr>
<tr>
<td></td>
<td>- Complete</td>
</tr>
<tr>
<td></td>
<td>Replication has completed successfully.</td>
</tr>
<tr>
<td>Started</td>
<td>The time at which the most recent replication began.</td>
</tr>
<tr>
<td>Ended</td>
<td>The time at which the most recent replication finished.</td>
</tr>
<tr>
<td>Size</td>
<td>The number of bytes of replicated data.</td>
</tr>
</tbody>
</table>

See “Viewing Control Center replication status” on page 400.

See “Replicating the Control Center database manually” on page 402.
Replicating the Control Center database manually

You can configure Symantec Brightmail Gateway to replicate the Control Center database to the Scanners according to the schedule that you specify. However, you can perform a manual replication as needed. Ensure that you have enabled Scanner replication before you to initiate a manual replication. And the Scanners must be installed and enabled. You must have Full Administration rights or Manage Status and Logs modify rights to perform a manual replication.

Replication takes some time to be initiated and performed. The amount of time depends on the number of records that must be synchronized.

See “About LDAP synchronization and Control Center replication” on page 395.

**Note:** Perform synchronization before replication. If a replication begins while synchronization is in process, the synchronization process stops.

See “Replication status information” on page 401.

See “Canceling an LDAP synchronization in progress” on page 399.

If you initiate a manual replication and want to stop it, you can cancel it.

See “Canceling a Control Center replication in progress” on page 402.

**To replicate the Control Center database manually**

1. In the Control Center, click **Status > System > LDAP Synchronization**.
2. Click the **CC to Scanners** tab.
3. Click **Replicate Now**.
4. On in the navigation pane under System, click **LDAP Synchronization**, and then click the **CC to Scanners** tab to refresh the page and view the status of the replication in progress.

See “Replication status information” on page 401.

Canceling a Control Center replication in progress

You can cancel a manual Control Center replication or scheduled Control Center replication at any time. If you cancel a replication, you cannot reinitiate it at a later time. You can either perform a manual replication or wait until the next scheduled replication.

You must have Full Administration rights or Manage Status and Logs modify rights to cancel a Control Center replication.
To cancel Control Center replication in progress
1  In the Control Center, click **Status > System > LDAP Synchronization**.
2  Click the **CC to Scanners** tab.
3  Click **Cancel Replication** to cancel a replication in progress.

About logs

Symantec Brightmail Gateway logs information about the Control Center, Spam Quarantine, and each Scanner. You specify the level of information that you want logged. Some Scanner logs can be sent to syslog on a remote server in addition to or instead of being viewed on the Control Center.

See “Log types” on page 403.
See “Configuring log levels” on page 410.
See “Configuring remote logging to syslog” on page 412.

Scanner log files are maintained on that Scanner. At a regularly scheduled interval, Symantec Brightmail Gateway's Control Center accesses Scanner logs. It copies and stores the Scanner log information in a log database that is stored on the Control Center computer. When you generate a log from the Control Center, Symantec Brightmail Gateway uses the information in the log database to compile the report.

See “Viewing log files” on page 406.
See “Saving log files” on page 407.

By default, the maximum size of the log database is 10 MB. However you can modify this size. You can also purge the files that are in the log database at the frequency and interval that you choose.

See “Managing the log database size” on page 408.
See “Manually deleting Scanner log files” on page 410.

You must have Full Administration rights or Manage Status and Logs view or modify rights to view logs. You must have Full Administration rights or Manage Status and Logs modify rights to modify log settings.

Log types

Symantec Brightmail Gateway logs let you monitor performance for your Scanners, the Control Center, and Spam Quarantine.

Table 15-6 describes the log types that are available for Scanners.
### Table 15-6  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 issues or for monitoring the product.</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>IM Relay</td>
<td>Records the status about instant messaging activities, such as scanning instant messages for viruses.</td>
</tr>
<tr>
<td>Premium Compliance</td>
<td>Records the status about Premium Compliance.</td>
</tr>
</tbody>
</table>

Table 15-7 describes the log types that are available for the Control Center console.

### Table 15-7  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 15-8 describes the log types that are available for the Control Center database.

### Table 15-8  Control Center log types—Database

<table>
<thead>
<tr>
<th>Database log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error.log</td>
<td>Records any errors that occur while the Control Center accesses the MySQL database.</td>
</tr>
</tbody>
</table>
Table 15-8  Control Center log types—Database (continued)

<table>
<thead>
<tr>
<th>Database log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slow-queries.log</td>
<td>Records the slow MySQL queries.</td>
</tr>
</tbody>
</table>

Table 15-9 describes the log types that are available for the Control Center LDAP synchronization and replication.

Table 15-9  Control Center log types—LDAP

<table>
<thead>
<tr>
<th>LDAP log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access.log.1</td>
<td>Records the status of the LDAP commands that run by the LDAP synchronization and replication service.</td>
</tr>
<tr>
<td>command.log.1</td>
<td>Records the internal commands that run by the LDAP synchronization and replication service.</td>
</tr>
<tr>
<td>&lt;directory_type&gt;CNA.trace.log</td>
<td>Records the status of the change notification agent for a directory that relates to LDAP synchronization and replication.</td>
</tr>
<tr>
<td>ensure.log.1</td>
<td>Records the status of the LDAP synchronization and replication service.</td>
</tr>
<tr>
<td>error.log.1</td>
<td>Records the LDAP errors that relate to the LDAP synchronization and replication service.</td>
</tr>
<tr>
<td>init.log</td>
<td>Records the operational status of the LDAP synchronization and replication service.</td>
</tr>
<tr>
<td>mapping_upgrade.log</td>
<td>Records the status of the LDAP synchronization and replication service migration utility.</td>
</tr>
<tr>
<td>trace.log.1</td>
<td>Records the status of the LDAP synchronization and replication service.</td>
</tr>
</tbody>
</table>

describes the log type that is available for the Control Center events.

Table 15-10  Control Center log types—Events

<table>
<thead>
<tr>
<th>Event log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brightmail_Admin_Events.</td>
<td>Records all changes made in the Control Center for the date indicated in the log file name.</td>
</tr>
<tr>
<td>&lt;yyy-mm-dd&gt;.log</td>
<td></td>
</tr>
</tbody>
</table>
Table 15-11 describes the log type that is available for Spam Quarantine.

### Table 15-11  Quarantine log types

<table>
<thead>
<tr>
<th>Quarantine log file</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>

See “About logs” on page 403.

See “Viewing log files” on page 406.

### Viewing log files

You can view the events that are logged for the Control Center, your Scanners, and Spam Quarantine. When you create a filter and display it, Symantec Brightmail Gateway generates the list of log events based on the criteria that you specify. You must have Full Administration rights or Manage Status and Logs view or modify rights to view filtered logs.

See “About logs” on page 403.

Table 15-12 lists the filter options that you can use to view specific log events.

### Table 15-12  Log view options

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host (drop-down)</td>
<td>Select a host from the list. This option is only available for Scanner logs.</td>
</tr>
<tr>
<td>Severity (drop-down)</td>
<td>Select a severity level from the list. This option is only available for Scanner logs.</td>
</tr>
<tr>
<td>Time range (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>
<tr>
<td>Component (drop-down)</td>
<td>Select a component for which to view logs: Scanner, Control Center, or Quarantine.</td>
</tr>
<tr>
<td>Log type (drop-down)</td>
<td>Select a log type from the list. See “Log types” on page 403.</td>
</tr>
</tbody>
</table>
Table 15-12  Log view options (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log actions (drop-down)</td>
<td>Select the type of actions to log: system events, message actions, blocking 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.

See “Saving log files” on page 407.

See “Managing the log database size” on page 408.

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.

Saving log files

Symantec Brightmail 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 and Quarantine 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 and Quarantine log require that you save the Log files that you want individually.

See “About logs” on page 403.

To save log files

1. In the Control Center, click **Status > System > Logs**.
2. Create a log.
   
   See “Viewing log files” on page 406.
3  Do any of the following:

To save a Scanner log file  
Click Save Log.

To save Control Center or Quarantine logs  
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.

Managing the log database size

At a regularly scheduled interval, Symantec Brightmail Gateway's Control Center accesses Scanner logs. It copies and stores the Scanner log files in a log database on the Control Center. When you generate a log, Symantec Brightmail Gateway uses the log files that are stored in its log database to compile the information.

See “About logs” on page 403.

See “Viewing log files” on page 406.

Depending on your environment and the level of information that is logged, the log database size can become unmanageable.

To restrict the size of the database, Symantec Brightmail Gateway provides default settings to maintain the log database size and to purge older log files. However, you can modify those settings. You must have Full Administration rights or Manage Status or Logs modify rights to modify the log database storage size.

Table 15-13 lists the options that you can configure to manage the log database size.
Table 15-13  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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The default value is 7.</td>
</tr>
<tr>
<td>Log Expunger frequency</td>
<td>Specifies how frequently the Expunger utility runs.</td>
</tr>
<tr>
<td></td>
<td>The Log Expunger deletes older log files to enforce the maximum log size.</td>
</tr>
<tr>
<td></td>
<td>The default setting is Every day.</td>
</tr>
<tr>
<td>Log Expunger start time</td>
<td>Specifies the time in which the Expunger starts.</td>
</tr>
<tr>
<td></td>
<td>The time is based on a 24-hour clock. For example, 23:00 is 11:00 P.M.</td>
</tr>
<tr>
<td></td>
<td>The default setting is 02:00 (2:00 A.M.).</td>
</tr>
</tbody>
</table>

**Note:** When the Log Expunger runs, it deletes log file database entries in the Log database. It does not compact the database. To compact the database and decrease the size of the database, Symantec Brightmail 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 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.

**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**.

**Manually deleting Scanner log files**

In addition to purging the log database, you can also manually delete the Scanner log files that are stored in the Control Center log database. When you delete Scanner log files, you delete those items that appear in the filtered view, which are compiled from the Control Center log database. The original, raw log files remain on the Scanner. This feature only applies to Scanner logs.

See “About logs” on page 403.

See “Managing the log database size” on page 408.

You must have Full Administration rights or Manage Status or Logs modify rights to manually delete Scanner logs.

**To manually delete Scanner log files**

1 In the Control Center, click **Status > System > Logs**.

2 Create a log for a Scanner.

   See “Viewing log files” on page 406.

3 Click **Clear All Scanner Logs**.

**Configuring log levels**

You can specify the log levels that you want for your Scanners and their components. The level that you select should contain the type of information that you want to monitor. But not so much information that would take up large amounts of disk space for storage or consume large processing loads 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.

**Warning:** The higher the logging level, the greater the demand on system resources.

Table 15-14 lists the log levels from the lowest level to the highest level.

<table>
<thead>
<tr>
<th>Table 15-14</th>
<th>Log levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Errors</td>
<td>Provides the most important information. This level provides the least amount of log information.</td>
</tr>
<tr>
<td>Warnings</td>
<td>Provides warning information and all Errors level data. 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. This level provides the greatest amount of log information. <strong>Warning:</strong> Consult Symantec Technical Support before you use this log level.</td>
</tr>
</tbody>
</table>

See “Log types” on page 403.

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.

See “About logs” on page 403.

See “Viewing log files” on page 406.

**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**.

4 Click the drop-down list and select the host for which you want to set the log levels.

5 Use the Component Local Log Levels drop-down lists to select the log level for each component.

6 Click **Save**.

To configure log levels for all local Scanners

1 In the Control Center, click **Administration > Settings > Logs**.

2 Click the **Local** tab.

3 Under Local Logging, uncheck **Enable local logs for components of the following host**.

4 Use the Component Local Log Levels drop-down lists to select the log level for each component.

5 Check **Apply these Local Log Levels to all hosts**.

6 Click **Save**.

To configure log levels for remote Scanners

1 In the Control Center, click **Administration > Settings > Logs**.

2 Click the **Remote** tab.

3 Use the Component Remote Log Levels drop-down lists to select the log level the facility for each component.

   See “Configuring remote logging to syslog” on page 412.

4 Click **Save**.

### 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.

   See “Format of audit logs” on page 613.

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 Brightmail 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>
jlu-controller: [Brightmail] (INFO:21145.3071248064): [54038]
AV definitions are up-to-date. |

- **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 Brightmail 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 send to a remote syslog. The following is a log message for one event as it would appear on the remote syslog.
You can configure Symantec Brightmail 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 413.

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,</td>
<td>Jan 15 11:51:33</td>
<td>scanner1</td>
<td>syslog-ng</td>
<td>syslog-ng version 1.6.5 starting syslog-ng[25257]:</td>
</tr>
<tr>
<td>facility, log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>level, and IP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See “Standard prefix for Scanner logs sent to remote syslog” on page 413.

The log messages that are sent to the remote syslog take the following form:

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, JLU Controller, and IM Relay for remote syslog

You can configure Symantec Brightmail 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 413.

The following table contains sample log messages for the following components in the same order listed:

- Conduit
- Brightmail Client
- Brightmail Engine
- JLU Controller
- IM Relay

|-----------------|---------------|--------------------|------------------------|-----------------------------|-------------------------|---------|
| Date, time, facility, log level, and IP address | Jan 15 11:34:51 | scanner1 | conduit: [Brightmail] | (DEBUG: 19713. 3071461056): 586:initialize | | Appending HTTP header: 'Spamwall_ID: (null)'
| | Jan 15 11:36:16 | scanner1 | ecelerity: [Brightmail] | (DEBUG: 20132. 3082545888): | | DPP system initialized
| | Jan 15 11:37:05 | scanner1 | bmserver: [Brightmail] | (DEBUG: 20516. 3066324672): rhk_hint_parse | | rhk hint for rule 43731290 has been successfully parsed
| | Jan 15 11:38:05 | scanner1 | jlu-controller: [Brightmail] | (INFO: 54038) | | AV definitions are up-to-date.
|----------------|--------------|-------------------|-----------------------|-----------------------------|------------------------|---------|

The following is a log message for one event as it would appear on the remote syslog.


**Log format of mail transfer agent for remote syslog**

You can configure Symantec Brightmail 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 413.

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</td>
<td>scanner1</td>
<td>ecelerity: [21911]</td>
<td>THPL-00150: Defer_queue_suspect_bad_message thread -1696945232 starting</td>
</tr>
</tbody>
</table>

The facility for MTA messages is always mail. See “Standard prefix for Scanner logs sent to remote syslog” on page 413.

The date and time is the date and time that the log message was recorded on the Scanner.

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 Brightmail 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 413.

The message audit log messages sent to the remote syslog take the following form:
<table>
<thead>
<tr>
<th><strong>Standard prefix</strong></th>
<th><strong>Date and time</strong></th>
<th><strong>Scanner host name</strong></th>
<th><strong>Process:</strong></th>
<th><strong>Message</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date, time, facility, log level, and IP address</td>
<td>Jan 15 15:42</td>
<td>scanner1</td>
<td>ecelerity: 1230876822</td>
<td>0ad9200d-b7b61ae000005b81-00-495db08c9df2</td>
</tr>
</tbody>
</table>

See “Standard prefix for Scanner logs sent to remote syslog” on page 413.

<table>
<thead>
<tr>
<th><strong>Date and time</strong></th>
<th><strong>Name of the Scanner on which the log message was created.</strong></th>
<th><strong>Name of the process that generated the log message.</strong></th>
<th><strong>Log message.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date in the format month date. Time in the format hour:minute. The time is in 24-hour clock notation.</td>
<td>The following is a log message for one event as it would appear on the remote syslog.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>This is the date and time that the log message was recorded on the Scanner.</td>
<td>01-15-2009 11:44:53 Local3.Info 10.217.32.13</td>
<td>Jan 15 15:42:42 scanner1 ecelerity: 1230876822</td>
<td>0ad9200d-b7b61ae000005b81-00-495db08c9df2</td>
</tr>
</tbody>
</table>

### About message audit logging

Symantec Brightmail 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.
**Note:** Log entries for messages are created after all policy actions applicable to a message have taken place. Because some actions, like Forward a copy of the message and Add BCC recipients, modify the envelope, it can be difficult to distinguish between the original and later email recipients.

**Note:** Messages that are rejected by the Spam Quarantine because they exceed the size limit appear in the Message Audit Log with no indication of the rejection. Instead, the rejection is recorded in the BrightmailLog.log file with the associated Audit ID that matches the entry in the Message Audit Log.

See “Checking the Control Center error log” on page 435.

To use the Message Audit log, employ the information and procedures described in this section. For a description of the logged information, see the search instructions in this section.

See “Searching for a message in the Message Audit Log” on page 419.

**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. The number of messages that a query can return is limited to 1,000. However, to reach this limit Symantec Brightmail Gateway counts multiple entries for the different recipients of the same message as one message.

### Enabling the Message Audit Log

By default, the Message Audit Log is disabled. You must enable this feature before any auditing information is available for viewing or searching. It is important to realize that storage for message auditing can become large, and searching the logs can create high demand for Scanner processing time.

**To enable the Message Audit Log**

1. In the Control Center, click **Administration > Settings > Logs**.
2. On the Local tab, under Message Audit Logs, check **Enable message logs**.
3. 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 Brightmail 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 15-15.

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 15-16.

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 15-15 describes the items you can choose for your single required filter.

Table 15-15  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 Brightmail Gateway and included as a message header</td>
</tr>
</tbody>
</table>
Table 15-15  Choices for the mandatory search criteria *(continued)*

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection IP</td>
<td>IP address of the connecting server. In cases where Symantec Brightmail 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.</td>
</tr>
</tbody>
</table>

Table 15-16 describes the items you can choose for your single optional filter.

Table 15-16  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>Recipient</td>
<td>Name of the message recipient</td>
</tr>
<tr>
<td>Subject</td>
<td>Message subject</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. Because the Message ID is not generated by Symantec Brightmail Gateway, the uniqueness of the ID cannot be guaranteed. Spammers have used this header to mask the identity of a message originator.</td>
</tr>
<tr>
<td>Verdict</td>
<td>Verdict and/or other characteristics of a message such as Message has malformed mime. When this filter option is selected, a list of possible verdicts appears in the Option filter value drop-down list. Use these values to filter messages that resulted in a given verdict.</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. These verdicts are available to inform you of any policies that are not currently associated with a recipient/sender group that would have been triggered for a given message.</td>
</tr>
</tbody>
</table>
### Table 15-16  Choices for the optional search criteria (continued)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action taken</td>
<td>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 exceeding size limit ▪ Rejected message due to lost connection ▪ Rejected message for all recipients ▪ Rejected message The Rejected message reason indicates that Symantec Brightmail Gateway was unable to tell why the message was rejected. In many cases this occurs when a connection is lost at an early stage, or when the sending mail server stops transmission at an incomplete state.</td>
</tr>
<tr>
<td>Connection IP</td>
<td>Connection IP used to receive the message.</td>
</tr>
<tr>
<td>Target IP</td>
<td>IP address of the message destination.</td>
</tr>
<tr>
<td>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 compliance policy.</td>
</tr>
<tr>
<td>Reason for unscannable verdict</td>
<td>Reason that the message matched the &quot;If a message is unscannable for viruses&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>
</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 Brightmail Gateway counts multiple entries for the different recipients of the same message as one message.

---

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 compliance 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 incident** or **Hold incident for review** 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.
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.
6. Click the File Encoding drop-down list to choose a character encoding for the CSV file.
7. Click the CSV Delimiter drop-down list and choose a delimiter for the CSV file.
   Symantec Brightmail 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. After you stop the message flow, you can attempt to redeliver the messages by flushing the queue. You can also delete the messages that block the queue. When you resolve the issue, you can restart the message flow.

See “Monitoring message queue size and volume” on page 428.
See “Viewing queued messages” on page 425.
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 Brightmail Gateway also has the filtering options that let you further customize the queued messages to view. Based on your filter criteria, Symantec Brightmail 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 Errors column.

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 senders.

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.
   
To refresh the view

◆ On the Message Queues page, click Refresh.

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 cannot access the messages that are queued, nor can you save them. 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. Before you delete all queued messages, you might want to temporarily stop the mail flow.

See “Stopping the mail flow” on page 427.

You must have Full Administration rights or Manage Status and Logs modify rights to delete queued messages.

See “Adding administrators” on page 439.

**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 425.
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: Click Delete all.

**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 also 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 427.

See “MTA and message queue behavior” on page 111.

See “Managing services, Scanner replication, and MTA operations” on page 108.
You must have Full Administration rights or Manage Status and Logs modify
rights to flush message queues.

You can also flush email queues from command line.

See “mta-control” on page 619.

**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 mail flow direction.
4. Click **Flush**.
5. Wait until the message queue is empty (repeat the previous step as needed).

**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 426.

See “Deleting queued messages” on page 425.

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 not scanned and accumulates in the delivery message queue.

See “MTA and message queue behavior” on page 111.

See “Turning off an appliance” on page 466.

See “Managing services, Scanner replication, and MTA operations” on page 108.

**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**.
4. If the queue is started, click **Stop**.
5. From the Queues drop-down list, select **Outbound** and click **Display**.
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**.

**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 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. You can configure alerts for message queues on the Alerts page.

See “Configuring SMTP Advanced Settings” on page 118.

You must have Full Administration rights or Manage Status and Logs view rights.

See “About message queues” on page 424.

See “Viewing queued messages” on page 425.

See “Flushing message queues” on page 426.

**To monitor message queue size and volume**

1 In the Control Center, click **Status > System > Hosts**.
2 Click the **Message Queues** tab.

**Troubleshooting the message queue**

When a message queue becomes too large, Symantec Brightmail Gateway can become unresponsive or crash. To attempt to deter this issue, by default, Symantec Brightmail 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 118.

If you experience issues with the message queue, try the following:

- Make sure that your downstream delivery host is functioning and accepting mail.
  
  See “Viewing the status of software and services” on page 394.

- Configure the MTA to reject incoming messages.
  
  See “Managing services, Scanner replication, and MTA operations” on page 108.

- Watch and monitor the queues until they reach acceptable limits.
See “Viewing queued messages” on page 425.

Repeat these measures until the issue is resolved.

**Viewing IM users that are signed on**

You can view a list of both the registered and unregistered IM users that are currently signed on. IM users that are currently signed on are known as active IM users.

See “About registering IM users” on page 259.

You can view all active IM users, or you can create a filter to display only the active IM users that you want to view. The filter that you create is based on the values that you specify for one or more of the available user attributes. For example, you can create a filter to display the active IM users of a specific IM network, specific IP address, or both.

You can also use a wildcard in your filters to further specify the active IM users that you want to view. When creating a filter for Screen Name, Email Address, or IP Address, you can use the asterisk (*) to represent one or more characters in the filter value that you specify. In addition, you can use more than one wildcard in the same filter value. For example, if you specify jsmith*@*.com as the email address, IM users jsmith1@hotmail.com and jsmith10@gmail.com appear.

You can create a filter by using the following user attributes:

**IM Account**

The screen name of the IM user.

You can specify a complete screen name, or you can use a wildcard to represent one or more characters within a screen name. For example, if you specify jsmith*, users jsmith1 and jsmith10 appear.

**Note:** The screen name that you specify cannot begin with a wildcard. For example, you cannot specify *smith.

**Email Address**

The email address of the IM user.

You can specify a complete email address, or you can use a wildcard to represent one or more characters within the email address. For example, if you specify jsmith*@hotmail.com, users jsmith1@hotmail.com and jsmith10@hotmail.com appear.

**Note:** The email address that you specify cannot begin with a wildcard. For example, you cannot specify *smith@hotmail.com.
The IM network of the IM user. These include:
- AOL
- Google Talk
- MSN Messenger
- Yahoo IM

You can select one of the IM networks from the drop-down list, or you can select All networks.

The IP address of the IM network from which the IM user is signed on.

You can specify a single IP address, or you can use a wildcard to represent one or more characters within one of the IP address's bytes. For example, if you specify 192.255.255.*, all active IM users for that network appear.

The IP address that you specify cannot:
- Contain more than 3 dots
- Contain consecutive dots
- Begin or end with a dot
- Contain a number that is greater than 255

**To view active IM users**

1. In the Control Center, click **Status > Instant Messaging > Active Users**.
2. (Optional) Under Filter, type the value of one or more user attributes that you want to use to display the active IM users.

   The attributes include:
   - IM Account
   - Email Address
   - IM Network
   - IP Address

   See “Viewing IM users that are signed on” on page 429.
3. Do one of the following:
   - Click **Display Filtered** to display the active IM users that are based on the values of your current filter.
   - Click **Clear Filters** to clear the values of your current filter.

You can specify the number of active IM users that you want to appear on each page of your search results. This number is based on increments of 10, 25, 50 or
100. Based on the increment that you specify, you can navigate immediately to any page that contains additional search results. For example, if you specify that you want 10 users to appear on each page, and your search results yield 100 users, you can navigate to the page that contains users 21-30. Using the control buttons, you can also navigate to the first page, the previous page, the next page, or the last page at any time.

The search results contain the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IM Account</td>
<td>The IM screen name of the user.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The corporate email address of the user. The email address appears only if the user is registered. See “About registering IM users” on page 259.</td>
</tr>
<tr>
<td>IM Network</td>
<td>The IM network of the user.</td>
</tr>
<tr>
<td>Client Version</td>
<td>The version number of the user’s IM client.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the user's IM client, such as &quot;online&quot; or &quot;away.&quot; The status is based on the various status types that are available for each IM client, including custom status types.</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address from which the IM user is signed on.</td>
</tr>
<tr>
<td>Duration</td>
<td>The amount of time that the IM user has been signed on. The duration is based on days, hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>

By default, the active IM users that appear in your search results are sorted in ascending order by the users’ IM Account name. However, you can re-sort your search results in ascending or descending order by IM Account, Email Address, or IM Network.

After you display your search results, you can export them to a comma-separated values (CSV) file. The CSV file contains all the users that appear in your search results (not just the users that appear on the current page).

To work with the search results

1. From the Entries per page drop-down list, select the number of IM users that you want to appear on each page.

   The default setting is 25.

2. To view another page, do one of the following:
   - From the Display drop-down list, select the page that you want to view.
   - Click the First Page, Previous Page, Next Page, or Last Page button.
Viewing the connection status of your IM networks

You can view the connection status of each IM network that you support from each Scanner that is in your corporate network. This feature may be helpful after you initially configure your DNS, after you configure a Scanner, or when IM connectivity problems are reported.

Each Scanner in your corporate network regularly attempts to connect to the public IM network servers that Symantec Brightmail Gateway supports.

Based on the success or failure of these connection attempts, the following results appear on the IM Network Status page:

- If a Scanner establishes a connection with an IM network, a green check mark appears in the column for that network. This includes IM networks to which you blocked access.
  
  See “Blocking access to an IM network” on page 269.

- If a Scanner is unable to establish a connection with an IM network, Unknown appears in the column for that network.

- If a Scanner is disabled, a dash appears in the column for each IM network that is associated with that Scanner.

- If an IM client is directed back to the Scanner instead of the Internet, Loopback appears in the column for the network that is associated with that client. This typically means that your DNS is configured incorrectly. See the Symantec Brightmail Gateway Installation Guide.

To view IM network status

- In the Control Center, click Status > Instant Messaging > Network Status.
Administering your product through the Control Center

This chapter includes the following topics:

- About simultaneous Control Center access
- About backing up log data
- Checking the Control Center error log
- Running network utilities from the Control Center
- Licensing your product
- Viewing license statuses
- Enforcing strong passwords
- Adding administrators
- Editing an administrator
- Deleting an administrator
- Administrator rights
- Resetting an administrator password
- Configuring alert notification criteria
- Monitoring devices through SNMP
- About specifying host names for Control Center access
- Specifying a custom user logon help page
Setting the locale encoding and fallback encoding

About maintaining adequate disk space

Specifying SMTP host settings for product generated alerts, reports, and messages

Replicating data between the Control Center and your Scanners

Modifying or disabling the port through which the Control Center accepts messages

About configuring certificate settings

Turning off an appliance

Gracefully turning off the appliance due to loss of power

Restarting an appliance

Resetting an appliance to its factory defaults

Scheduling backups

Editing a scheduled backup

Deleting a scheduled backup

Performing an on-demand backup

Restoring an appliance from backups

Determining what version of software is installed

Updating your software

Scanning non-plain text file attachments for content compliance

Determining which message caused a Brightmail Engine failure

### 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.
About backing up log data

In general, there is no reason to backup 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 “Viewing log files” on page 406.
See “Saving log files” on page 407.
See “Managing the log database size” on page 408.

Checking the Control Center error log

You might 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:

```plaintext
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.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)
```
To check 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.

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 hosts that 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 on the Internet

To run network utilities from the Control Center

1. In the Control Center, click Administration > Hosts > Utilities.
2. From the Host drop-down list, select a host name.
3. 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.
4. Click Run.
   - The results of the operation appear in the Results box.

Licensing your product

You must have valid licenses for the following Symantec Brightmail Gateway features for each Scanner that you install and enable:

- **Antispam**
Antivirus
- Premium Content Control
- Software updates

You can use the same license file to register multiple Scanners.

**Note:** License files must be on the same computer on which the Control Center runs unless you have specifically mapped a drive to an external computer.

See “Viewing license statuses” on page 437.

**To license your product**

1. In the Control Center, click **Administration > Hosts > Licenses**.
2. Do one of the following tasks:
   - In the **Provide a license file** field, type the full path and license file name.
   - Click **Browse** and locate the license file.
3. Click **Register License**.

**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 Brightmail 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.

See “Licensing your product” on page 436.

**To view license statuses**

1. In the Control Center, click **Administration > Hosts > Licenses**.
2. In the Host drop-down list, select a Scanner.
   - The status of the licenses and their expiration dates appear.
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.

See “Strong password criteria” on page 439.

See “Resetting an administrator password” on page 446.

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.

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 439.

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 and instant messaging 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 438.

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.

**Adding administrators**

When you add an administrator, you can specify the administrator's rights and which alerts and notifications the administrator receives.

See “Editing an administrator” on page 441.

See “Deleting an administrator” on page 441.

**To add an administrator**

1. In the Control Center, click **Administration > Users > Administrators**.
2. Click **Add**.
3. In the User namebox, 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 Choose the administrative rights that you want to assign to the administrator as follows:

<table>
<thead>
<tr>
<th>Full Administration Rights</th>
<th>Click <strong>Full Administration Rights</strong> to let the administrator view and modify all available rights.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited Administration Rights</td>
<td>Click <strong>Limited Administration Rights</strong> and choose the specific rights for this administrator as follows:</td>
</tr>
<tr>
<td>■ None</td>
<td>Administrators do not have any rights on selected task.</td>
</tr>
<tr>
<td>■ View</td>
<td>Administrators can view appropriate pages but cannot manage them.</td>
</tr>
<tr>
<td>■ Modify</td>
<td>Administrators have full rights to view and modify selected tasks.</td>
</tr>
<tr>
<td></td>
<td>See “Administrator rights” on page 442.</td>
</tr>
</tbody>
</table>

9 If you select Limited Administration Rights, beside Compliance Folders, choose the specific rights for this administrator as follows:

<table>
<thead>
<tr>
<th>None</th>
<th>Administrators can see compliance folder names but cannot see incidents in the Incident Management Overview page for a given folder.</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Administrators can view incidents in the indicated compliance folder but cannot manage them. Administrators with View permissions cannot perform any actions on incidents in the indicated compliance folder.</td>
</tr>
<tr>
<td>Modify</td>
<td>Administrators can view and modify all incidents in the indicated compliance folder.</td>
</tr>
</tbody>
</table>

10 Check **Receive Incident Notifications** to indicate the administrator is to receive notifications for the incidents that are created for the specific compliance folder.
11 Click **Save**.
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 442.
- Whether the administrator receives notifications about compliance folder incidents

See “Adding administrators” on page 439.

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 delete the administrator.

See “Editing an administrator” on page 441.

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.
Administrator rights

When you add or edit an administrator, you can assign that administrator full administration rights or limited administration rights. This section explains limited administration rights.

You can assign limited administration rights to an administrator on the Add Administrator or Edit Administrator page, both available from the Administration > Users > Administrators page. You can choose None, View, or Modify rights for each of the following:

- Manage Status and Logs
- Manage Reports
- Manage Policies
- Manage Settings
- Manage Administration
- Manage Quarantine

In addition, under Compliance Folders, you can choose None, View, or Modify for each compliance folder you have created, and you can check Receive Incident Notifications for any compliance folder.

Any administrator without either Full Administration Rights or Manage Administration rights will see the Administration > Users > Administrators page but will only be able to change his or her own password on that page.

Each type of limited administrator rights grants the administrator the ability to view a subset of the pages of the Control Center.

Note: Although many of the types of limited administrator rights allow you to view the pages for all compliance folders, they do not allow you to actually see the content of those compliance folders. To view or modify the contents of a compliance folder, you must have View or Modify rights for that folder under Compliance Folders on the Add Administrator or Edit Administrator page.

Table 16-1 shows the pages available to an administrator with Manage Status and Logs rights.
Table 16-1  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, Hosts, LDAP Synchronization, Logs</td>
</tr>
<tr>
<td>Status</td>
<td>SMTP</td>
<td>Message Audit Logs, Message Queues</td>
</tr>
<tr>
<td>Status</td>
<td>Instant Messaging</td>
<td>Active Users, Network Status</td>
</tr>
<tr>
<td>Compliance</td>
<td>Incident Management</td>
<td>Folder Overview</td>
</tr>
<tr>
<td>Administration</td>
<td>Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>Administration</td>
<td>Settings</td>
<td>LDAP, Logs</td>
</tr>
<tr>
<td>Administration</td>
<td>Hosts</td>
<td>Configuration, Licenses, Utilities</td>
</tr>
</tbody>
</table>

Table 16-2 shows the pages available to an administrator with Manage Reports rights.

Table 16-2  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, Favorite Reports</td>
</tr>
<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 16-3 shows the pages available to an administrator with Manage Policies rights.
### Table 16-3  Manage Policies pages

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>Instant Messaging</td>
<td>Network Access Control</td>
</tr>
<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></td>
<td></td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>Spam</td>
<td>Settings</td>
<td>Sender Authentication</td>
</tr>
<tr>
<td>Virus</td>
<td>Policies</td>
<td>Email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>Compliance</td>
<td>Policies</td>
<td>Email</td>
</tr>
<tr>
<td>Compliance</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>Groups</td>
</tr>
</tbody>
</table>

Table 16-4 shows the pages available to an administrator with Manage Settings rights.

### Table 16-4  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>
</tbody>
</table>
Table 16-4  Manage Settings pages (continued)

<table>
<thead>
<tr>
<th>Tab</th>
<th>Menu</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>Instant Messaging</td>
<td>▪ Registered Users</td>
</tr>
<tr>
<td>Spam</td>
<td>Settings</td>
<td>▪ Quarantine Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Scan Settings</td>
</tr>
<tr>
<td>Virus</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>Compliance</td>
<td>Settings</td>
<td>▪ Archive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ All compliance folders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Vontu DLP Connect</td>
</tr>
<tr>
<td>Administration</td>
<td>Settings</td>
<td>▪ Alerts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Certificates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Control Center</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ LDAP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ SNMP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ UPS</td>
</tr>
<tr>
<td>Administration</td>
<td>Hosts</td>
<td>▪ Configuration</td>
</tr>
</tbody>
</table>

Table 16-5 shows the pages available to an administrator with Manage Administration rights.

Table 16-5  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>▪ Administrators</td>
</tr>
<tr>
<td>Administration</td>
<td>Hosts</td>
<td>▪ Licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Shutdown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Version</td>
</tr>
</tbody>
</table>

Table 16-6 shows the pages available to an administrator with Manage Quarantine rights.
**Table 16-6** Manage Quarantine pages

<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>Administration</td>
<td>Users</td>
<td>Administrators</td>
</tr>
<tr>
<td>Administration</td>
<td>Settings</td>
<td>LDAP</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 442.

After resetting an administrator's password, use a secure method (such as a phone call) to notify the administrator of the new password. Email and instant messaging are not typically secure methods.

See “Enforcing strong passwords” on page 438.

See “Editing an administrator” on page 441.

**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**.
Configuring alert notification criteria

You can specify the email address that appears in the alert notification email and how frequently alerts are sent. You can also specify the conditions for which alerts are sent. Alerts are sent to the administrators that you specify when you create administrators. Administrators must have full administration privileges or Receive alert notifications privileges to receive alerts.

See “Adding administrators” on page 439.

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 “Types of alerts” on page 447.

To configure alert notification criteria

1. In the Control Center, click Administration > Settings > Alerts.
2. Under Notification, in the Send from box, type the email address.
3. In the Notification Frequency box, specify how frequently you want notifications sent.
4. Under Alert Conditions, check the alert conditions for which alerts are to be sent.
   Specify duration, percentage, or size parameters where necessary, with the appropriate boxes and drop-down lists.
5. Click Save.

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 alert notification criteria” on page 447.

Table 16-7 describes the available alert settings.

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send from</td>
<td>The email address that appears in the alert notification's From: header.</td>
</tr>
<tr>
<td>Alert setting</td>
<td>Explanation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Notification Frequency</td>
<td>The interval at which notifications are sent. The default is hourly.</td>
</tr>
<tr>
<td>Outbreak detection</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>Spam 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>
<tr>
<td>Virus filters are older than</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 7 days is recommended. The default setting is 10 days.</td>
</tr>
<tr>
<td>New virus filters are available</td>
<td>An alert is sent because new virus rules are available for download from Symantec Security Response. New virus rules are updated daily. Rapid Response rules are updated hourly.</td>
</tr>
<tr>
<td>The combined message queue is larger than</td>
<td>An alert is sent when the total combined size of all three message queues exceeds the size specified next to the alert description. Message queues include Inbound, Outbound and Delivery. Queues can grow if the MTA has stopped, or if an undeliverable message is blocking a queue.</td>
</tr>
<tr>
<td>Available Spam Quarantine is less than</td>
<td>An alert is sent when the disk space available for the Spam Quarantine is less than the specified amount.</td>
</tr>
<tr>
<td>Available Content Compliance folder is less than</td>
<td>An alert is sent when the disk space available for the Content Compliance folder is less than the specified amount.</td>
</tr>
<tr>
<td>LDAP synchronization errors</td>
<td>An alert is sent because of LDAP synchronization errors. These errors occur because of problems in directory synchronization. Only the messages that log at the error level cause alerts.</td>
</tr>
<tr>
<td>LDAP Scanner replication errors</td>
<td>An alert is sent because of replication errors. These errors occur because of problems in the replication of LDAP data from the Control Center to attached and enabled Scanners. Only the messages that log at the error level cause alerts.</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>
</tbody>
</table>
### Table 16-7  Alerts page (continued)

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<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>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 when a new software update release is available.</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>
</tbody>
</table>
| A queue reaches the message limit | An alert is sent when one of the three message queues (inbound, outbound, or delivery) exceeds the maximum number of messages set on the SMTP Advanced Settings page.  
See “Configuring SMTP Advanced Settings” on page 118. |
| A service is not responding or working | An alert is sent because of a nonresponsive service. Services include the Conduit, Brightmail Engine, IM, MTA, and LiveUpdate. |
| Hardware failures             | An alert is sent due to a hardware problem such as a fan failure or disk failure.                                                             |
| Service start after improper shutdown | An alert is sent because a service restarted after an improper shutdown. Services include the Conduit, Brightmail Engine, IM, MTA, and LiveUpdate. |
| Service shutdown              | An alert is sent because a service turned off normally. Services include the Conduit, Brightmail Engine, IM, MTA, and LiveUpdate.            |
| Service start                 | An alert is sent because a service was started. Services include the Conduit, Brightmail Engine, IM, MTA, and LiveUpdate.                  |
### Monitoring devices through SNMP

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.

Before you configure SNMP settings, you must first download the Management Information Base (MIB) database and import it to your SNMP client.

See “Downloading a Management Information Base for SNMP” on page 451.

**To monitor devices through SNMP**

1. In the Control Center, click **Administration > Settings > SNMP**.
2. Check **Enable SNMP**.
3. In the SNMP community string box, type the SNMP Agent’s community string.
4. In the SNMP listen port box, type the port at which the SNMP agent listens for network traffic.
5. In the SNMP trap host box, type the IP address of the device that receives SNMP trap alerts.
6. 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** and then type the IP address of specific hosts that you want to have access to the SNMP client.
7. Click **Add**.
8. You can delete any currently SNMP-access-enabled hosts by checking the box next to their names and clicking **Delete**.
9. Click **Save**.

### Table 16-7

<table>
<thead>
<tr>
<th>Alert setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
Downloading a Management Information Base for SNMP

Before you configure SNMP settings, you must first download the Management Information Base (MIB) database and import it to your SNMP client.

The following SNMP MIBs are provided for hardware related alerts:

- LSI-AdapterSAS.txt
- LSI-AdapterSASIR.txt
- PERC-MIB.txt
- afa-MIB.txt

The following SNMP MIB is provided for Symantec Brightmail Gateway applications:

- SYMANTEC-EMAIL-SECURITY.txt

See “Monitoring devices through SNMP” on page 450.

To download a MIB for SNMP

1. Log into the Control Center.
2. Type /snmp-mibs in the URL path in your browser after /brightmail and press Enter.
   
   For example: https://your_hostname/brightmail/snmp-mibs
   
   The MIBs page appears.
3. Download the appropriate MIB for your appliance and save it to the computer that runs the SNMP monitoring program.
4. Import the MIB file into any SNMP v2c-compliant monitoring program.

About specifying host names for Control Center access

When you specify host names for Control Center access, the Control Center lets clients connect based on the Control Center's DNS perspective. If the client's IP address resolves into a name that matches an allowed host name (a “reverse lookup”), then the Control Center permits access to the client.

The owner of a netblock controls the reverse lookup of an IP address. So users often have no control over what name their IP addresses resolve to. Also, multiple DNS servers may each have mappings for the same netblock that are not the same. For example, the client's authoritative DNS server has a reverse lookup record of 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
dhcp23.symantecexample.com for the same IP address. In this case, the Control
Center sees the dhcp23.symantecexample.com name whenever the client connects.
So that is the name that you should 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 452.

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 into 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 451.

---

**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 `clear
bcchostacl` command to clear the list of computers that are permitted to access
the Control Center. See “clear” on page 595.

---

**To specify which hosts can access the Control Center**

1. In the Control Center, click **Administration > Settings > Control Center**.
2. 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.
3  Click **Add**.

4  Click **Save**.

**Specifying a custom user logon help page**

By default, when users click the Need help logging in? link on the Control Center logon page, Symantec online Help appears. You can customize the logon help with a custom logon Help page. This change only affects the logon Help page, not the rest of the online Help.

Create a Web page that tells your users how to log on and make it available on your network. The Web page should be accessible from any computer where users log on.

See “Viewing spam and suspected messages in quarantine” on page 223.

**To specify a custom user logon help page**

1  In the Control Center, click **Administration > Settings > Control Center**.

2  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.

3  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.

To set the locale encoding and fallback encoding
1. In the Control Center, click Administration > Settings > Control Center.
2. Under System Locale and Fallback Encoding, click the System locale drop-down list and select an encoding.
3. Click the Quarantine fallback encoding drop-down list and select an encoding.
4. Click Save.

About maintaining adequate disk space

Symantec Brightmail Gateway performs better with more available disk space. Periodically compare the disk usage to the disk capacity to ensure that the Control Center and Scanners have adequate disk space. Certain features such as extended reporting data and Spam Quarantine can use a large quantity of disk space. Modify Expunger settings to reduce disk usage.

See “Modifying the disk space allotted for Suspect Virus Quarantine” on page 207.
See “Specifying when and how often Spam Quarantine is purged” on page 245.
See “About purging report data” on page 383.
See “Viewing the status of your hardware” on page 392.
See “Viewing information about your hardware” on page 393.

Specifying SMTP host settings for product generated alerts, reports, and messages

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 Brightmail 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 Brightmail 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 “Updating your software” on page 474.

**To specify SMTP host settings for product generated alerts, reports, and messages**

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Under SMTP Host do one of the following:
   - Click **Use existing non-local relay settings**.
     See “Configuring Scanner inbound email delivery settings” on page 102.
   - 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.

3. Click **Save**.

**Replicating data between the Control Center and your Scanners**

In the Control Center, replication refers to the process by which LDAP data stores are propagated from the Control Center to attached and enabled Scanners. Global settings in the Control Center and locally configurable settings on each Scanner control the replication process. You configure local replication settings for each Scanner through the Scanner configuration.

See “About LDAP synchronization and Control Center replication” on page 395.

No replication can occur until you have defined one or more LDAP servers to the Control Center and one full synchronization cycle is complete.

See “About LDAP synchronization” on page 481.
The replication attributes determine how replication operates. You can determine if replication is to take place and how often it occurs. These settings are in addition to those available on local Scanners that are attached and enabled through the Control Center.

The replication process does not complete until an LDAP synchronization source is available.

To replicate data between the Control Center and your Scanners

1. In the Control Center, click Administration > Settings > Control Center.
2. To activate Scanner replication, under LDAP Replication, check Enable LDAP Replication.
3. In the Replication frequency box and drop-down list, set the replication frequency.
4. Click Replicate Now to have LDAP data replicated to all attached and enabled Scanners immediately.
5. Click Save.

See “Viewing LDAP synchronization status” on page 396.

Modifying or disabling the port through which the Control Center accepts messages

By default, Spam Quarantine, Suspect Virus Quarantine, and Compliance 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 compliance folders” on page 346.

See “About quarantining spam” on page 220.

See “About quarantining suspected viruses” on page 199.
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 Under Listener Port in the Port box, do one of the following:
   - Type the new port number.
   - Type 0 to disable the listener port.

3 Click **Save**.

### About configuring certificate settings

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.

For successful SMTP/TLS or HTTPS authentication, 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 Brightmail Gateway includes pre-installed certificates for the most common Certificate Authority vendors. The Certificate Authority tab on the Certificate Settings page lists the pre-installed 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.

Symantec Brightmail Gateway supports the following types of certificates:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MTA TLS certificate</strong></td>
<td>The inbound and the outbound mail flows in each Scanner use the TLS certificate that is assigned to them to accept TLS-encrypted messages for scanning.</td>
</tr>
<tr>
<td></td>
<td>See “To assign an MTA TLS certificate to a Scanner” on page 464.</td>
</tr>
<tr>
<td><strong>User interface HTTPS certificate</strong></td>
<td>The Control Center uses the HTTPS certificate to secure communications for its Web-based management tools.</td>
</tr>
<tr>
<td></td>
<td>See “To assign a user interface HTTPS certificate to the Control Center” on page 465.</td>
</tr>
</tbody>
</table>
**Note:** When you purchase or generate a certificate, you must 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 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 request 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.

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.

### Adding a self-signed certificate

A self-signed certificate for HTTPS communication does not offer the same level of security as a CA-signed certificate. A self-signed certificate is not appropriate for SMTP/TLS.

See “Adding a CA certificate” on page 459.

See “About configuring certificate settings” on page 457.

**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, click **Self Signed**.
6. Complete the remainder of information on the page.
7. Click **Create**.
Requesting a Certificate Authority-signed certificate

A CA-signed certificate provides more security than a self-signed certificate and is appropriate for HTTPS and SMTP/TLS 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 Certificate Authorities may not support certificates that are created using an IP address instead of a domain name for the common name. Check with your Certificate Authority.

See “Viewing existing CA certificates” on page 463.

See “About configuring certificate settings” on page 457.

Each Certificate Authority has its own set of procedures to request certificates and issue certificates. Consult your Certificate Authority for details and follow the instructions that are appropriate for your installation.

See “Adding a CA certificate” on page 459.

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 Certificate Authority Signed.
6. Fill in the information the remainder of the page as appropriate.
7. Click Request.
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 Certificate Authority request form at a later time.

9. Submit the CSR to a Certificate Authority with the method that the Certificate Authority requires.

Adding a CA certificate

Symantec Brightmail Gateway includes pre-installed certificates for the most common Certificate Authority vendors. Add a CA certificate if the CA issues you an SMTP/TLS or HTTPS certificate that 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 a CA certificate, you complete the certificate chain to permit authentication of the new certificate. All of your configured Scanners can access the CA certificates in the Control Center for SMTP/TLS and HTTPS authentication.

Ensure that you have the CA certificate before you proceed. The CA certificate may have been included when you received the certificate from the CA. Alternatively, you may be able to download the CA certificate from the Certificate Authority's Web site. The file that contains the CA certificate must be in PEM format.

See “About configuring certificate settings” on page 457.

See “Requesting a Certificate Authority-signed certificate” on page 459.

See “About PEM format requirements for certificates and CA certificates” on page 460.

**To add a CA 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 certificate.
6. Click **Update**.

A status message appears at the top of the page to indicate success or failure.

**About PEM format requirements for certificates and CA certificates**

When you add a certificate or CA certificate to Symantec Brightmail Gateway, ensure that the certificate meets the following requirements:

- The certificate must be stored in a file in PEM format with the certificate included as Base64-encoded text between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`
  Any text outside of the begin and end certificate markers is ignored. 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 does not matter, but the .txt or .crt extension are typically used.

The file that contains the certificate must be accessible from the browser that you use to access the Control Center.

The following is a sample PEM format CA certificate:

```
-----BEGIN CERTIFICATE-----
MIICPTCCaaYCEQDNun9W8/N/kvFT+IqyczqpVMA0GCSqGSIb3DQEBAgUAMF8xCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwqSW5jLjE3MDUGA1UECxMuQ2xh
c3MgM5BQdXJ0aWMgUHJpbWFyQ2ZCZJ0aWZpY2F0aW9uIF1dGhvcm10eTAeFw05
NjAxMjkwMDAwMDBwaFw0yODA4MTEyMzU5NT1aMF8xCzABcBGNVBAYTAlVTMRcwFQYD
VQQKew5KZjU2InhiwqSW5jLjE3MDUGA1UEAxMwQ2xhMjC3MDkQc2VydGVyM2UtMV4x
NzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA5Rm/baNWYS2ZSHH2Z965jeu3noaACpEo+
jgl0aIguVzqKCBjJF0N
H8xlbgx0FaEGLeaBpsQoXPftFg5a27BhXVqKg/qhIjGTgsf7A01480Z4gJzRQR
4k5FVmkfeAKA2txHksm7NsljXMXgjy2He6G3MrB7MLoqlLzG7q7Nn2tsCAwEATAN
BkgkwhiG9w0BAQIFAAOBoQBBMP71Lxmf7kMzd3ppssHhE16M/+SG/Q2rdiVjzo
Ewx8QszznC7EBz8UsA9P/5CSvnnvErpj82ggAr3xSnxgiJduLHdqSjeyUVR5B5
FvjqBUuUfx3CHMjyQTQQdTw18fU+hi5Ia0e6E1srlhJ7qos/OJ0ANACY89Fx
1A==

-----END CERTIFICATE-----
```

Text before Begin Certificate is ignored.

Text after End Certificate is ignored.

See “Adding a CA certificate” on page 459.

See “Adding a self-signed certificate” on page 458.

Importing a Certificate Authority-signed certificate

When you receive a certificate from a Certificate Authority, you must import it to make it available in the Control Center. In addition to the certificate, the Certificate Authority might have sent you an intermediate certificate that you also need to install in the Control Center.

See “Adding a CA certificate” on page 459.
To import a Certificate Authority signed certificate

1 When you receive the certificate file from the Certificate Authority, 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.

Changing a CA certificate name

You can change a certificate 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 CA certificate” on page 459.

To change a CA 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.

6 Click Save.

Replacing existing CA certificates

You can replace 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 “About PEM format requirements for certificates and CA certificates” on page 460.
To replace 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.

Viewing existing CA certificates
You can view a list of the currently installed CA certificates.
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.

Backing up CA certificates
You can back up the CA certificates that are installed in the Control Center.
See “Viewing existing CA certificates” on page 463.
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.

Viewing an SMTP/TLS or HTTPS certificate
You can view the SMTP/TLS or HTTPS certificates that you have.
See “Deleting an SMTP/TLS or HTTPS certificate” on page 464.
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 or delete.
4. Click View.

Deleting an SMTP/TLS or HTTPS certificate
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 463.

To delete an SMTP/TLS or HTTPS certificate
1. Click Administration > Settings > Certificates.
2. Click the TLS & HTTPS Certificates tab.
3. Check the box next to the certificate that you want to delete.
4. Click Delete.

Assigning an MTA TLS certificate to a Scanner
Ensure that there is a chain of trust from your TLS certificate to the CA certificates that is installed in Symantec Brightmail Gateway. If you have assigned a TLS certificate and the Scanner does not accept TLS-encrypted email, an intermediate CA certificate may not be installed. Check the Scanner MTA log for TLS-encrypted the messages that the Scanner Certificate Authority signed certificate does not acknowledge. Before you proceed, ensure that you have a CA-signed certificate. You may also need to install an intermediate CA certificate.

Additional TLS encryption settings are available.

See “Requesting a Certificate Authority-signed certificate” on page 459.

See “Adding a CA certificate” on page 459.

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 Inbound Mail Settings, check Accept TLS encryption for inbound or outbound mail settings if you want this Scanner to scan for inbound or outbound TLS-encrypted email, respectively.
In the adjacent drop-down list, choose the MTA TLS certificate that is appropriate to the inbound mail flow or outbound mail flow.

You can assign the same certificate to both inbound and outbound TLS-encrypted email filtering.

Check **Request client certificate** if you want the connecting client to present a TLS certificate for authentication.

This step is required for the inbound mail setting only.

You may need to install an intermediate CA certificate to authenticate the connecting client's TLS certificate.

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 CA-signed certificate. If you use a CA-signed certificate, you may need to install an intermediate CA certificate.

See “Adding a CA certificate” on page 459.

**To assign a user interface HTTPS certificate to the Control Center**

1. In the Control Center, click **Administration > Settings > Control Center**.
2. Under Control Center Validation, click the User interface HTTPS certificate drop-down list and select a certificate.
3. 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 459.

2. Import the certificate that you receive from a Certificate Authority.

   See “Importing a Certificate Authority-signed certificate” on page 461.

3. Install an intermediate certificate, if needed.

   See “Adding a CA certificate” on page 459.

4. Assign the certificate as the Control Center HTTPS certificate.

   See “Assigning a user interface HTTPS certificate to the Control Center” on page 465.

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 465.

To designate a Control Center certificate

1. In the Control Center, click Administration > Settings > Control Center.

2. Under Control Center Validation, click the User interface HTTPS certificate drop-down list to select the certificate that you want to use.

   See “About configuring certificate settings” on page 457.

3. Click Save.

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.
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 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.

Gracefully turning off the appliance due to loss of power

Symantec Brightmail 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.
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 629.

**To gracefully turn off the appliance due to loss of power**

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.

   To disable a feature, type a value of 0.

---

**Restarting an appliance**

You can restart an appliance when needed. Restarting an appliance entails the appliance turning itself off and then restarting itself.

**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.
3. Click **Reboot**.

   All connections close and the system restarts.

---

**Resetting an appliance to its factory defaults**

You can return to the factory defaults with which an appliance was originally delivered. When you enable this feature, Symantec Brightmail Gateway does all of the following actions:

- Stops all Scanner hosts
- Clears all Hosts from the host table
- Clears all logs from the database
- Clears all reports from the database
- Clears all status information from the database
- Resets all settings and policies to their default values
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 125.

To reset an appliance to its factory defaults
1  In the Control Center, click Administration > Hosts > Version.
2  On the Factory Reset tab, click the Host drop-down list and select a host.
3  Click Reset.
4  Click OK to confirm reset or Cancel to stop the process.

Scheduling backups

Symantec Brightmail Gateway contains a backup program and scheduler in the Control Center. Use these features to back up of various types of Symantec Brightmail Gateway data. Restore backup data on the Restore/Download tab of the Host Version page.

See “Restoring an appliance from backups” on page 472.

Note: The db-backup command can back up your appliance with SCP. The Control Center does not offer this option.

See “db-backup” on page 597.

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, type a description of the scheduled backup.
4. Under Backup Data, choose from among the following backup types:

<table>
<thead>
<tr>
<th>Backup Type</th>
<th>Description</th>
<th>File Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Backup</td>
<td>Backs up the complete database, as well as Suspect Virus Quarantine messages and compliance messages that are stored on disk.</td>
<td>db-backup.brightmail.mm-dd-yr-hr-mm.full.manual.tar.bz2</td>
</tr>
<tr>
<td>Backup only Configuration and Incidents</td>
<td>Backs up all configuration data in the database, as well as compliance data and compliance messages that are stored on disk.</td>
<td>db-backup.brightmail.mm-dd-yr-hr-mm.config.incidents.tar.bz2</td>
</tr>
<tr>
<td>Backup only Configuration, Incidents, Logs and Reports</td>
<td>Backs up all configuration, incident, report, and log data in the database; as well as compliance messages that are stored on disk.</td>
<td>db-backup.brightmail.mm-dd-yr-hr-mm.config.incidents.reports.logs.tar.bz2</td>
</tr>
</tbody>
</table>

For all file types, "month" is expressed in standard three-letter format. The following example shows the file name of a full backup:

db-backup.brightmail.Aug-31-09-10-04.full.manual.tar.bz2

5. Under Backup Schedule, define the time and frequency to run the backup.

6. Under Backup To, specify whether to store backups on the local server or on a remote host using FTP.
   
The following shows sample values for specifying a remote backup through FTP:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>host.symantecs.org (or 192.168.2.42)</td>
</tr>
<tr>
<td>Port</td>
<td>21</td>
</tr>
<tr>
<td>Path</td>
<td>/home/username/backups/</td>
</tr>
</tbody>
</table>
7 If you back up on the local server, indicate how many backup versions to keep. The default is 3. You only need to specify the number of backup versions that are retained when you store files locally. When you store backup data at a remote location, you must supply the necessary information for FTP transfer. You must also provide user authentication information when required by the remote location.

8 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 469.

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 an on-demand backup of the appliance at any time. Restore backup data on the Restore/Download tab of the Host Version page.
See “Restoring an appliance from backups” on page 472.
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, click the backup data type that you want.
4. Under Backup To, specify whether the backup data is to be stored on the local server or at a remote location through file transfer protocol.
   When you store backup data at a remote location, you must supply the necessary information for FTP transfer. You must also provide user authentication information when required by the remote location.
5. Click Backup Now.

Restoring an appliance from backups

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 appear after the restore.

Note: After you restore an appliance that functions as your Control Center from a different IP address than the original IP address, you must reboot the appliance. If that appliance also hosts a Scanner, you should stop the Scanner first.

See “Restarting an appliance” on page 468.

See “Stopping and starting Scanners” on page 127.

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 to 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:

   Domain/IP address  host.symantecs.org (or 192.168.2.42)
   Port 21
   Path /home/username/backups/

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.

Determining what version of software is installed

You can determine what version of software is installed on your appliance.
See “Updating your software” on page 474.

To determine what 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.
Updating your software

You can determine whether software updates are available for your product. If updates are available, you can obtain the updates through the Control Center.

See “Determining what version of software is installed” on page 473.

To determine if software updates are available

1 In the Control Center, click Administration > Hosts > Version.
2 On the Updates tab, select a host from the drop-down list.
   When available, newer versions of software appear as radio buttons with a status of Available.
3 If software updates are available, select an update and click View Description to see a list of the included upgrades.

To update your software

1 In the Control Center, click Administration > Hosts > Version.
2 On the Updates tab, select a host.
3 If available, select an updated software version and click Update.
4 After you install a software update, close and restart your Web browser before you logon to the appliance.

Scanning non-plain text file attachments for content compliance

Symantec Brightmail Gateway checks plain text files against words as defined in content-related policies. But Symantec Brightmail Gateway can also check the attachments that are not plain text files against dictionaries. Scanning non-plain text files maximizes the effect of content filtering, it can impact the system load and slow down email filtering.

To scan non-plain text file attachments for content compliance

1 Click Protocols > SMTP > Settings.
2 Under Content Filtering Settings, check Enable scanning of non-plain text attachments for words in dictionaries.
   This setting can decrease scanning efficiency.
3 Click Save.
Determining which message caused a Brightmail Engine failure

In rare instances, a malformed email message may cause the Brightmail Engine to fail. If this situation occurs, Symantec Brightmail 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 Brightmail 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 `mta-control` command-line option.

Once the malformed message is identified, you have several options when you use the `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 “About administering your product through the command line” on page 591.

**To determine which message caused a Brightmail Engine failure**

1. Click **Protocols > SMTP > Settings**.
2. Under Scan Settings, check **Enable bad message handling**.
3. Type a value in the **Number of retries before classifying a message as bad** field.
4. Click **Save**.
Determining which message caused a Brightmail Engine failure
Using LDAP for Symantec Brightmail Gateway

This chapter includes the following topics:

- About the supported LDAP services and directories
- About the authentication service
- About LDAP synchronization
- About the LDAP routing service
- About recipient validation
- About Configuring LDAP settings and sources
- Configuring LDAP settings and adding source definitions
- About replicating data to Scanners

About the supported LDAP services and directories

LDAP (Lightweight Directory Access Protocol) is a directory name service that allows an organization to centralize email directory data. As the email "system of record," an organization's LDAP directory maintains the security of groups and distribution lists.

LDAP data includes the following:

- Email addresses of users and distribution lists
- Membership information for groups and distribution lists
- Authentication information for users
Symantec Brightmail Gateway can use the information that is stored in an LDAP source to provide a variety of services. You provide and configure these sources using the Settings page. Symantec Brightmail Gateway only reads LDAP directory data. It never writes data back to the LDAP source.

See “About Configuring LDAP settings and sources” on page 490.

Symantec Brightmail Gateway provides you with the ability to configure your LDAP directory using a number of directory types and services.

### Table 17-1 LDAP services

<table>
<thead>
<tr>
<th>LDAP service</th>
<th>Supported features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Authentication end-user login to Spam Quarantine</td>
</tr>
<tr>
<td></td>
<td>Validates email recipients for messages that are stored in Spam Quarantine</td>
</tr>
<tr>
<td></td>
<td>Enables end users to configure personal Good and Bad Sender lists based on email address (synchronization also required)</td>
</tr>
<tr>
<td></td>
<td>Enables end users to configure personal language settings (synchronization also required)</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Validates email recipient data and drops invalid recipients</td>
</tr>
<tr>
<td></td>
<td>Enables directory harvest attack recognition</td>
</tr>
<tr>
<td></td>
<td>Enables end users to configure personal Good and Bad Sender lists based on email address (authentication also required)</td>
</tr>
<tr>
<td></td>
<td>Enables end users to configure personal language settings (authentication also required)</td>
</tr>
<tr>
<td></td>
<td>Expands distribution list recipients to their individual members</td>
</tr>
<tr>
<td></td>
<td>Resolves group and distribution-list membership to enable scanners to apply policies</td>
</tr>
<tr>
<td>Routing</td>
<td>Routes email messages based on email alias</td>
</tr>
<tr>
<td></td>
<td>Routes email based on per-entry or per-domain mailhost settings</td>
</tr>
<tr>
<td>Recipient validation</td>
<td>Validates email recipient data and rejects invalid recipients (synchronization not required)</td>
</tr>
<tr>
<td></td>
<td>Enables directory harvest attack recognition (synchronization not required)</td>
</tr>
</tbody>
</table>
Symantec Brightmail Gateway provides you with the ability to manage your LDAP configuration using a number of directory types and services and supports the following LDAP directory types and services.

**Table 17-2  Supported LDAP directory services**

<table>
<thead>
<tr>
<th>Directory type</th>
<th>Authentication</th>
<th>Synchronization</th>
<th>Routing</th>
<th>Recipient validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2003 Active Directory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows 2000 Active Directory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sun Directory Server 5.2 (formerly known as iPlanet, SunONE, and Java directory servers) + service pack 4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange 5.5 service pack 3</td>
<td>Yes</td>
<td>Yes (full synchronization only)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lotus Domino LDAP Server 6.5.1</td>
<td>Yes</td>
<td>Yes (full synchronization only)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lotus Domino LDAP Server 7.0.2 (September 26, 2006)</td>
<td>Yes</td>
<td>Yes (full synchronization only)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OpenLDAP v2.3.14</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Other</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note:** If you use Sun Directory Server 5.2, Symantec recommends that you update to patch 5 or later. This patch resolves some known issues related to crashes in changelog processing.

Use the Other directory type for LDAPv3 implementations that support simple bind authentication and use a schema that represents attributes in the following ways:

- Primary email addresses in a simple single valued attribute – e.g., mail: user@domain.com
- Aliases in a simple multivalued attribute – e.g., mailAlias: user.alias1@domain.com, mailAlias: user.alias2@domain.com
- A single-valued login attribute – e.g., mailHost: smtp1.somedomain.com

Some LDAPv3 implementations may use the same primary email attribute as the login attribute – that is, end-users login using email address and password. In such a case the routing mail host should be expressed as a simple hostname or IP address.
OpenLDAP and LDAPv3 implementations cannot be used for synchronization—only for authentication, routing, and recipient validation. Symantec is unable to test its product against every possible implementation of LDAPv3.

See “About Configuring LDAP settings and sources” on page 490.

**About the authentication service**

The authentication service caches data from the specified LDAP source to authenticate end-user access to the Control Center. A user must be authenticated to log in to Spam Quarantine and can modify their Good and Bad Sender lists.

While the same LDAP source can also be used for both authentication and synchronization, no other LDAP source may be used for authentication. You do not need to configure LDAP synchronization to use the LDAP source to authenticate user access to Spam Quarantine. However, you do need to configure synchronization to enable users to configure personal Good and Bad Sender lists.

See “About Configuring LDAP settings and sources” on page 490.

During login or email recipient resolution, Symantec Brightmail Gateway substitutes a string that corresponds to the parts of the query delineated by the login and email attributes. The LDAP source should return at most a single entry to such a query.

For example, consider that LDAP Authentication Query Details have been configured to access an Active Directory server with the following attributes:

- **Login attribute**: samAccountName
- **Primary Email address**: mail
- **Email alias**: proxyAddresses

When the Control Center receives email addressed to john_smith@mycompany.com that has been flagged for quarantine, it replaces the Primary email address and Email alias attributes in the following Login query pattern

```
(&(|(objectCategory=group)(objectCategory=person))(&(|mail=*)(proxyAddresses=*)(sAMAccountName=*))
```

with the values for john_smith@mycompany.com to generate the following Login query:

```
(&(|(objectCategory=group)(objectCategory=person))
  (&(|mail=john_smith@mycompany.com)(proxyAddresses=john_smith@mycompany.com)(sAMAccountName=*))
```
Normally, if the email address corresponds to an existing user, the Active Directory server returns a single entry, and this entry is used to determine the primary deliverable email address. If the Active Directory server returns no results, it is considered an invalid recipient and the recipient can optionally be deleted or marked as 'postmaster' for review by users with administrator access to the Control Center.

If the Active Directory server returns more than one result or an error is encountered when attempting to query the server, the message is returned to the Scanner, where it is periodically resubmitted to quarantine. If the error is not resolved within the retry limit of the MTA, the message is bounced back to the original sender. A similar operation occurs when an end user logs on to the Control Center. If the Active Directory server verifies that the user name and password credentials are valid, the username is substituted into the Login attribute of the query.

```
(&(|(objectCategory=group)(objectCategory=person))(&(mail=*)(proxyAddresses=*))(sAMAccountName=jsmith))
```

If the query returns exactly one entry, that user is logged in, and quarantined messages to that user (john_smith@mycompany.com in our example) are displayed.

If the Active Directory server returns no results, more than one result, or an error is encountered when attempting to query the server, the user is not allowed to login, since the Control Center cannot verify the user's identity.

**Note:** For Exchange 5.5, the user directory Name (rdn) must be the same as the alias (uid) for that user.

Use the Add LDAP server page to configure LDAP authentication.

### About LDAP synchronization

You can provide Scanner access to LDAP directory information by synchronizing LDAP user, alias, group, and distribution-list data with the Control Center's own directory data stores.

See “About Configuring LDAP settings and sources” on page 490.

The Symantec Brightmail Gateway synchronization service first queries the LDAP source for user, group, and distribution-list data and inserts them into the Control Center LDAP database. Synchronization converts the directory data to a database format that is optimized for subsequent replication to attached and enabled Scanners. Scanners use this data to expand distribution lists and to carry out actions according to the conditions set by email filtering policies.
You must configure an LDAP source for synchronization if you want to drop invalid recipients. Select the Drop invalid recipients check box on the Invalid Recipient Handling page after configuring a synchronization source.

See “Configuring invalid recipient handling” on page 88.

When Enable distribution list expansion is checked on the LDAP Settings page, Symantec Brightmail Gateway enables distribution-list expansion for all LDAP sources that use synchronization. Mail is sent to the primary addresses of distribution list members unless Preserve recipient addresses is also checked, in which case the recipient alias address is preserved.

When Preserve recipient addresses on the LDAP Settings page is checked, Symantec Brightmail Gateway preserves recipient alias addresses when sending email to distribution list members if Enable distribution list expansion is left unchecked. If both Enable distribution list expansion and Preserve recipient addresses are 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. If Preserve recipient addresses is left unchecked and Enable distribution list expansion is checked, the recipient alias address resolves to the primary addresses of members in the distribution list; the alias address is not preserved. If both Preserve recipient addresses and Enable distribution list expansion are left unchecked, the alias does not resolve to primary addresses.

**Note:** After synchronizing Control Center and LDAP directory data, you need to replicate directory data to the Scanners on your network. Synchronization and replication are separate but not independent processes. Synchronization copies data from the LDAP source and stores it in the Control Center. Replication copies LDAP data stored in the Control Center to attached and enabled Scanners.

See “About replicating data to Scanners” on page 504.

You do not need to configure LDAP authentication to synchronize LDAP source data with the Control Center’s LDAP database unless you plan to enable end-user settings for Good and Bad Sender lists or Language preferences.

Symantec Brightmail Gateway's LDAP synchronization service supports both full and change-based synchronization. You should be aware of how the two types of synchronization affect performance.

- **Full synchronization** – Symantec Brightmail Gateway performs a full synchronization from an LDAP source to a Control Center when you initially enable synchronization and whenever scheduled afterwards (default is once every three hours). Because group- and distribution-list membership must be resolved for each user entry, a full LDAP synchronization can take up to several
hours to complete, depending on the number of members in groups and distribution lists. Domino LDAP services fully synchronize every time that synchronization is initiated.

- **Synchronize changes** – After an initial full synchronization, you can choose to schedule periodic synchronization that update only those directory entries that have changed since the last synchronization. By synchronizing changes only, you can reduce the time it takes to process LDAP synchronization. However, synchronizing a large number of changes may take much longer than synchronizing the same number entries using Full synchronization. If your directory deployment typically encounters a large number of changes (for instance, if user entries are updated every time a user logs into a single-sign-on application), you may want to consider using only Full synchronization.

**Warning:** If you use a load balancer, DNS round robin, or other scheme to provide high availability among multiple LDAP server hosts, Symantec Brightmail Gateway may not correctly detect changes published to your directory server if your source's synchronization type is set to Synchronize changes. If you cannot use a specific, single LDAP host for your source, use Full synchronization for its synchronization type.

**Note:** If you need to change Host, Port, base DN, ldap Group filter, User filter, or Distribution List filter after saving an LDAP synchronization source, you must delete the source, add the source including all attributes to be filtered, and perform a full synchronization.

Use the following settings on the Add LDAP Server page (Administration > Settings > LDAP/Add) to configure LDAP synchronization. This section only appears if Synchronization is checked under LDAP Server Usage.

Unlike authentication, routing, and recipient validation sources, LDAP synchronization sources use preset object classes and attributes, which cannot be modified from the Control Center. Use the Synchronization Query Details Auto Fill button to retrieve the values supplied by your LDAP source. Table 17-3 lists the values supplied by the different LDAP directory servers.
Table 17-3 Directory object classes and attributes

<table>
<thead>
<tr>
<th>Directory server</th>
<th>Object classes</th>
<th>Email attributes</th>
<th>Group membership attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>User: user, contact, publicFolder Distribution List: group, msExchDynamicDistributionList Group: group</td>
<td>Primary email: mail Email alias: proxyAddresses</td>
<td>member memberOf</td>
</tr>
<tr>
<td>Exchange 5.5</td>
<td>User: organizationalperson Distribution List: groupOfNames Group: groupOfNames</td>
<td>Primary email: mail Email alias: otherMailBox</td>
<td>member memberOf</td>
</tr>
<tr>
<td>SunONE</td>
<td>User: person Distribution List: groupOfNames, groupOfUniqueNames Group: groupOfNames, groupOfUniqueNames</td>
<td>Primary email: mail Email alias: mailAlternateAddress</td>
<td>member uniqueMember</td>
</tr>
<tr>
<td>Domino</td>
<td>User: dominoPerson, dominoServerMailInDatabase Distribution List: dominoGroup Group: dominoGroup</td>
<td>Primary email: mail Email alias: (*)</td>
<td>member</td>
</tr>
</tbody>
</table>

* Aliases are constructed from the values of the first, last, and short name entries when the Primary Domain and/or Domain Aliases fields are specified.

Where a directory entry qualifies as either a group or a distribution list by virtue of its object class and an email address is present, LDAP synchronization evaluates the entry as a distribution list. If no email address is present, an LDAP synchronization source evaluates the entry as a Group.

Symantec Brightmail Gateway offers limited support for dynamic distribution lists. Dynamic distribution lists, such as those supported by Active Directory in combination with Exchange 2003, are updated when members are added, deleted, or modified in the LDAP source. Symantec Brightmail Gateway synchronization cannot determine or resolve membership in dynamic distribution lists. Nevertheless it maintains the email addresses of all distribution lists, including
memberless distribution lists, as valid addresses in its address-resolution database. Therefore, it delivers email addressed to those distribution lists according to policies configured for them. Symantec Brightmail Gateway does not, however, apply policies for members of a distribution list when mail is addressed to the dynamic distribution list.

Initiating LDAP synchronization

Saving changes to an LDAP synchronization definition initiates a full synchronization. Control Center performance may be diminished while the synchronization is in progress.

To initiate synchronization from an LDAP source to the Control Center

1. Click Status > System > LDAP Synchronization.
2. Click LDAP to CC if it is not already selected.
3. If you want to synchronize fewer than 1,000 changes of LDAP data, click Synchronize Changes.
   See “About LDAP synchronization” on page 481.
4. If you want to synchronize 1,000 changes of LDAP data or more, click Full Synchronization.
5. Ensure that you can replicate data from the Control Center to attached and enabled Scanners with the Replicate now button.
   Begin replication only after initial synchronization has completed successfully.
   If synchronization has not completed successfully, the LDAP Synchronization Status page displays error messages.
   You can delay start of replication to a time when email traffic is less.
   See “Starting or stopping replication” on page 504.

About the LDAP routing service

Symantec Brightmail Gateway’s LDAP routing service queries the LDAP source for user data that the MTA uses to route email messages to external domains specified in the LDAP directory. Set the email alias and/or transport attributes that you want Symantec Brightmail Gateway to use to query the LDAP source for routing information.

For example, you can use LDAP routing to route email addressed to users, such as consultants, who maintain a company email address but who receive mail at an alias on another mail host or at an external domain. You can also configure
LDAP routing by transport attribute, which forwards all email addressed to a specified domain to another, associated mail host.

See “About Configuring LDAP settings and sources” on page 490.

**Note:** If your directory server is Exchange 5.5, you should not use attributes that are not delivered as part of the schema. In other words, use only the attributes provided in the schema.

**Note:** You do not need to configure LDAP authentication and synchronization to use LDAP routing. If LDAP routing is configured, the MTA queries the LDAP source for aliases and/or external domains associated with the address before delivering any inbound email.

The following examples demonstrate the ways in which Symantec Brightmail Gateway constructs routing queries from attribute values. In the case of an Exchange 5.5 directory server, you should only use the attributes supplied by the LDAP schema for your installation.

When using the email alias attribute to construct an email filter, set the email alias attribute to search the LDAP source for either the fully qualified email address or the user ID. For example, consider an example where routing is configured to the following settings:

**Query base:** `dc=example, dc=com`

**Query filter:** `mail`

**Email Alias:** `alternateMailaddress`

- With the Query filter set to `mail=%s`, the system will search the query base for the value of the mail attribute that matches the fully qualified email address of the recipient. For example, assume that the directory includes the following entry for John Doe:

  - Dn: `cn=John Doe, dc=example, dc=com`
  - cn: John Doe
  - alternateMailaddress: qaMgr@symantec.com
  - mail: john_doe@anywhere.com

  Any mail addressed to john_doe@anywhere.com will be forwarded to the address indicated by the value of the alternateMailaddress attribute, i.e., to qaMgr@symantec.com.

- Even without a fully qualified email address, you can configure Symantec Brightmail Gateway to route email based on the user ID portion of the email
address. For example, by changing the query filter to \( (\text{mail}=%u) \), the system searches the query base for the user ID portion of the email address. When Symantec Brightmail Gateway receives any mail addressed to john_doe@anywhere.com or john_doe@somewhere.com, it matches a mail attribute value that is set to john_doe, as in the following example:

- `Dn: cn=John Doe, dc=example, dc=com`
- `cn: John Doe`
- `alternateMailaddress: qaMgr@symantec.com`
- `mail: john_doe`

Mail sent to john_doe@anywhere.com or john_doe@somewhere.com is forwarded to an email alias address value set to qaMgr@symantec.com.

- You can also configure Symantec Brightmail Gateway to route mail to users based solely on the domain name portion of an email address. For example, by changing the query filter to \( (\text{email}=%d) \), the system searches the query base for entries that match the value of the mail attribute. For example, assume that the LDAP directory includes the following entry:

- `Dn: cn=John Doe, dc=example, dc=com`
- `cn: John Doe`
- `alternateMailaddress: qaMgr@symantec.com`
- `mail: anywhere.com`

Email that is addressed to any recipient at anywhere.com, regardless of user ID, to be forwarded to qaMgr@symantec.com

Routing can also be configured to route email to other mail hosts according to the value of a transport attribute. Symantec Brightmail Gateway uses the query filter to search for matches on the mail attribute value and forwards incoming mail to the server identified by the transport attribute.

- For example, assume that the LDAP directory includes a mail attribute value `email` and a transport attribute `mailHost` as in the following entry:

- `cn=John Doe`
- `email=john_doe@anywhere.com`
- `class=Employee`
- `mailHost=incoming.anywhere.com`

A query filter such as `(&(\text{class}=\text{Employee})(\text{email}=%s))` matches mail sent to john_doe@anywhere.com and route it to john_doe@incoming.anywhere.com.

- Assume that the directory includes the following entry:
A query filter set to \((& (class=Employee) (email=%s))\) matches mail addressed to john_doe@anywhere.com or john_doe@somewhere.com and forward it to john_doe@incoming.anywhere.com.

## About recipient validation

Recipient validation lets you validate email recipients without having to enable LDAP synchronization. With an LDAP source configured for recipient validation, messages to invalid recipients are rejected if Reject invalid recipients is enabled. By bypassing synchronization, you can avoid some of the drawbacks of maintaining synchronization, including the time it takes to synchronize and replicate LDAP directory data.

See “About Configuring LDAP settings and sources” on page 490.

**Caution:** The LDAP client for recipient validation resides on the Scanner, not on the Control Center (as it does for synchronization). Some firewall configuration may be required where a Scanner is deployed within a network DMZ. Contact your network administrator if you plan to configure an LDAP source for recipient validation and the Scanner resides between two firewalls—one separating the Scanner from the Internet and one separating the Scanner from the Control Center and an internal mail server.

Once you have enabled recipient validation for an LDAP source, you must click the Reject invalid recipient check box on the Invalid Recipient Handling page (Protocols > SMTP > Invalid Recipients) and the Enable Recipient Validation for this domain check box on the Edit Domains page (Protocols > SMTP > Domains > Edit).

See “Configuring invalid recipient handling” on page 88.

See “Adding or editing local domains” on page 81.

**Note:** An LDAP source that is configured for recipient validation can only be used to reject email addressed to invalid recipients. If you want Symantec Brightmail Gateway to drop messages to invalid recipients, you must configure an LDAP source for synchronization.
When using the email alias attribute to construct an email filter, set the email alias attribute to search the LDAP source for either the fully qualified email address or the user ID. Consider an example where recipient validation is configured to the following settings:

**Query base:** dc=example, dc=com

**Primary email attribute:** mail

- With the Query filter set to mail=%s, the system searches the query base for the value of the mail attribute that matches the fully qualified email address of the recipient. For example, assume that the directory includes the following entry for John Doe:

  Dn: cn=John Doe, dc=example, dc=com
  cn: John Doe
  mail: john_doe@anywhere.com

  Symantec Brightmail Gateway validates mail addressed to john_doe@anywhere.com, because the query filter (mail=john_doe@anywhere.com) matches for the cn=John Doe entry above.

- Without a fully qualified email address available on directory entries, you can configure Symantec Brightmail Gateway to validate email based on the user ID portion of the email address. For example, by changing the query filter to (uid=%u), the system searches the query base for the user ID portion of the email address. When Symantec Brightmail Gateway receives any mail addressed to john_doe@anywhere.com or john_doe@somewhere.com, it results in a search on the directory with a query filter of (uid=john_doe), which would match the following directory entry:

  Dn: cn=John Doe, dc=example, dc=com
  cn: John Doe
  uid: john_doe
  mail: johnathan.doe@anywhere.com

  Mail sent to john_doe@anywhere.com or john_doe@somewhere.com is validated. Symantec Brightmail Gateway, however, does not change the recipient address to the primary email address. Note that, with the primary email attribute set to mail, the matching entry must have at least one value set to mail in order to be considered valid. If the directory entries in this example did not include mail attribute values, the primary email attribute could be changed to uid, resulting in all (uid=%u) matches in this example being considered valid.

- You can also configure Symantec Brightmail Gateway to validate recipients based solely on the domain name portion of an email address. For example,
by changing the query filter to domain=%d and the primary email attribute to domain, and given that the LDAP directory includes the following entry:

Dn: domain=anywhere.com, dc=example, dc=com
domain: anywhere.com

Email that is addressed to any recipient at anywhere.com, is considered a valid recipient.

About Configuring LDAP settings and sources

You configure and edit your LDAP settings and sources using the LDAP Settings page and then use Detail pages to configure the specifics of your LDAP sources. You can configure multiple LDAP synchronization, routing, and recipient validation sources, but you can only configure one authentication source per Control Center.

Authentication and synchronization or recipient validation sources are typically configured to cover the same part of an LDAP directory, but you can configure different sources for different parts of the same directory or for different directories altogether.

By specifying a different base Distinguished Name (base DN) as the starting point for queries that Symantec Brightmail Gateway runs against the LDAP source, you can divide LDAP directory information among multiple LDAP sources.

Specifying a more restrictive base DN can shorten the time it takes to process queries. The base DN or the search queries of multiple LDAP synchronization or recipient validation sources using the same directory should differ so that primary email entries do not overlap. Group and distribution-list memberships can span multiple synchronization or recipient validation sources.

The following suggestions can help you determine how you want to configure your sources:

- Configure a synchronization source when you require recipient validation and you want to drop invalid recipients. Configure a recipient validation source when you do not need synchronization services and want to reject invalid recipients.
  See “Configuring invalid recipient handling” on page 88.

- Depending on LDAP usage, you can configure various attributes that Symantec Brightmail Gateway uses to query the LDAP source. You can use the Auto Fill button to supply default values for these attributes, or you can supply attribute values that Symantec Brightmail Gateway uses to construct queries. For email routing using Exchange 5.5, use only those attributes supplied by the LDAP source.
Unlike authentication, routing, or recipient validation sources, LDAP synchronization sources do not permit you to fully modify the attributes used to construct the query. See Table 17-3 on page 484.

- If you plan to use your organization's LDAP directory data to authenticate end-user access to Spam Quarantine or validate email-recipient addresses stored in Spam Quarantine, you need to configure an LDAP source for authentication. See “About the authentication service” on page 480.

- If you want Symantec Brightmail Gateway to drop invalid recipient email, detect directory harvest attacks, expand distribution lists, and resolve group and distribution-list memberships for policies, you need to configure a synchronization LDAP source, synchronize the LDAP source directory with the Control Center's data stores, and replicate directory data to attached and enabled Scanners. Synchronization and replication can result in significant processing overhead that may delay scanning of email. If you only need an LDAP source to handle invalid recipients or detect directory harvest attacks, consider configuring a recipient validation LDAP source instead. See “About LDAP synchronization” on page 481.

**Note:** If you plan to allow end users to configure personal Good and Bad Sender lists or personal language settings, you need to configure an LDAP source for both authentication and synchronization.

- If you want Symantec Brightmail Gateway to route incoming email to aliases and remote domains, you need to configure an LDAP source for routing. See “About the LDAP routing service” on page 485.

- If you want Symantec Brightmail Gateway to reject invalid-recipient email or detect directory harvest attacks, you need configure an LDAP source for recipient validation. You do not need to configure a synchronization source when you enable a recipient validation source unless you want Symantec Brightmail Gateway to also drop invalid recipients for some domains. See “About recipient validation” on page 488.

Keep the following additional issues in mind when configuring LDAP settings:

- If you attempt to save an authentication source with a Login query that does not include the Login attribute or does not contain the Primary email or email alias attributes, the Control Center warns you that it may not be able to resolve users or distribution lists correctly. However, you are not prevented from saving the source with that query.
The LDAP term "alias" should not be confused with its use as the Windows term for "distribution list." The LDAP email alias attribute contains one or more alternative email addresses for a user or distribution list. Messages addressed to a distribution list are expanded and delivered to each member of the distribution list group. A message sent to an LDAP email alias, on the other hand, is simply delivered to that entity (if a user, to the user's email box, and if a distribution list, to the list's members).

Symantec Brightmail Gateway administrators who use the Windows Active Directory LDAP directory service may first need to modify LDAP administrator permissions to enable the Control Center to log on to Active Directory using the Administrator Credential's Name (bind DN) setting. You need to make this modification if the following conditions are true:

- If your Bind DN entry does not have the same read and list permissions as a regular administrative entry; for example, if it is not a member of the Administrators or Domain Admins groups in Active Directory.
- You anticipate using Synchronize changes to update Control Center email directory data stores. Synchronize changes polls the LDAP directory for changes made since the last synchronization and may miss Active Directory deletions held in its deleted objects container. Full synchronization, on the other hand, first clears the Control Center email directory data stores, then recopies the entire directory from the LDAP source, so any deletions are detected implicitly. However, in most cases full synchronization takes longer to complete.

Download and install the ADAM Administration Tools (available from Microsoft Support) to modify Active Directory permissions to add a non–Active Directory administrator DN to the list of security principals allowed to log on. Log on to ADAM as a member of the Domain Admins group and navigate to the ADAM Tools Command Prompt. Use the `dsacls` command with the name of the deleted objects container for your domain and the `takeownership` argument. For example:

```
    dsacls "CN=Deleted Objects,DC=MyDomain,DC=com" /takeownership
```

Once ADAM Administration Tools returns output, use the `dsacls` command again to add your DN to the list of allowed principals granted permissions to view the contents of the deleted objects container. For example:

```
    dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /g

    MyDomain\MyDistinguishedName:LCRP
```

The List Contents (LC) and Read Property (RP) permissions are equivalent to Active Directory's default permissions Administrators group and do not allow you to modify the contents of the deleted objects container. For detailed instructions, consult the Microsoft Support page from which you downloaded ADAM Administration Tools.
If you see the error Failed to create user mappings for source during server creation, and you have recently changed DNS servers, restart your LDAP synchronization components. Log in as the admin user and issue the following command:

```
service ldapsync restart
```

Then, repeat the procedure for adding an LDAP source.

If an LDAP source connection fails or if an LDAP query returns more than one email recipient, then spam messages bound for Spam Quarantine are held in the Scanner's deferred queue.

See “About replicating data to Scanners” on page 504.

---

### Configuring LDAP settings and adding source definitions

You can configure multiple LDAP synchronization, routing, and recipient validation sources. However, you can only configure one authentication source per Control Center.

See “About Configuring LDAP settings and sources” on page 490.

This topic describes how to configure your LDAP settings and sources. Use this task to configure your basic LDAP settings and sources, then refer to the following topics to provide configuration details for your chosen sources.

See “Configuring authentication source details” on page 496.

See “Configuring synchronization source details” on page 497.

See “Configuring recipient validation source details” on page 500.

#### To configure LDAP settings and adding source definitions

1. In the Control Center, click **Administration > Settings > LDAP**.

2. Check **Enable distribution list expansion** to enable Symantec Brightmail Gateway to validate and resolve distribution list membership. With distribution list expansion enabled, email addressed to a distribution list may trigger different policies, depending on which policies apply to individual member recipients.

   Uncheck **Enable distribution list expansion** to prevent email addressed to a distribution list from triggering policies that apply to individual member recipients.

3. Check **Preserve Recipient Addresses** if you want Symantec Brightmail Gateway to retain the addresses of messages sent to email aliases once the recipient addresses resolve to the primary email addresses of group members.
4 Click **Add**. The **Add LDAP Server** page appears.

5 Enter the necessary information in the **Description**, **Host**, and **Port** fields. The default port value is set to 389, if possible, we suggest changing it to 3268 for improved performance.

6 Select the type of LDAP directory that is appropriate for this source from the **Directory type** drop-down menu.

   See “About the supported LDAP services and directories” on page 477.

7 In the Administrator Credentials section, select either **Anonymous bind**, to bypass the LDAP directory server's authentication mechanism, or select **Use the following**, and specify login information.

   To use anonymous bind to create a synchronization source to a SunONE directory server, you must modify the access control information (aci) attribute to permit anonymous access to the 'cn=changelog' context root if you plan to enable Synchronize changes. Symantec recommends that you contact Technical Support for information on setting access controls for a SunONE synchronization source using anonymous bind to synchronize changes.

   **Warning:** Making directory data accessible using anonymous bind is not a secure practice. Symantec recommends instead that you configure your directory server to require authentication for data access. To use anonymous bind, your LDAP directory must be configured to grant anonymous access to the changelog and base DN. Anyone with anonymous access to the changelog can retrieve information about added, deleted, or modified entries that might otherwise be protected by access controls on the entries themselves. If necessary, anonymous changelog access should be granted only if the entire directory is open to anonymous access so that Test Login can be used to confirm administrator access to the changelog. When an admin with insufficient access attempts a test login against a SunONE synchronization source configured to synchronize changes, the Control Center returns an error message.

   A synchronization source that uses anonymous bind to log into a Domino directory cannot access Group and dlist data.

   Symantec Brightmail Gateway administrators may need to modify Active Directory permissions to enable the Control Center to log on using the Name (bind DN) setting.
If you intend to use Active Directory as an authentication source, you must populate the **Windows Domain Names** field with any Windows Domain names used to log into the Control Center.

Click **Test Login** to confirm that the Control Center can log into the specified LDAP directory.

A verification message in blue appears at the top of the Add LDAP Server page if login is successful. Otherwise a message in red informs you of the reason that the login attempt failed.

Under LDAP Server Usage, check the appropriate **Usage** boxes for this source. You can configure multiple server usages per source but only one authentication source per Control Center. Depending on the directory type and the server usage that you select, additional fields may appear. Only those fields that you need to complete for a particular server usage or combination of server usages appears.

If you intend to use Active Directory as an authentication source, you must populate the **Windows Domain Names** field with any Windows Domain names used to log into the Control Center.

If you use a Domino directory to define a synchronization source, optionally enter primary and secondary Internet domain names. Enter names for either setting that applies to this source definition. **Primary domain** is the domain to which mail is delivered. **Domain aliases** are domain names that resolve to the primary domain. Leaving both fields blank suppresses auto-generation of aliases.

Complete the necessary query details for defining an LDAP source or click **Auto Fill** to retrieve default attribute values.

Attributes differ depending on usage. See the Query Details table appropriate to the usage for this source.

See “Configuring authentication source details” on page 496.

See “Configuring synchronization source details” on page 497.

See “Configuring routing source details” on page 499.

See “Configuring recipient validation source details” on page 500.

Click **Test** to validate queries.

Note that when you validate queries in this manner, only the first 1000 results are displayed.

For a routing source, check **Enable MX lookup for transport** if you want Symantec Brightmail Gateway to locate a domain name using MX Lookup.
For a synchronization source, indicate the type of synchronization and schedule the frequency with which you want to synchronize the LDAP directory with Control Center data stores.

Click **Save**.

Saving an LDAP synchronization source definition initiates full synchronization. Control Center performance may be diminished while the synchronization is in progress.

**Note:** If you defined an LDAP source for synchronization and want to drop invalid recipients or if you defined an LDAP source for recipient validation and want to reject invalid recipients, you must configure invalid recipient handling.

See “Configuring invalid recipient handling” on page 88.

### Configuring authentication source details

Use the Add LDAP Server page to define an LDAP source and to select the LDAP services that are appropriate for your organization.

See “Configuring LDAP settings and adding source definitions” on page 493.

If you configure an authentication source, you must also provide the appropriate query details as described in this section.

**Note:** You should allow up to four hours for any changes you make to the LDAP source to be reflected in the Control Center's LDAP cache. If you require an immediate refresh, restart the Control Center.

See “About the authentication service” on page 480.

See “About Configuring LDAP settings and sources” on page 490.

**Table 17-4** Add LDAP Server—Authentication Query Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Fill</td>
<td>Places default values in the fields for you to modify as needed. You can have only one authentication server defined in the Control Center.</td>
</tr>
<tr>
<td>Query start (Auth base DN)</td>
<td>Designates the point in the directory from which to start searching for entries to authenticate. If an entry contains an ampersand, you must escape the ampersand with a backward slash () so that it is read as a literal character. e.g.: ou=Sales &amp; Marketing,dc=company,dc=com</td>
</tr>
</tbody>
</table>
Table 17-4 Add LDAP Server—Authentication Query Details (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login attribute</td>
<td>Specifies the attribute that identifies a directory entry representing a person.</td>
</tr>
<tr>
<td>Primary email attribute</td>
<td>Finds users based on the attribute which represents a mailbox.</td>
</tr>
<tr>
<td>Email alias attribute</td>
<td>Finds users based on the attribute representing an alternative address for the entities' mailbox.</td>
</tr>
</tbody>
</table>
| Login query           | Finds users and distribution lists based on their Login and Primary and Email alias attributes.  
Create a query from the Login and email attributes that should return a single entry from the LDAP directory.  
If the directory returns no results or if it returns more than one result, the recipient address is left unresolved and the user is not allowed to log in. |
| Test                  | Attempts to execute the query as defined.                                                                                                   |

Configuring synchronization source details

You can provide Scanner access to LDAP directory information by synchronizing LDAP user, alias, group, and distribution-list data with the Control Center's own directory data stores.

Use the Add LDAP Server page to define an LDAP source and to select the LDAP services that are appropriate for your organization.

See “Configuring LDAP settings and adding source definitions” on page 493.

If you configure a synchronization source, you must also provide the appropriate query details as described in this section.

See “About LDAP synchronization” on page 481.

See “Configuring LDAP settings and adding source definitions” on page 493.

Table 17-5 Add LDAP Server—Synchronization Query Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto Fill | Obtains default query attributes from the LDAP source. You cannot modify the attributes in User, Group, or Distribution List queries. You can only specify a Custom query start.  
See Table 17-3 on page 484. |
Table 17-5  Add LDAP Server—Synchronization Query Details (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Query start (Sync base DN)          | Designates the point in the directory from which to start searching for entries with email addresses/aliases or groups. To use this field, begin by clicking Auto Fill for the naming contexts of the directory. Reduce the received list of DN’s brought into the field by Auto Fill to a single DN, or write your own DN based on the provided list. If an entry contains an ampersand, do NOT escape the ampersand with a backward slash (\), e.g.:  
ou=Sales & Marketing,dc=company,dc=com |
| Custom query start                  | Allows for the addition of a customized query start (base dn).                                                                                                                                      |
| User Query                          | Finds users in the LDAP source. Test checks to see that your Custom/User query works.                                                                                                               |
| Group Query                         | Finds LDAP groups in the LDAP source. Test checks your Group query to see that it works.                                                                                                              |
| Distribution List Query             | Finds distribution lists in the LDAP source. Test checks to see that your Distribution query works.                                                                                                  |
| Synchronization Type                | Indicates whether to perform Full Synchronization or to Synchronize Changes only.                                                                                                                     |
| Synchronize every                   | Specifies how often scheduled synchronization occurs. You can specify a number of minutes, hours, or days. The default is every 3 hours.                                                              |
| Audit level                         | Verbosity setting for LDAP audit logs. Choices of Off, Low, and Verbose are available. The default is Off.                                                                                          |
Table 17-5  Add LDAP Server—Synchronization Query Details (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page size</td>
<td>If you selected Domino as your Directory Type, this option does not display. Domino does not implement paged searching. Specifies the number of entries the LDAP source should return for each page of results from a search query. Setting this value too low can impede performance; setting it too high can cause synchronization to fail if the page size exceeds the limit set by the LDAP server. The default server-side limit for this value varies according to directory type:  ■ Active Directory: 1000  ■ SunONE: 100 (Recommended: 0)  ■ Exchange 5.5: 100  To change this limit on your directory server, see your directory server documentation. To disable paged searching entirely, set this value to 0. 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.</td>
</tr>
</tbody>
</table>

Configuring routing source details

Use the Add LDAP Server page to define an LDAP source and to select the LDAP services that are appropriate for your organization.

See “Configuring LDAP settings and adding source definitions” on page 493.

If you configure a routing source, you must also provide the appropriate query details as described in this section.

These detail fields appear on the Add LDAP Server page (Administration > Settings > LDAP > Add) when routing is checked under LDAP Server Usage.

See “About Configuring LDAP settings and sources” on page 490.

See “About the LDAP routing service” on page 485.

See “Configuring LDAP settings and adding source definitions” on page 493.

Table 17-6  Add LDAP Server—Routing Query Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Fill</td>
<td>Places default values in the fields for you to modify as needed.</td>
</tr>
</tbody>
</table>
Table 17-6  Add LDAP Server—Routing Query Details (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Query start (Routing base DN)       | Designates the point in the directory from which to start searching for entries to be routed elsewhere. If an entry contains an ampersand, you must escape the ampersand with a backward slash (\) so that it is read as a literal character:  
  ou=Sales \& Marketing,dc=company,dc=com |
| Query filter                        | Describes the LDAP search criteria and tells the MTA how to match the email address of a recipient with a specific LDAP record. For example, email=%s describes a filter that finds a record with an attribute named email that matches the %s format (example@company.com). A more complex filter can look only for records of a certain class or that have other attributes set. The following formats are available:  
  ■ %s – Email address to find, including user ID and fully-qualified domain name  
  ■ %u – User ID portion of the email address to find  
  ■ %d – Domain portion of the email address to find |
| Email alias attribute               | Names the attribute that is used for alternate email address for primary user's mailbox. If this attribute is present, mail is delivered to that address or the value of this attribute. If left blank, no email aliasing takes place. |
| Transport attribute                 | Names the attribute in the record that specifies which mail server to use for that person. For transport routing lookups, this field in the LDAP database must contain the host name of the next hop for email delivery. If left blank, no LDAP-based transport routing is performed for this source. |
| Enable MX Lookup for transport      | Allows MX lookup for the specified transport.                                                                                                                                                              |

Configuring recipient validation source details

Use the Add LDAP Server page to define an LDAP source and to select the LDAP services that are appropriate for your organization.

See “Configuring LDAP settings and adding source definitions” on page 493.

If you configure a recipient validation source, you must also provide the appropriate query details as described in this section. Recipient validation uses the same query syntax as LDAP routing.
See “About Configuring LDAP settings and sources” on page 490.
See “About recipient validation” on page 488.

Table 17-7  Add LDAP Server—Recipient Validation Query Details

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Fill</td>
<td>Places default values in the fields for you to modify as needed.</td>
</tr>
<tr>
<td>Query start (Access base DN)</td>
<td>Designates the point in the directory from which to start searching for entries to be routed elsewhere. If an entry contains an ampersand, you must escape the ampersand with a backward slash () so that it is read as a literal character: ou=Sales &amp; Marketing,dc=company,dc=com</td>
</tr>
</tbody>
</table>
| Query filter                | Describes the LDAP search criteria and tells the MTA how to match the email address of a recipient with a specific LDAP record. For example, email=%s describes a filter that finds a record with an attribute named email that matches the %s format (example@company.com). A more complex filter can look only for records of a certain class or that have other attributes set. The following formats are available:  
  ■ %s – Email address to find, including user ID and fully-qualified domain name  
  ■ %u – User ID portion of the email address to find  
  ■ %d – Domain portion of the email address to find |
| Primary email attribute     | Finds users based on the attribute which represents a mailbox.             |

Editing an LDAP source definition

You can edit an existing LDAP source definition's Administration Credentials; authentication, routing, or recipient validation query details; and the synchronization schedule of an existing LDAP source definition. You cannot, however, change the LDAP Server details (Description, Host, Port, and Directory fields), synchronization query details, or synchronization type or page size. If you need to change any of these elements of a source definition, you need to add a new LDAP source definition.
To edit an LDAP source definition

1. If you are editing a synchronization source definition, in the Control Center, click Status > System > LDAP Synchronization. Otherwise, proceed to 5.
2. If a synchronization of the LDAP source that you want to edit is in progress, click Cancel Synchronization on the LDAP to CC tab or wait until synchronization has completed and the Status column indicates synchronization was successful.
3. Click the CC to Scanners tab to view replication status.
4. If replication is in progress for attached and enabled Scanners, click Cancel Replication or wait until replication has completed and the Status column indicates replication was successful.
5. In the Control Center, click Administration > Settings > LDAP.
6. Check the box beside the name of the LDAP source whose definition you want to edit and click Edit or click the corresponding numbered link.
   The Edit LDAP Server page appears.
7. Modify the Administration Credentials and query details according to your new requirements.
   If you are editing a synchronization source definition, you cannot edit the query details. You can change the synchronization schedule.
8. Click Test Login to validate the new Administrator credentials.
9. If login was successful, click Test for those query details that you have modified.
10. Click Save.

You must manually initiate Full synchronization for changes to a synchronization source to take effect. For large organizations, full synchronization may affect peak performance and is best scheduled for off-peak hours.

See “Initiating LDAP synchronization” on page 485.

You must also replicate synchronized data to attached and enabled Scanners.

See “About replicating data to Scanners” on page 504.

Saving edits to other source definitions may result in some false positives during scanning until your LDAP directory data refreshes.

Enabling or disabling an LDAP source

Enable and Disable buttons let you connect to or disconnect from LDAP source definitions.
Note: If you must disable an LDAP synchronization source while a synchronization process is in progress, you must first cancel the synchronization and then disable the LDAP source.

To enable or disable an LDAP source

1. From the Control Center, click **Status > System > LDAP Synchronization**.

2. Check the box that is adjacent to the name of the LDAP source that you want to disable or enable.

   A green check mark indicates an enabled LDAP source. A black dash indicates a source that is disabled.

3. Click **Enable** or **Disable** as appropriate.

Deleting an LDAP source

You cannot delete a synchronization source while synchronization is running. To check if a synchronization process is under way, click **Status > LDAP Synchronization**.

Note: If you need to change the IP address of your LDAP server, you must delete the LDAP source using the Control Center before changing the IP address of the LDAP server machine, and then re-add the LDAP source from the Control Center using the new IP address.

You cannot delete a synchronization source when Drop invalid recipients is enabled for a local domain. You cannot delete a recipient validation source if Reject invalid recipients is enabled for a local domain.

To delete an LDAP source

1. In the Control Center, click **Status > System > LDAP Synchronization**.

   Check to make sure that no synchronization or replication process is running before you delete a synchronization server.

2. Click **Administration > Settings > LDAP**.

3. Choose one or more LDAP source definitions from the list.

4. Click **Delete**.
A dialog box appears asking you to confirm deletion of the LDAP source. Click OK to proceed with deleting the source or Cancel to cancel the deletion.

If you are deleting an authentication or synchronization source, a second dialog box informs you that deleting an LDAP source also deletes user preferences associated with the LDAP source. Click OK to continue deleting only if you want to delete user preferences as well. Click Cancel if you want to preserve user preferences and continue deleting the non-routing LDAP source. Clicking Cancel does not cancel LDAP source deletion. It only preserves user preferences associated with a non-routing source. Closing the dialog box without clicking OK or Cancel results in LDAP source deletion.

(Authentication and synchronization only) If you clicked OK, a second dialog box informs you that deleting an LDAP source also deletes user preferences associated with the LDAP source. Click OK to continue deleting only if you want to delete user preferences as well. Click Cancel if you want to preserve user preferences and continue deleting the LDAP source.

About replicating data to Scanners

After an LDAP source has been defined to the Control Center, and after the synchronization of LDAP data between the LDAP source and the Control Center has successfully completed one full cycle, LDAP data must be replicated to all attached and enabled Scanners.

For replication to work properly, you must have configured, enabled, and scheduled Scanner replication and made certain that Scanner replication is enabled for each Scanner.

See “Replicating data between the Control Center and your Scanners” on page 455.

Replication will not complete until at least one LDAP synchronization source is available and synchronization has completed successfully. Until this happens, there is no data that replication can use to update Scanners.

See “Starting or stopping replication” on page 504.

See “Configuring recipient validation source details” on page 500.

Starting or stopping replication

You may occasionally need to start or stop replication manually.
To start a manual replication cycle

1. In the Control Center, click **Status > System > LDAP Synchronization**.
2. Click **CC to Scanners** if it is not already selected.
3. Click **Replicate Now**.

To stop a replication in progress

1. In the Control Center, click **Status > Synchronization > CC to Scanners** tab.
2. Click **Cancel Replication**.

Troubleshooting replication

The following procedures can help you troubleshoot replication problems.

**Basic troubleshooting procedure**

1. Verify that synchronization has occurred.
2. If a successful synchronization has not occurred, check your replication status and take one or more of the actions described below.

**To verify that synchronization has completed successfully**

1. In the Control Center, click **Status > LDAP Synchronization > LDAP to CC** tab.
2. Check the Status column for a Success message.
   
   See “Synchronization status information” on page 396.

**To check replication status**

1. In the Control Center, click **Status > LDAP Synchronization > CC to Scanners** tab.
2. Check the Status column for each attached and enabled Scanner on the list.
   
   See “Replication status information” on page 401.

Troubleshooting status messages

If the Scanner has a Status of Success, all attached and enabled Scanners are fully updated with LDAP information and no action is required.

Otherwise, consider the following alternatives:

- If a message is displayed indicating that replication has been canceled and was not canceled via **Status > LDAP Synchronization > LDAP to CC** and clicking **Cancel Synchronization**, an LDAP synchronization source was found. Either synchronization has not yet completed, or synchronization has failed.
Perform one of the following actions:

- Check your synchronization status. See “To check replication status” on page 505.

- Check the Control Center log for errors about creating or moving synchronization data within the Control Center, or errors regarding communication between the Control Center and a Scanner. Check LDAP synchronization logs for any errors that occur in transforming data from the Control Center database to a Scanner database.

- If you see the message No scanners configured for replication, make sure you have successfully added an LDAP synchronization server, that the initial synchronization service has completed successfully, that you have enabled global replication under Scanner Replication on the Administration > Settings > Control Center page, and that replication is enabled on at least one attached and enabled Scanner on the Services tab at Administration > Settings > Hosts/Edit.

- To resolve a replication process with a message of In-Progress, perform a manual replication from the Control Center. If replication still stalls, restart the Control Center software and begin the entire cycle again with a full synchronization.
Action and verdict combinations

This appendix includes the following topics:

- Limits on combining actions
- Action processing combinations
- User interface action combinations
- Verdict combinations

Limits on combining actions

Symantec Brightmail Gateway includes two kinds of limitations on action combinations:

| Limitations imposed by message processing | Table A-2 shows these limitations. |
| Limitations imposed by the Control Center user interface | Table A-3 shows these limitations. Note that these limitations apply when you are creating a policy. When more than one policy applies to a message, additional combinations can result that exceed these limitations. |

Action processing combinations

In general, the actions invoked by each policy determine how a message is processed, not the policies themselves. However, there are exceptions to this rule.
Actions invoked by end-user Good and Bad Senders groups override all actions except those actions invoked by compliance policies.

See “Verdict combinations” on page 512.

**Note:** If two actions are both the result of content compliance policies, additional restrictions on their combination apply.

See “About multiple content compliance policies” on page 63.

Table A-1 shows the processing category for each action. Use the processing category to find the action in Table A-2.

### Table A-1 Action processing categories

<table>
<thead>
<tr>
<th>Processing Category</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Defer SMTP Connection, Reject SMTP Connection, Reject messages failing bounce attack validation</td>
</tr>
<tr>
<td>Event</td>
<td>Archive the message, Create an incident (without holding for review), Forward a copy of the message, Send a bounce message, Send notification</td>
</tr>
<tr>
<td>Delay</td>
<td>Create an incident and hold message for review, Hold message in Suspect Virus Quarantine, Strip and Delay in Suspect Virus Quarantine</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete message</td>
</tr>
<tr>
<td>Modify</td>
<td>Add a header, Add annotation, Add BCC recipients, Clean the message, Deliver the message to the recipient’s Spam folder, Deliver message with TLS encryption, Modify the subject line, Remove unresolved recipients, Strip attachments</td>
</tr>
<tr>
<td>Route</td>
<td>Hold message in Spam Quarantine, Route the message</td>
</tr>
<tr>
<td>No action</td>
<td>Deliver message normally</td>
</tr>
</tbody>
</table>

Table A-2 shows how actions in processing categories combine. Actions are listed according to their processing category. Match an action-processing category in the left-hand column with an action-processing category in the top row to see how actions in those processing categories combine. Actions whose names begin with Treat as are processed according to the action specified by the policy to which they refer. For example, the Treat as a virus action is processed according to the action specified by your virus policy. Actions whose names begin with Bypass are subject only to the limitations described in Table A-3.
Special rules apply when combining routing and modify actions, as follows:

- If one action is Hold message in Spam Quarantine and one is Route the message, the message is moved to Spam Quarantine.
- If both actions are Hold message in Spam Quarantine, the message is moved to Spam Quarantine.
- If both actions are Route the message, the message is routed to the routing address that appears first in an alphanumeric sort.
- When combining Route and Modify actions, if one action is Hold message in Spam Quarantine and one action is Deliver message with TLS encryption, the TLS encryption does not take place.

### Table A-2

<table>
<thead>
<tr>
<th></th>
<th>Firewall</th>
<th>Event</th>
<th>Delay</th>
<th>Delete</th>
<th>Modify</th>
<th>Route</th>
<th>No action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
<td>Firewall</td>
</tr>
<tr>
<td>Event</td>
<td>Firewall</td>
<td>Event + delay</td>
<td>Event + delay</td>
<td>Delete + event</td>
<td>Modify + event</td>
<td>Route + event</td>
<td>Event</td>
</tr>
<tr>
<td>Delay</td>
<td>Firewall</td>
<td>Event + delay</td>
<td>Delay</td>
<td>Delete</td>
<td>Delay, defer modification</td>
<td>Delay, defer routing</td>
<td>Delay</td>
</tr>
<tr>
<td>Delete</td>
<td>Firewall</td>
<td>Delete + event</td>
<td>Delete</td>
<td>Delete</td>
<td>Delete</td>
<td>Delete</td>
<td>Delete</td>
</tr>
<tr>
<td>Modify</td>
<td>Firewall</td>
<td>Modify + event</td>
<td>Delay, defer modification</td>
<td>Delete</td>
<td>Modify + modify</td>
<td>Modify + route</td>
<td>Modify</td>
</tr>
<tr>
<td>Route</td>
<td>Firewall</td>
<td>Route + event</td>
<td>Delay, defer routing</td>
<td>Delete</td>
<td>Modify + route</td>
<td>One route wins</td>
<td>Route</td>
</tr>
<tr>
<td>No action</td>
<td>Firewall</td>
<td>Event</td>
<td>Delay</td>
<td>Delete</td>
<td>Modify</td>
<td>Route</td>
<td>No action</td>
</tr>
</tbody>
</table>

## User interface action combinations

Table A-3 describes the limitations on combining actions within a filtering policy. These limitations are imposed by the Control Center user interface. Note that the Treat as actions are those listed in the last 6 rows of the table.

When you create a policy, the Control Center user interface imposes the limitations described in Table A-3. More than one policy can impact a message. Therefore, these limitations can be exceeded for a particular message. The limitations described in Action processing combinations cannot be exceeded.
### Table A-3  Compatibility of filtering actions by verdict

<table>
<thead>
<tr>
<th>Action</th>
<th>Compatibility with other actions</th>
<th>Can add multiple times?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a header</td>
<td>Any except Delete message, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>Yes</td>
</tr>
<tr>
<td>Add annotation</td>
<td>Any except Delete message, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Add BCC recipients</td>
<td>Any except Delete message, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>Yes</td>
</tr>
<tr>
<td>Archive the message</td>
<td>Any except Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Bypass compliance policy</td>
<td>Any except Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>Yes. One per compliance policy.</td>
</tr>
<tr>
<td>Bypass spam scanning</td>
<td>Any except Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Clean the message</td>
<td>Any except Delete message, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Create an incident (without Hold message for review option)</td>
<td>Any except Delete message, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>Yes</td>
</tr>
<tr>
<td>Create an incident (with Hold message for review option checked)</td>
<td>Can only be combined with Send notification.</td>
<td>No</td>
</tr>
<tr>
<td>Defer SMTP Connection</td>
<td>Cannot be used with other actions</td>
<td>No</td>
</tr>
<tr>
<td>Delete message</td>
<td>Send a bounce message, Send notification, Archive the message, Create an incident, Forward a copy of the message, Bypass compliance policy, Bypass spam scanning</td>
<td>No</td>
</tr>
<tr>
<td>Deliver message normally</td>
<td>Any except Hold message in Suspect Virus Quarantine, Delete message, Hold message in Spam Quarantine, Strip and Delay in Suspect Virus Quarantine, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Deliver the message to the recipient’s Spam folder</td>
<td>Any except Delete message, Defers SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Action</td>
<td>Compatibility with other actions</td>
<td>Can add multiple times?</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Deliver message with TLS encryption</td>
<td>Any except Delete message, Deliver message normally, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Forward a copy of the message</td>
<td>Any except Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>Yes</td>
</tr>
<tr>
<td>Hold message in Spam Quarantine</td>
<td>Any except Hold message in Suspect Virus Quarantine, Deliver the message normally, Delete message, Route the message, Strip and Delay in Suspect Virus Quarantine, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If used with Deliver the message to the recipient's spam folder, affected messages are quarantined. If released from Spam Quarantine, messages are delivered to the recipient's Spam folder.</td>
<td>No</td>
</tr>
<tr>
<td>Hold message in Suspect Virus Quarantine</td>
<td>Any except Delete message, Deliver message normally, Hold message in Spam Quarantine, Strip and Delay in Suspect Virus Quarantine, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Modify the subject line</td>
<td>Any except Delete message, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>One for prepend and one for append</td>
</tr>
<tr>
<td>Reject messages failing bounce attack validation</td>
<td>Cannot be used with other actions</td>
<td>No</td>
</tr>
<tr>
<td>Reject SMTP Connection</td>
<td>Cannot be used with other actions</td>
<td>No</td>
</tr>
<tr>
<td>Remove unresolved recipients</td>
<td>Any except Delete message, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Route the message</td>
<td>Any except Delete message, Defer SMTP Connection, Hold message in Spam Quarantine, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Send a bounce message</td>
<td>Any except Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Send notification</td>
<td>Any except Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table A-3  Compatibility of filtering actions by verdict (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Compatibility with other actions</th>
<th>Can add multiple times?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strip and Delay in Suspect Virus Quarantine</td>
<td>Any except Delete message, Deliver the message normally, Hold message in Spam Quarantine, Hold message in Suspect Virus Quarantine, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>No</td>
</tr>
<tr>
<td>Strip attachments</td>
<td>Any except Delete message, Defer SMTP Connection, Reject SMTP Connection, Treat as actions</td>
<td>Yes</td>
</tr>
<tr>
<td>Treat as a bad sender</td>
<td>Cannot be used with other actions.</td>
<td>No</td>
</tr>
<tr>
<td>Treat as a mass-mailing worm</td>
<td>Cannot be used with other actions.</td>
<td>No</td>
</tr>
<tr>
<td>Treat as a good sender</td>
<td>Cannot be used with other actions. When used in a compliance policy, messages that match the policy will not be scanned for spam.</td>
<td>No</td>
</tr>
<tr>
<td>Treat as a virus</td>
<td>Cannot be used with other actions.</td>
<td>No</td>
</tr>
<tr>
<td>Treat as spam</td>
<td>Cannot be used with other actions.</td>
<td>No</td>
</tr>
<tr>
<td>Treat as suspected spam</td>
<td>Cannot be used with other actions.</td>
<td>No</td>
</tr>
</tbody>
</table>

### 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 and Bad Sender Groups
- Global Good and Bad Sender Groups

These actions occur before the Brightmail Engine processes the messages.

See “How Symantec Brightmail Gateway works” on page 28.

During connection processing, certain steps can be skipped, as shown in Table A-4.
### Table A-4  Connection-time good sender processing

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>Symantec Brightmail Gateway 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 143. See Table 3-1 on page 54.

During Brightmail Engine message processing, certain steps may be skipped, as shown in Table A-5 and Table A-6.

### Table A-5  Brightmail Engine inbound message processing

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>Symantec Brightmail Gateway does not check for any of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third Party Good Senders</td>
<td>Third Party Bad Senders</td>
</tr>
<tr>
<td></td>
<td>Spam</td>
</tr>
<tr>
<td></td>
<td>Suspected spam</td>
</tr>
<tr>
<td></td>
<td>Sender authentication failure</td>
</tr>
<tr>
<td>Local Good Sender Domains</td>
<td></td>
</tr>
<tr>
<td>Local Good Sender IPs</td>
<td></td>
</tr>
<tr>
<td>Content compliance policy with a Bypass spam scanning action</td>
<td></td>
</tr>
<tr>
<td>Content compliance policy with a Treat as good sender action</td>
<td></td>
</tr>
<tr>
<td>Symantec Global Good Senders</td>
<td></td>
</tr>
<tr>
<td>End user Good Senders List</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Third Party Bad Senders</td>
</tr>
<tr>
<td></td>
<td>Spam</td>
</tr>
<tr>
<td></td>
<td>Suspected spam</td>
</tr>
<tr>
<td></td>
<td>Sender authentication failure</td>
</tr>
<tr>
<td></td>
<td>Symantec Global Bad Senders</td>
</tr>
</tbody>
</table>
### Table A-5  Brightmail Engine inbound message processing (continued)

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>Symantec Brightmail Gateway does not check for any of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Good Sender IPs</td>
<td>Local Bad Sender IPs</td>
</tr>
<tr>
<td>Content compliance policy with a Treat as a good sender action</td>
<td>Local Bad Sender Domains</td>
</tr>
<tr>
<td>End user Good Senders List</td>
<td></td>
</tr>
<tr>
<td>Local Good Sender Domains</td>
<td>Local Bad Sender Domains</td>
</tr>
<tr>
<td>Spam</td>
<td>Suspected spam</td>
</tr>
<tr>
<td>When the associated policy specifies a Bypass compliance policy action:</td>
<td>All content compliance policies or those content compliance policies specified in the policy</td>
</tr>
<tr>
<td>■ Local Good Sender Domains</td>
<td></td>
</tr>
<tr>
<td>■ Local Good Sender IPs</td>
<td></td>
</tr>
<tr>
<td>■ Third Party Good Senders</td>
<td></td>
</tr>
<tr>
<td>■ Local Bad Sender Domains</td>
<td></td>
</tr>
<tr>
<td>■ Local Bad Sender IPs</td>
<td></td>
</tr>
<tr>
<td>■ Third Party Bad Senders</td>
<td></td>
</tr>
<tr>
<td>■ Symantec Global Good Senders</td>
<td></td>
</tr>
<tr>
<td>■ Symantec Global Bad Senders</td>
<td></td>
</tr>
<tr>
<td>■ Spam</td>
<td></td>
</tr>
<tr>
<td>■ Suspected spam</td>
<td></td>
</tr>
<tr>
<td>■ Sender authentication failure</td>
<td></td>
</tr>
</tbody>
</table>

### Table A-6  Brightmail Engine outbound message processing

<table>
<thead>
<tr>
<th>If any of these match:</th>
<th>Symantec Brightmail Gateway does not check for any of these:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content compliance policy with a Bypass spam scanning action</td>
<td>Spam</td>
</tr>
<tr>
<td></td>
<td>Suspected spam</td>
</tr>
<tr>
<td>When the associated policy specifies a Bypass compliance policy action:</td>
<td>All content compliance policies or those content compliance policies specified in the policy</td>
</tr>
<tr>
<td>■ Spam</td>
<td></td>
</tr>
<tr>
<td>■ Suspected spam</td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td>Suspected spam</td>
</tr>
</tbody>
</table>
This appendix includes the following topics:

- Described Content Compliance policy templates
- Structured Data Compliance policy templates
- Regular expressions for context-filtering conditions
- Premium attachment list resources
- Premium pattern resources
- Premium dictionary resources
- Premium regular-expression resources keyed to policy templates
- U.S. regulatory policy templates
- Confidential data-protection policy templates
- Acceptable use policy templates
- Customer and employee data-protection templates
- Network security policy templates
- UK and international regulatory policy templates
- Page settings for adding a compliance folder
- Compliance Conditions
- Attachment characteristics for attachment lists
Described Content Compliance policy templates

This section describes the Described Content Compliance policy templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.
## Table B-1
Compliance policy templates (Described Content)

<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy templates</th>
<th>Associated Premium resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. regulatory policies</td>
<td>Export Administration Regulations (EAR)</td>
<td>Dictionaries: EAR Country Codes; EAR CCL Keywords</td>
</tr>
<tr>
<td>See “U.S. regulatory policy templates” on page 542.</td>
<td>Gramm-Leach-Bliley</td>
<td>Dictionaries: US SSN Keywords; Credit Card Number Keywords; ABA Routing Number Keywords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Patterns: Valid Credit Card; Valid Social Security Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rule: US Social Security Numbers</td>
</tr>
<tr>
<td>HIPAA (including PHI)</td>
<td>Dictionaries: US SSN Keywords; Prescription Drug Names; Medical Treatment Keywords; Disease Names; TPO Email Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patterns: Valid Social Security Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Regex rule: Drug Codes</td>
<td></td>
</tr>
<tr>
<td>International Traffic in Arms Regulations (ITAR)</td>
<td>Dictionaries: ITAR Country Codes; ITAR Munition Codes</td>
<td></td>
</tr>
<tr>
<td>NASD Rule 2711 and NYSE Rules 351 and 472</td>
<td>Dictionaries: Analysts' Email Addresses (user-defined); NASD 2711 Keywords</td>
<td></td>
</tr>
<tr>
<td>NASD Rule 3010 and NYSE Rule 342</td>
<td>Dictionaries: NASD 3010 Stock Keywords; NASD 3010 Buy/Sell Keywords; NASD 3010 General Keywords</td>
<td></td>
</tr>
<tr>
<td>NERC Security Guidelines for Electric Utilities</td>
<td>Dictionaries: Sensitive Keywords; Vulnerability Keywords</td>
<td></td>
</tr>
<tr>
<td>Compliance policy type</td>
<td>Premium policy templates</td>
<td>Associated Premium resources</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>U.S. regulatory policies</td>
<td>Office of Foreign Assets Control (OFAC)</td>
<td>Dictionaries: SDN List; OFAC SDN Country Codes; OFAC Country Codes</td>
</tr>
<tr>
<td></td>
<td>Payment Card Industry Data Security Standard</td>
<td>Dictionary: Credit Card Number Keywords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pattern: Valid Credit Card</td>
</tr>
<tr>
<td>Sarbanes-Oxley</td>
<td>Dictionaries: SEC Fair Disclosure Keywords; Company Name Keywords (user-defined); Financial Keywords; Confidential/Proprietary Words</td>
<td>Attachment List: SEC Fair Disclosure Regulation</td>
</tr>
<tr>
<td>SEC Fair Disclosure Regulation</td>
<td>Dictionaries: SEC Fair Disclosure Keywords; Company Name Keywords (user-defined)</td>
<td>Attachment List: SEC Fair Disclosure Regulation</td>
</tr>
<tr>
<td>State Data Privacy</td>
<td>Dictionaries: 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</td>
<td>Patterns: Valid Social Security Number; Valid Credit Card</td>
</tr>
<tr>
<td></td>
<td>Regex rules: ABA Routing Numbers; Drivers License Keywords; CA Drivers License Numbers; NY Drivers License Numbers; IL Drivers License Numbers; NJ Drivers License Numbers; Letter + 12 Digits Drivers License Numbers</td>
<td></td>
</tr>
</tbody>
</table>
Table B-1  Compliance policy templates (Described Content) *(continued)*

<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy templates</th>
<th>Associated Premium resources</th>
</tr>
</thead>
</table>
| Confidential data protection | Confidential Documents | Dictionaries: Confidential Keywords; Proprietary Keywords; Internal Use Only Keywords; Not For Distribution Words  
Attachment Lists: Confidential Documents; Documents Not for Distribution; Internal Use Only Documents; Proprietary Documents |
| Defense Message System (DMS) GENSER Classification | | Dictionaries: Top Secret; Secret; Classified or Restricted; Other Sensitive Information |
| Design Documents | | Dictionary: Design Document Extensions  
Attachment List: Design Documents |
| Encrypted Data | | Dictionaries: GPG Encryption Keywords; PGP file extensions; PGP8 Keywords  
Attachment List: Password Protected Files; PGP Files  
Regex rule: S/MIME |
| Financial Information | | Dictionary: Financial Keywords; Confidential/Proprietary Words  
Attachment Lists: Financial Information |
| Mergers and Acquisitions Data | | Dictionary: M & A Project Code Names (user-defined) |
Attachment List: Publishing Documents |
| Project Data | | Dictionary: Sensitive Project Code Names (user-defined) |
| Resumes | | Dictionaries: Job Search Keywords, Education; Job Search Keywords, Work; Job Search Keywords, General  
Attachment Lists: Resumes, All |
| Source Code | | Dictionary: Source Code Extensions  
Regex rules: C Source Code; VB Source Code; Java Import Statements; Java Class Files; PERL indicator; PERL variable  
Regex rule: PERL Keywords |
| | | Dictionaries: Top Secret; Secret; Classified or Restricted |
Table B-1  Compliance policy templates (Described Content) (continued)

<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy templates</th>
<th>Associated Premium resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Intelligence Control Markings (CAPCO) &amp; DCID 1/7</td>
<td>Competitor Communications</td>
<td>Competitor Domains (user-defined)</td>
</tr>
<tr>
<td>Acceptable use enforcement</td>
<td>Gambling</td>
<td>Dictionaries: Gambling Keywords, Confirmed; Gambling Keywords, Suspect</td>
</tr>
<tr>
<td></td>
<td>Illegal Drugs</td>
<td>Dictionaries: Street Drug Names; Manufd. Controlled Substances</td>
</tr>
<tr>
<td></td>
<td>Media Files</td>
<td>Dictionary: Media Files Extensions; Attachment List: Media Files</td>
</tr>
<tr>
<td></td>
<td>Offensive Language</td>
<td>Dictionaries: Offensive Language, Explicit; Offensive Language, General</td>
</tr>
<tr>
<td></td>
<td>Sexually Explicit Language</td>
<td>Dictionaries: Sex. Explicit Keywords, Confirmed; Sex. Explicit Words, Suspect; Sex. Explicit Words, Possible</td>
</tr>
<tr>
<td></td>
<td>Racist Language</td>
<td>Dictionary: Racist Language</td>
</tr>
<tr>
<td></td>
<td>Restricted Files</td>
<td>Attachment List: MSAccess files and Executables</td>
</tr>
<tr>
<td></td>
<td>Restricted Recipients</td>
<td>Dictionary: Restricted Recipients (user-defined)</td>
</tr>
<tr>
<td></td>
<td>Violence &amp; Weapons</td>
<td>Dictionaries: Violence Keywords; Weapons Keywords</td>
</tr>
</tbody>
</table>

See “Acceptable use policy templates” on page 558.
<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy templates</th>
<th>Associated Premium resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer and employee data protection</td>
<td>Dictionary: Canadian Social Ins. No. Words</td>
<td>Pattern: Canadian Social Insurance Numbers</td>
</tr>
<tr>
<td>Credit Card Numbers</td>
<td>Dictionary: Credit Card Number Keywords</td>
<td>Pattern: Valid Credit Card</td>
</tr>
<tr>
<td>Customer Data Protection</td>
<td>Dictionaries: US SSN Keywords; Credit Card Number Keywords; ABA Routing Number Keywords</td>
<td>Patterns: Valid Credit Card; Valid Social Security Number</td>
</tr>
<tr>
<td>Employee Data Protection</td>
<td>Dictionaries: US SSN Keywords; Credit Card Number Keywords; ABA Routing Number Keywords</td>
<td>Patterns: Valid Credit Card; Valid Social Security Number</td>
</tr>
<tr>
<td>Individual Taxpayer Identification Numbers (ITIN)</td>
<td>Dictionary: US ITIN Keywords</td>
<td></td>
</tr>
<tr>
<td>SWIFT Codes</td>
<td>Dictionary: SWIFT Code Keywords</td>
<td></td>
</tr>
<tr>
<td>UK Drivers License Numbers</td>
<td>Dictionary: UK Keywords</td>
<td></td>
</tr>
<tr>
<td>UK Electoral Roll Numbers</td>
<td>Dictionaries: UK Keywords; UK Electoral Roll Number Words</td>
<td></td>
</tr>
<tr>
<td>UK National Insurance Number</td>
<td>Dictionary: UK NIN Keywords</td>
<td></td>
</tr>
<tr>
<td>UK Passport Numbers</td>
<td>Dictionary: UK Passport Keywords</td>
<td></td>
</tr>
<tr>
<td>UK Tax ID Numbers</td>
<td>Dictionary: UK Tax ID Number Keywords</td>
<td></td>
</tr>
</tbody>
</table>
### Table B-1

<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy templates</th>
<th>Associated Premium resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Social Security Numbers</td>
<td>Dictionary: US SSN Keywords</td>
<td>Pattern: Valid Social Security Number</td>
</tr>
<tr>
<td>Network security enforcement</td>
<td>Network Security</td>
<td>Dictionaries: Hacker Keywords; Keylogger Keywords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rule: GoToMyPC Activity</td>
</tr>
<tr>
<td>Network Diagrams</td>
<td>Attachment List: Network Diagrams with IP Address Keyword; Valid IP Address</td>
<td></td>
</tr>
<tr>
<td>Password Files</td>
<td>Dictionary: Password Filename</td>
<td>Regex rules: /etc/passwd Format; /etc/shadow Format; SAM password</td>
</tr>
<tr>
<td>UK and international regulatory enforcement</td>
<td>Caldicott Report</td>
<td>Dictionaries: Prescription Drug Names; Disease Names; Medical Treatment Keywords; UK NIN Keywords</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rule: UK National Insurance Number</td>
</tr>
<tr>
<td>Data Protection Act 1998</td>
<td>Dictionaries: UK NIN Keywords; UK Tax ID Number Keywords; UK Keywords; UK Passport Keywords; UK Electoral Roll Number Words</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rules: UK Electoral Roll Numbers; UK National Insurance Number; UK Tax ID Numbers; UK Drivers License Numbers; Drivers License Keywords; UK Passport Numbers (Old Type); UK Passport Numbers (New Type)</td>
</tr>
<tr>
<td>Human Rights Act 1998</td>
<td>Dictionaries: UK Personal Data Keywords; UK Keywords; UK Electoral Roll Number Words</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rules: UK Electoral Roll Numbers</td>
</tr>
<tr>
<td>PIPEDA</td>
<td>Dictionaries: Canadian Social Ins. No. Words; ABA Routing Number Keywords; Credit Card Number Keywords</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Patterns: Valid Credit Card</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rule: ABA Routing Numbers; Canadian Social Insurance Numbers</td>
</tr>
</tbody>
</table>

### Structured Data Compliance policy templates

This section describes the Structured Data Compliance policy templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.
<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy template</th>
<th>Associated Premium resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. regulatory policies</td>
<td>Export Administration Regulations (EAR)</td>
<td>Dictionary: EAR Country Codes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record resource with SKU data</td>
</tr>
<tr>
<td></td>
<td>Gramm-Leach-Bliley</td>
<td>Record resource with following fields: Account number; Bank card number; Email address; First name; Last name; PIN number; Phone number; Social Security Number; ABA Routing Number; Canadian Social Insurance Number; UK National Insurance Number; Date of Birth</td>
</tr>
<tr>
<td></td>
<td>HIPAA (including PHI)</td>
<td>Dictionaries: Prescription Drug Names; Medical Treatment Keywords; Disease Names; TPO Email Addresses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regex rule: Drug Codes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record resource with following fields: Last name; Tax payer ID (SSN); Email address; Account number; ID card number; Phone number</td>
</tr>
<tr>
<td></td>
<td>International Traffic in Arms Regulations (ITAR)</td>
<td>Dictionary: ITAR Country Codes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record resource with Stock Keeping Unit (SKU) data</td>
</tr>
<tr>
<td></td>
<td>Payment Card Industry Data Security Standard</td>
<td>Record resource view.</td>
</tr>
<tr>
<td></td>
<td>State Data Privacy</td>
<td>Dictionary: Affiliate Domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record resource with following fields: First name; Last name; Tax payer ID; Bank card; Account; PIN; State ID; Driver's license; Password; ABA number; Date of birth; SSN</td>
</tr>
<tr>
<td>Confidential data protection</td>
<td>Price Information</td>
<td>Record resource with fields for Stock Keeping Unit (SKU) numbers and prices.</td>
</tr>
<tr>
<td></td>
<td>Resumes</td>
<td>Dictionaries: Job Search Keywords, Education; Job Search Keywords, Work; and Job Search Keywords, General</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Attachment list: Resumes, Employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record resource with fields for employee first and last names.</td>
</tr>
</tbody>
</table>
Table B-2  Compliance policy templates (Structured Data) (continued)

<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy template</th>
<th>Associated Premium resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer and employee data protection</td>
<td>Customer Data Protection</td>
<td>Record resource with the following fields: 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.</td>
</tr>
<tr>
<td>Employee Data Protection</td>
<td></td>
<td>Record resource with the following fields: 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.</td>
</tr>
</tbody>
</table>
Table B-2  Compliance policy templates (Structured Data) (continued)

<table>
<thead>
<tr>
<th>Compliance policy type</th>
<th>Premium policy template</th>
<th>Associated Premium resource</th>
</tr>
</thead>
</table>
| UK and international regulatory enforcement | Caldicott Report | Dictionaries: Prescription Drug Names; Disease Names; Medical Treatment Keywords  
See “UK and international regulatory policy templates” on page 569.  
Record resource with the following fields: NIN (National Insurance Number), account number, last name, ID card number, email, phone, and UK NHS (National Health Service) number. |
| Data Protection Act 1998 | Record resource with the following fields: 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. |
| EU Data Protection Directives | Dictionary: EU Country Codes  
Record resource with the following fields: 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. |
| Human Rights Act 1998 | Dictionary: UK Personal Data Keywords  
Record resource with last name and electoral roll number fields. |
| PIPEDA | Record resource with following fields: 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. |

Regular expressions for context-filtering conditions

This section describes the regular expressions that can be used in policy conditions.  
See “About using regular expressions in conditions” on page 327.
## Table B-3

<table>
<thead>
<tr>
<th>Regex rule name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Routing Numbers</td>
<td>Any digit other than a 4, 5 or 9 followed by any 8 digits.</td>
<td>0123465789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2222222222</td>
</tr>
<tr>
<td></td>
<td></td>
<td>841471235</td>
</tr>
<tr>
<td>CA Drivers License Numbers</td>
<td>Any sequence of a letter followed by 7 digits, immediately preceded and</td>
<td>a1234567</td>
</tr>
<tr>
<td></td>
<td>succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>A1234567</td>
</tr>
<tr>
<td>Canadian Social Insurance Numbers</td>
<td>Matches numbers in the form DDD-DDD-DDD or DDD DDD DDD</td>
<td>123-456-789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>123 456 789</td>
</tr>
<tr>
<td>C Source Code</td>
<td>The sequence #include, followed by any number of spaces, followed by a '&lt;' or</td>
<td>#include &lt;stdio.h&gt;</td>
</tr>
<tr>
<td></td>
<td>&quot;&quot;, followed by any number of letters, digits or underscores, followed by a</td>
<td>#include &quot;fdfdfd&quot;</td>
</tr>
<tr>
<td></td>
<td>&lt; or &quot;.&quot;</td>
<td></td>
</tr>
<tr>
<td>Drivers License Keywords</td>
<td>Looks for combinations of driv followed by characters followed by lic followed</td>
<td>Driver License</td>
</tr>
<tr>
<td></td>
<td>by characters OR dl # or dl# OR lic # or lic# all case insensitive.</td>
<td>Driver License</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dl #</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DL#</td>
</tr>
<tr>
<td>Drug Codes</td>
<td>Matches NDC Drug Code format <a href="http://www.fda.gov/cder/ndc/">http://www.fda.gov/cder/ndc/</a></td>
<td>12345-1234-12</td>
</tr>
<tr>
<td>/etc/passwd Format</td>
<td>Looks for sequences that match an /etc/passwd format.</td>
<td>bob:fdshfjhf:78978:45:fdsf:</td>
</tr>
<tr>
<td>/etc/shadow Format</td>
<td>Looks for sequences that match an /etc/shadow format.</td>
<td>bob:fdsfd:343:45454: 4343:122:343:545</td>
</tr>
<tr>
<td>GoToMyPC Activity</td>
<td>Looks for a case insensitive match of the sequence 'jedi?request=' or '/erc/Poll?machinekey'</td>
<td>jedi?request= /erc/Poll?machinekey</td>
</tr>
<tr>
<td>IL Drivers License Numbers</td>
<td>Any sequence of a letter followed by 11 digits, immediately preceded and</td>
<td>a12346578901</td>
</tr>
<tr>
<td></td>
<td>succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>A12345678901</td>
</tr>
<tr>
<td>Regex rule name</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Address</td>
<td>Looks for a case insensitive match of the sequence 'IP Address.'</td>
<td>IP Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPaDdress</td>
</tr>
<tr>
<td>Java Class Files</td>
<td>Optional public, private or protected followed by class or interface followed a class name by an optional extends or implements followed by a class name.</td>
<td>public class Foo</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protected class Bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>implements Foo</td>
</tr>
<tr>
<td>Java Import Statements</td>
<td>Looks for import followed by a class name followed by a semicolon.</td>
<td>import</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java.util.Collection;</td>
</tr>
<tr>
<td>NY Drivers License Numbers</td>
<td>Any sequence of 9 digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>123456789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>987654321</td>
</tr>
<tr>
<td>Letter + 12 Digits Drivers License Numbers</td>
<td>Any sequence of a letter followed by 12 digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>a123456789012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A123456789012</td>
</tr>
<tr>
<td>NJ Drivers License Numbers</td>
<td>Any sequence of a letter followed by 13 digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>a1234567890123</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A1234567890123</td>
</tr>
<tr>
<td>SAM Passwords</td>
<td>Looks for sequences that match a SAM passwords format.</td>
<td>bob:3434:12345678901234567890123456789012345678901234567890123456789012:</td>
</tr>
<tr>
<td>PERL Keywords</td>
<td>A case sensitive match of the sequence 'perl'</td>
<td>perl</td>
</tr>
<tr>
<td>PERL indicator</td>
<td>Looks for the sequence #!</td>
<td>#!</td>
</tr>
<tr>
<td>PERL variable</td>
<td>Looks for sequences that start with a $ followed by any letter or underscore then followed by any number of letters, digits or underscore.</td>
<td>$something;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$another;</td>
</tr>
<tr>
<td>Regex rule name</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Looks for MIME-type that begins with application/pkcs7-mime or application/x-pkcs7-mime or application/pkcs7-signature or application/x-pkcs7-signature</td>
<td>example.p7c example.p7m example.p7s example.p7a</td>
</tr>
<tr>
<td>SWIFT Code Regex</td>
<td>4 characters followed by a dash followed by 2 characters followed dash followed by 2 characters followed by an optional dash and 2 characters.</td>
<td>ABCD-EF-GH ABCD-EF-GH-IJK</td>
</tr>
<tr>
<td>UK Drivers License Numbers</td>
<td>5 characters or digits followed by a digit followed by one of the inner groupings followed by a digit followed by 3 characters or digits followed by 2 characters.</td>
<td>A1234501023ABCDE</td>
</tr>
<tr>
<td>UK Electoral Roll Numbers</td>
<td>Two or three upper case letters, followed by one to four digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>AB1 AB12 AB123 AB1234 ABC1 ABC1234</td>
</tr>
<tr>
<td>UK National Insurance Number</td>
<td>Two upper case letters from the group A-CEGHJ-NOPR-TW-Z followed by 6 digits, followed by an optional upper case letter (A through D), immediately preceded and succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>AB123456 AB132456C</td>
</tr>
<tr>
<td>UK Passport Numbers (Old Type)</td>
<td>An upper case letter or digit, followed by 4 digits, followed by an upper case letter or digit, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore (_).</td>
<td>A1234B 12345C 132456 A12345</td>
</tr>
</tbody>
</table>
### Table B-3

Regular expressions *(continued)*

<table>
<thead>
<tr>
<th>Regex rule name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Passport Numbers (New Type)</td>
<td>Any sequence of 9 digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore.</td>
<td>A1234B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12345C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>132456</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A12345</td>
</tr>
<tr>
<td>UK Tax ID Numbers</td>
<td>Any sequence of 10 digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore.</td>
<td>AB123456</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AB132456C</td>
</tr>
<tr>
<td>US ITIN</td>
<td>Looks for a 9 followed by 2 digits, followed by a dash, followed by a 7 or 8 followed by a digit, followed by a dash, followed by any four digits, immediately preceded and succeeded by a character that is not a letter, a digit, or underscore.</td>
<td>912-71-1234</td>
</tr>
<tr>
<td></td>
<td></td>
<td>902-81-0234</td>
</tr>
<tr>
<td>VB Source Code</td>
<td>A case sensitive match of the sequence Attribute followed by a space character followed by VB_Name.</td>
<td>Attribute VB_Name</td>
</tr>
</tbody>
</table>

### Premium attachment list resources

This section describes the premium attachment lists resources provided by Symantec Brightmail Gateway.

See “About attachment list resources” on page 311.
<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</td>
</tr>
<tr>
<td>Design Documents</td>
<td>Vector graphic Document</td>
<td>AutoCAD DXF Binary, AutoCAD DXF Text, AutoDesk Drawing (DWG)</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>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>Spreadsheet formats</td>
<td>Ability Spreadsheet, Applix Spreadsheets, CSV (Comma Separated Values), Data Interchange Format (DIF), Enable Spreadsheet, Lotus 1-2-3, Lotus 1-2-3 97, Lotus 1-2-3 Formatting, Lotus 1-2-3 Release 9, Microsoft Excel, Microsoft Excel 2000, Microsoft Excel 95, Microsoft Excel 97, Microsoft Excel Chart, Microsoft Excel Macro, Microsoft Excel Macro 2007 XML, Microsoft Excel 2007 XML, Microsoft Excel XML, Microsoft Works for MAC Spreadsheet, Microsoft Works for Windows Spreadsheet, Multiplan (Mac), Multiplan (PC), PeachCalc, Quattro Pro for DOS, Quattro Pro for Windows, SmartWare II Spreadsheet, StarOffice Spreadsheet XML, Supercalc, SYLK, Symphony, Uniplex Ucalc</td>
</tr>
<tr>
<td>Scheduling/Planning Format</td>
<td></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>Executable Files</td>
<td>Executable File</td>
<td>ELF Executable MS-DOS Batch File 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 Macro, 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>Raster image Documents</td>
<td>MacPaint, MS Windows Device Independent Bitmap, OLE DIB object, OS/2 PM Metafile, PC Paintbrush Graphics (PCX), PCD Format, Portable Bitmap Utilities ASCII Format, Portable Bitmap Utilities Binary Format, Portable Greymap Utilities ASCII Format, Portable Greymap Utilities Binary Format</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>Documents Not For</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distribution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Use Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proprietary Documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presentation</td>
<td>Microsoft PowerPoint 2000, PowerPoint 95, PowerPoint 97, PowerPoint MAC, PowerPoint PC</td>
<td></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>Media Files</td>
<td>Animation File</td>
<td>Macromedia Director, Macromedia Flash</td>
</tr>
<tr>
<td></td>
<td>Vector graphic Document</td>
<td>Quickdraw 3D Metafile, VRML</td>
</tr>
<tr>
<td></td>
<td>Movie File</td>
<td>QuickTime Movie, RIFF Multimedia Movie, Video for Windows (AVI)</td>
</tr>
<tr>
<td></td>
<td>Sound File Format</td>
<td>Microsoft Wave, MIDI, MP3 (MPEG Audio), RealAudio, RIFF MIDI</td>
</tr>
<tr>
<td>MSAccess files and Executables</td>
<td>Library</td>
<td>DOS/Windows Object Library</td>
</tr>
<tr>
<td></td>
<td>Database Documents</td>
<td>Microsoft Access, Microsoft Access 2000, Microsoft Access 95 Microsoft, Access 97</td>
</tr>
<tr>
<td></td>
<td>Executables</td>
<td>MSDOS Device Driver, PC (.COM), MSDOS/Windows Program, 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></td>
<td>Object Module Format</td>
<td>Unix Object Module (old MS 8086), Unix Object Module (VAX Demand), Unix Object Module (Z8000)</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></td>
<td>Sound File Format</td>
<td>Amiga IFF (8SVX) Sound, Amiga MOD, Audio Interchange File Format (AIFF), Creative Voice (VOC), Microsoft Wave, MIDI, MPEG Audio, NeXT/Sun Audio Data, Real Audio, RIFF MIDI</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>Word Processor Document</td>
<td>Microsoft Visio 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>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></td>
<td>Presentation Document (password protected)</td>
<td>Microsoft PowerPoint 2000, PowerPoint 95, PowerPoint 97, PowerPoint MAC, PowerPoint PC</td>
</tr>
<tr>
<td></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>
<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 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>
</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 B-5  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>
<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>

Premium pattern resources

This section describes the premium pattern resources provided by Symantec Brightmail Gateway.

See “About pattern policy resources” on page 314.

Table B-6  Premium Pattern resources keyed to policy templates

<table>
<thead>
<tr>
<th>Premium resource</th>
<th>Associated policy template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid IP address</td>
<td>Network Diagrams</td>
</tr>
<tr>
<td>Valid Credit Card</td>
<td>Credit Card Numbers; Customer Data Protection; Employee Data Protection; PIPEDA; State Data Privacy; Payment Card Industry Data Security Standard; Gramm-Leach-Bliley</td>
</tr>
</tbody>
</table>
Table B-6  Premium Pattern resources keyed to policy templates (continued)

<table>
<thead>
<tr>
<th>Premium resource</th>
<th>Associated policy template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Social Security Number</td>
<td>HIPAA; Gramm-Leach-Bliley; US Social Security Numbers; Individual Taxpayer Identification Numbers (ITIN); State Data Privacy; Customer Data Protection; Employee Data Protection</td>
</tr>
</tbody>
</table>

**Note:** The Valid Credit Card and Valid Social Security Number patterns differ from the Credit Card and Social Security Number patterns provided in the Basic resource. Premium Pattern resources perform additional error-checking and validation in addition to regular-expression pattern matching. Symantec recommends that you use the Premium Pattern resource to reduce false positives.

### Premium dictionary resources

This section describes the premium dictionary resources provided by Symantec Brightmail Gateway.

See “About dictionary resources” on page 305.

Table B-7  Premium dictionaries keyed to policy templates

<table>
<thead>
<tr>
<th>Premium resource</th>
<th>Associated premium policy 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>Premium resource</td>
<td>Associated premium policy templates</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------</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>
<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>Financial Information</td>
<td></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>Premium resource</td>
<td>Associated premium policy templates</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>M &amp; A Project Code Names (user-defined)</td>
<td>Mergers and Acquisitions Data</td>
</tr>
<tr>
<td>Manufd. Controlled Substances</td>
<td>Illegal Drugs</td>
</tr>
<tr>
<td>Street Drug Names</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) GENESER 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></td>
<td></td>
</tr>
<tr>
<td>Premium resource</td>
<td>Associated premium policy templates</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</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>
<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>
</tbody>
</table>
Table B-7  Premium dictionaries keyed to policy templates (continued)

<table>
<thead>
<tr>
<th>Premium resource</th>
<th>Associated premium policy templates</th>
</tr>
</thead>
<tbody>
<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>

**Premium regular-expression resources keyed to policy templates**

This section describes the premium regular expressions provided by Symantec Brightmail Gateway and their associated policy templates.

See “About using regular expressions in conditions” on page 327.

Table B-8  Premium regular-expression resources keyed to policy templates

<table>
<thead>
<tr>
<th>Premium resource</th>
<th>Associated policy templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Routing Number</td>
<td>Customer Data Protection; Employee Data Protection; PIPEDA; State Data Privacy</td>
</tr>
<tr>
<td>Canadian Social Insurance Numbers</td>
<td>PIPEDA; Canadian Social Insurance Number</td>
</tr>
<tr>
<td>Drug Codes</td>
<td>HIPAA (including PHI)</td>
</tr>
<tr>
<td>CA Drivers License Numbers</td>
<td>State Data Privacy</td>
</tr>
<tr>
<td>Drivers License Keywords</td>
<td></td>
</tr>
<tr>
<td>NY Drivers License Numbers</td>
<td></td>
</tr>
<tr>
<td>Letter + 12 Digits Drivers License Numbers</td>
<td></td>
</tr>
<tr>
<td>IL Drivers License Numbers</td>
<td></td>
</tr>
<tr>
<td>NJ Drivers License Numbers</td>
<td></td>
</tr>
<tr>
<td>/etc/passwd Format</td>
<td>Password Files</td>
</tr>
<tr>
<td>/etc/shadow Format</td>
<td></td>
</tr>
<tr>
<td>SAM Passwords</td>
<td></td>
</tr>
<tr>
<td>Filename</td>
<td>Password Files; Encrypted Data</td>
</tr>
</tbody>
</table>
### Table B-8

<table>
<thead>
<tr>
<th>Premium resource</th>
<th>Associated policy templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoToMyPC Activity</td>
<td>Network Security</td>
</tr>
<tr>
<td>IP Address</td>
<td>Network Diagrams</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Encrypted Data</td>
</tr>
<tr>
<td>Java Source Code</td>
<td>Source Code</td>
</tr>
<tr>
<td>C Source Code</td>
<td></td>
</tr>
<tr>
<td>VB Source Code</td>
<td></td>
</tr>
<tr>
<td>PERL Keywords</td>
<td></td>
</tr>
<tr>
<td>PERL indicator</td>
<td></td>
</tr>
<tr>
<td>PERL variable</td>
<td></td>
</tr>
<tr>
<td>SWIFT Code Regex</td>
<td>Swift Codes</td>
</tr>
<tr>
<td>UK Drivers License Numbers</td>
<td>UK Drivers License Numbers</td>
</tr>
<tr>
<td>UK Electoral Roll Number</td>
<td>UK Electoral Roll Numbers; Human Rights Act 1998</td>
</tr>
<tr>
<td>UK National Insurance Number</td>
<td>UK National Insurance Number; Caldicott Report</td>
</tr>
<tr>
<td>UK Passport Numbers (Old Type)</td>
<td>UK Passport Numbers; Data Protection Act 1998</td>
</tr>
<tr>
<td>UK Passport Numbers (New Type)</td>
<td></td>
</tr>
<tr>
<td>UK Tax ID Numbers</td>
<td>UK Tax ID Numbers</td>
</tr>
<tr>
<td>US ITIN</td>
<td>Individual Taxpayer Identification Numbers (ITIN)</td>
</tr>
</tbody>
</table>

### U.S. regulatory policy templates

This section describes the US regulatory policy templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.
### Table B-9  U.S. regulatory policy templates

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Administration Regulations (EAR)</td>
<td>The Export Administration Regulations (EAR) are enforced by the US Department of Commerce. These regulations primarily cover technologies and technical information with both commercial and military applications. They are also known as dual use technologies (for example, chemicals, satellites, software, computers). This policy detects violations based on countries and controlled technologies designated by the EAR.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Gramm-Leach Bliley</td>
<td>The Gramm-Leach-Bliley (GLB) Act gives consumers the right to limit some sharing of their information by financial institutions. This policy detects transmittal of customer data.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>HIPAA (including PHI)</td>
<td>This policy strictly enforces the US Health Insurance Portability and Accountability Act (HIPAA) by searching for data concerning prescription drugs, diseases, and treatments in conjunction with Protected Health Information (PHI). This policy can be used by organizations that are not subject to HIPAA but want to control PHI data.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>International Traffic in Arms Regulations (ITAR)</td>
<td>The International Traffic in Arms Regulations (ITAR) are enforced by the US Department of State. Exporters of defense services or related technical data are required to register with the federal government and may need export licenses. This policy detects potential violations based on countries and controlled assets designated by the ITAR.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>NASD Rule 2711 and NYSE Rules 351 and 472</td>
<td>NASD Rule 2711 and NYSE Rules 351 and 472 protect the name(s) of any companies involved in an upcoming stock offering, internal project names for the offering, and the stock ticker symbols for the offering companies.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>NASD Rule 3010 and NYSE Rule 342</td>
<td>NASD Rule and NYSE Rule 342 require brokers-dealers to supervise certain brokerage employee's communications. This policy monitors the communications of registered principals who are subject to these regulations.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Table B-9  U.S. regulatory policy templates (continued)

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
</table>
| NERC Security Guidelines for Electric Utilities  
| Description |
| Detects information outlined in the North American Electric Reliability Council (NERC) security guidelines for protecting and securing potentially sensitive information about critical electricity infrastructure. |
| Described Content | X |

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
</table>
| Office of Foreign Assets Control (OFAC)  
See “Office of Foreign Assets Control (OFAC)” on page 549. |
| Description |
| The Office of Foreign Assets Control of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against certain countries, individuals, and organizations. This policy detects communications involving these targeted groups. |
| Described Content | X |

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
</table>
| Payment Card Industry Data Security Standard  
See “Payment Card Industry Data Security Standard” on page 549. |
| Description |
| The Payment Card Industry (PCI) data security standards are jointly determined by Visa and Mastercard to protect cardholders by safeguarding personally identifiable information. Visa’s Cardholder Information Security Program (CISP) and Mastercard’s Site Data Protection (SDP) program both work toward enforcing these standards. This policy detects credit card number data. |
| Described Content | X |

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
</table>
| Sarbanes-Oxley  
See “Sarbanes-Oxley” on page 550. |
| Description |
| The US Sarbanes-Oxley Act (SOX) imposes requirements on financial accounting, including the preservation of data integrity and the ability to create an audit trail. This policy detects sensitive financial data. |
| Described Content | X |

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
</table>
| SEC Fair Disclosure Regulation  
| Description |
| The US SEC Selective Disclosure and Insider Trading Rules prohibit public companies from selectively divulging material information to analysts and institutional investors prior to its general release to the public. This policy detects data indicating disclosure of material financial information. |
| Described Content | X |

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
</table>
| State Data Privacy  
See “State Data Privacy” on page 551. |
| Description |
| Many states in the US have adopted statutes mandating data protection and public disclosure of information security in which confidential data of individuals is compromised. This policy detects these breaches of confidentiality. |
| Described Content | X |

Export Administration Regulations (EAR)

Described Content condition:
EAR Commerce Control List and Recipients - 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.

Structured Data conditions:

- Indexed EAR Commerce Control List Items and Recipients – A compound condition that 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.

Included dictionaries:

- EAR Country Codes
- EAR CCL Keywords

Gramm-Leach-Bliley

Described Content conditions:

- 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.

Structured Data conditions:

- 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.

Included dictionaries:
- US SSN Keywords
- Credit Card Number Keywords
- ABA Routing Number Keywords

HIPAA

Described Content conditions:
- 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.

Structured Data conditions:
- 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 condition:

- 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.

Included dictionaries:
- US SSN Keywords
- Prescription Drug Names
- Medical Treatment Keywords
- Disease Names
- TPO Email Address

**International Traffic in Arms Regulations (ITAR)**

Described Content condition:

- ITAR Munitions List and Recipients - A compound rule that looks for both a recipient country code from the ITAR Country Codes dictionary and a keyword from the ITAR Munition Names dictionary.

Structured Data conditions:

- Indexed ITAR Munition Items and Recipients – A compound rule that 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.

Included dictionaries:
- ITAR Country Codes
- ITAR Munition Codes
NASD Rule 2711 and NYSE Rules 351 and 472

Described Content conditions:

- NASD Rule 2711 and NYSE Rules 351 and 472 - Compound rule that 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:

- Analysts' Email Addresses
- NASD 2711 Keywords

NASD Rule 3010 and NYSE Rule 342

Described Content conditions:

- 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.

Included dictionaries:

- NASD 3010 Stock Keywords
- NASD 3010 Buy/Sell Keywords
- NASD General Keywords

NERC Security Guidelines for Electric Utilities

Described Content condition:

- A compound rule that looks for any keyword matches from the "Sensitive Keywords" dictionary and the "Vulnerability Keywords" dictionary.

Included dictionaries:

- Sensitive Keywords
Vulnerability Keywords

Office of Foreign Assets Control (OFAC)

**Note:** 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.

Described Content conditions:

- **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.

Included dictionaries:

- SDN List
- OFAC SDN Country Codes
- OFAC Country Codes

Payment Card Industry Data Security Standard

Described Content condition:

- **Credit Card Numbers, All** - Looks for a match to the Valid Credit Card pattern and a keyword from the Credit Card Number Keywords dictionary.

Structured Data conditions:

- Searches record resource view for a match.
Included dictionary:

- Credit Card Number Keywords

**Sarbanes-Oxley**

Described Content conditions:

- 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.

Included dictionaries:

- SEC Fair Disclosure Keywords
- Company Name Keywords
- Financial Keywords
- Confidential/Proprietary Words

**SEC Fair Disclosure Regulation**

Described Content conditions:

- 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.

Included dictionaries:

- SEC Fair Disclosure Keywords
- Company Name Keywords

**State Data Privacy**

Described Content conditions:

- **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.

Structured Data conditions:

■ 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.

Included dictionaries:

■ 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

**Confidential data-protection policy templates**

This section describes the confidential data protection policy templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.

**Table B-10  Confidential data-protection policy templates**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential Documents</td>
<td>This policy detects company-confidential documents at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

See “Confidential Documents” on page 554.
### Table B-10

Confidential data-protection policy templates *(continued)*

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Message System (DMS) GENSER Classification</td>
<td>DMS General Service categories for messaging classify national security information according to access controls, which limit message distribution to authorized recipients. This policy template differs from US Intelligence Control Markings (CAPCO &amp; DCID 1/7) in that it includes terms used to identify unclassified but sensitive information.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Design Documents</td>
<td>This policy detects various types of design documents, such as CAD/CAM, at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Encrypted Data</td>
<td>This policy detects the use of encryption by a variety of methods including S/MIME, PGP, GPG, and file password protection.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Financial Information</td>
<td>This policy detects financial data and information.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mergers and Acquisitions Data</td>
<td>This policy detects information and communications about upcoming merger and acquisition activity. It may be modified with company-specific code words to detect specific deals.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Price Information</td>
<td>This policy detects specific SKU and/or pricing information at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Project Data</td>
<td>This policy detects discussions of sensitive projects.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Publishing Documents</td>
<td>This policy detects various types of publishing documents, such as FrameMaker files, at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Resumes</td>
<td>This policy detects active job searches.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Source Code</td>
<td>This policy detects various types of source code at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Table B-10  Confidential data-protection policy templates (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Intelligence Control Markings (CAPCO &amp; DCID 1/7)</td>
<td>This policy detects authorized terms to identify classified information in the US Federal Intelligence community as defined in the Control Markings Register, which is maintained by the Controlled Access Program Coordination Office (CAPCO) of the Community Management Staff (CMS). The register was created in response to the Director of Central Intelligence Directive (DCID) 1/7.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “US Intelligence Control Markings (CAPCO) and DCID 1/7” on page 558.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Confidential Documents

Described Content conditions:

- 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.

Included dictionaries:

- Confidential Keywords
- Proprietary Keywords
- Internal Use Only Keywords
- Not For Distribution Words
Defense Message System (DMS) GENSER Classification

Described Content condition:

- 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.

Included dictionaries:

- Secret
- Top Secret
- Classified or Restricted
- Other Sensitive Information

Design Documents

Described Content conditions:

- 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.

Included dictionary:

- Design Document Extensions

Encrypted Data

Described Content conditions:

- 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.

Included dictionaries:
- GPG Encryption Keywords
- PGP file extension
- PGP8 Keywords

Financial Information
Described Content condition:
- 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.

Included dictionaries:
- Financial Keywords
- Confidential/Proprietary Words

Mergers and Acquisition Data
Described Content condition:
- M & A Activity - 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.

Included dictionary:
- M & A Project Code Names

Price Information
Structured Data 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
Described Content condition:
Project Activity - Looks for any keywords in the Sensitive Project Code Names dictionary, which is user-defined.

Included dictionary:
- Sensitive Project Code Names

Publishing Documents

Described Content conditions:
- Publishing Documents - Looks for the specified file types: qxpress, frame, aldus_pagemaker, and publ (Microsoft Publisher).

Included dictionary:
- Publishing Document Extensions

Resumes

Described Content condition:
- Resumes, All - 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.

Structured Data conditions:
- Resumes, Employee – Matches files that are less than 50 KB of a specified type (e.g., .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.

Included dictionaries:
- Job Search Keywords, Education
- Job Search Keywords, Work
- Job Search Keywords, General

Source Code

Described Content conditions:
■ 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.

Included dictionary:
■ Source Code Extensions

US Intelligence Control Markings (CAPCO) and DCID 1/7

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.

Included dictionaries:
■ Secret
■ Top Secret
■ Classified or Restricted

Acceptable use policy templates

This section describes the acceptable use policy templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.

Table B-11  Acceptable use policy templates

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitor Communications</td>
<td>This policy detects communications with competitors.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Competitor Communications” on page 559.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gambling</td>
<td>This policy detects any reference to gambling.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Gambling” on page 560.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table B-11  Acceptable use policy templates (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegal Drugs</td>
<td>This policy detects conversations about illegal drugs and controlled substances.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Illegal Drugs” on page 560.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Files</td>
<td>This policy detects various types of video and audio files (including mp3).</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Media Files” on page 560.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offensive Language</td>
<td>This policy detects the use of offensive language.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Offensive Language” on page 560.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Racist Language</td>
<td>This policy detects the use of racist language.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Racist Language” on page 561.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Files</td>
<td>This policy detects various file types that are generally inappropriate to send out of the company such as MS Access and executable files.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Restricted Files” on page 561.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Recipients</td>
<td>This policy detects communications with any specified recipients such as former employees.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Restricted Recipients” on page 561.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexually Explicit Language</td>
<td>This policy detects vulgar and sexually explicit pornographic language content.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Sexually Explicit Language” on page 561.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Violence &amp; Weapons</td>
<td>This policy detects violent language and discussions about weapons.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Violence and Weapons” on page 562.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Competitor Communications

Described Content condition:

- Competitor List - Looks for keywords (domains) from the Competitor Domains dictionary, which is user-defined.

Included dictionary:

- Competitor Domains
Gambling

Described Content conditions:

■ 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.

Included dictionaries:

■ Gambling Keywords, Confirmed
 ■ Gambling Keywords, Suspect

Illegal Drugs

Described Content conditions:

■ 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.

Included dictionaries:

■ Street Drug Names
 ■ Manufd. Controlled Substances

Media Files

Described Content conditions:

■ 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.

Included dictionary:

■ Media Files Extensions

Offensive Language

Described Content conditions:


Included dictionaries:
■ Offensive Language, Explicit
■ Offensive Language, General

Racist Language

Described Content condition:
■ Racist Language - Looks for any single keyword in the Racist Language dictionary.

Included dictionary:
■ Racist Language

Restricted Files

Described Content condition:
■ MSAccess Files and Executables - Looks for files of the specified types: access, exe, and exe_unix.

Included dictionary:
■ None

Restricted Recipients

Described Content condition:
■ Restricted Recipients - Looks for messages to recipients with email addresses in the Restricted Recipients dictionary.

Included dictionary:
■ Restricted Recipients

Sexually Explicit Language

Described Content conditions:
■ 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.

Included dictionaries:
- Sex. Explicit Keywords, Confirmed
- Sex. Explicit Words, Suspect
- Sex. Explicit Words, Possible

Violence and Weapons

Described Content condition:
- Violence & Weapons - A compound condition that looks for a keyword from the Violence Keywords dictionary and a keyword from the Weapons Keywords dictionary.

Included dictionaries:
- Violence Keywords
- Weapons Keywords

Customer and employee data-protection templates

This section describes the customer and employee data-protection templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canadian Social Insurance Numbers</td>
<td>This policy detects patterns indicating Canadian social insurance numbers (SINs) at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Canadian Social Insurance Number” on page 564.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit Card Numbers</td>
<td>This policy detects patterns indicating credit card numbers at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Credit Card Numbers” on page 564.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Data Protection</td>
<td>This policy detects customer data at risk of exposure.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>See “Customer Data Protection” on page 564.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Described Content</td>
<td>Structured Data</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Employee Data Protection</td>
<td>This policy detects employee data at risk of exposure.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>See “Employee Data Protection” on page 565.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual Taxpayer Identification Numbers (ITIN)</td>
<td>An Individual Taxpayer Identification Number (ITIN) is a tax processing number issued by the US Internal Revenue Service (IRS). The IRS issues ITINs to track individuals that are not eligible to obtain a Social Security Number (SSNs).</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Individual Taxpayer Identification Numbers (ITIN)” on page 566.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIFT Codes</td>
<td>The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a cooperative organization under Belgian law and is owned by its member financial institutions. The SWIFT code (also known as a Bank identifier Code, or ISO 9362) has a standard format to identify a bank, location, and the branch involved. The codes are used when transferring money between banks, particularly across international borders.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “SWIFT Codes” on page 566.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK Drivers License Numbers</td>
<td>This policy detects UK Drivers License Numbers using the official specification of the UK Government Standards of the UK cabinet Office.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>See “UK Drivers License Numbers” on page 566.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK Electoral Roll Numbers</td>
<td>This policy detects UK Electoral Roll Numbers using the official specification of the UK Government Standards of the UK Cabinet Office.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “UK Electoral Roll Numbers” on page 567.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK National Insurance Number</td>
<td>The National Insurance Number is issued to individuals by the UK Department for Work and Pensions and Inland Revenue (DWP/IR) for administering the national insurance system.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “UK National Insurance Number” on page 567.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table B-12

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Passport Numbers</td>
<td>This policy detects valid UK passports using the official specification of the UK Government Standards of the UK Cabinet Office.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “UK Passport Numbers” on page 567.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK Tax ID Numbers</td>
<td>This policy detects UK Tax ID Numbers using the official specification of the UK Government Standards of the UK Cabinet Office.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “UK Tax ID Numbers” on page 567.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US Social Security Numbers</td>
<td>This policy detects patterns indicating social security numbers at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

### Canadian Social Insurance Number

**Described Content condition:**

- **Canadian Social Insurance Numbers** - Looks for a match to the Canadian Social Insurance Number regular expression and a keyword from the Canadian Social Ins. No. Words dictionary.

**Included dictionaries:**

- **Canadian Social Ins. No. Words**

### Credit Card Numbers

**Described Content condition:**

- **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.

**Included dictionary:**

- **Credit Card Number Keywords**

### Customer Data Protection

**Described Content conditions:**

- **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.

Structured Data conditions:

- Username/Password Combinations – Looks for usernames 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

Included dictionaries:

- US SSN Keywords
- Credit Card Number Keywords
- ABA Routing Number Keywords

Employee Data Protection

Described Content conditions:

- 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.

Structured Data conditions:

- Username/Password Combinations – Looks for usernames 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

Included dictionaries:
- US SSN Keywords
- Credit Card Number Keywords
- ABA Routing Number Keywords

### Individual Taxpayer Identification Numbers (ITIN)

Described Content condition:
- US ITIN - Looks for a match to the US ITIN regular expression and a keyword from the US ITIN Keywords dictionary.

Included dictionary:
- US ITIN Keywords

### SWIFT Codes

Described Content condition:
- SWIFT Code Regex - Looks for a match to the SWIFT code regular expression and a keyword from the SWIFT Code Keywords dictionary.

Included dictionary:
- SWIFT Code Keywords

### UK Drivers License Numbers

Described Content condition:
- Contains a single compound condition with three parts: a single keyword from the UK Keywords dictionary, the pattern matching that of the UK driver’s license regular expression, and different combinations of the phrase driver’s license using a regular expression.

Included dictionary:
- UK Keywords
UK Electoral Roll Numbers

Described Content condition:
- Contains 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.

Included dictionaries:
- UK Keywords
- UK Electoral Roll Number Words

UK National Insurance Number

Described Content condition:
- 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.

Included dictionaries:
- UK NIN Keywords

UK Passport Numbers

Described Content conditions:
- 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).

Included dictionary:
- UK Passport Keywords

UK Tax ID Numbers

Described Content condition:
- 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.

Included dictionaries:
UK Tax ID Number Keywords

US Social Security Numbers

Described Content conditions:

- 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.

Included dictionaries:

- US SSN Keywords

Network security policy templates

The following table provides an overview of the premium network security enforcement pre-built policy templates.

See “About compliance policy templates” on page 302.

**Table B-13**  
Network security policy templates

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Diagrams</td>
<td>This policy detects computer network diagrams at risk of exposure.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Network Diagrams”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>on page 568.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>This policy detects evidence of hacking tools and attack planning.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Network Security”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>on page 569.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Files</td>
<td>This policy detects password file formats, such as SAM, /etc/password, and</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>See “Password Files”</td>
<td>/etc/shadow.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network Diagrams

Described Content conditions:

- 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.

Included dictionary:
Network Security

Described Content conditions:
- 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.

Included dictionary:
- Hacker Keywords
- Keylogger Keywords

Password Files

Described Content conditions:
- 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.

Included dictionary:
- Password Filenames

UK and international regulatory policy templates

This section describes the UK and international regulatory templates provided by Symantec Brightmail Gateway.

See “About compliance policy templates” on page 302.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caldicott Report</td>
<td>The Caldicott Report (December 1997) was a review commissioned by the UK Chief Medical Officer to make recommendations to improve the way the National Health service handles and protects patient information. The Caldicott Committee was set up to review the confidentiality and flows of data throughout the NHS for purposes other than direct care, medical research or where there is a statutory requirement for information. Its recommendations are now being put into practice throughout the NHS and in the Health Protection Agency.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data Protection Act 1998</td>
<td>The Data Protection Act 1998 (replacement of Data Protection Act 1984) set standards which must be satisfied when obtaining, holding, using or disposing of personal data in the UK. The Data Protection Act 1998 covers anything with personal identifiable information (for example, data about personal health, employment, occupational health, finance, suppliers, and contractors).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>EU Data Protection Directives</td>
<td>Directives 95/46/EC of the European Parliament deal with the protection of individuals with regard to the processing and free movement of personal data. This policy detects personal data specific to the EU directives.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Human Rights Act 1998</td>
<td>The Human Rights Act 1998 allows UK citizens to assert their rights under the European Convention on Human Rights in UK courts and tribunals. The Act states that &quot;so far as possible to do so, legislation must be read and given effect in a way which is compatible with convention rights.&quot; This policy enforces Article 8 by ensuring the private lives of British citizens stay private.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Table B-14  UK and international regulatory policy templates (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Described Content</th>
<th>Structured Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIPEDA</td>
<td>Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

See “PIPEDA” on page 574.

Caldicott Report

Described Content conditions:

- 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.

Structured Data conditions:

- 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.
Health Service) number. This data must appear in combination with a keyword from the Medical Treatment Keywords dictionary.

Included dictionaries:
■ Prescription Drug Names
■ Disease Names
■ Medical Treatment Keywords
■ UK NIN Keywords

Data Protection Act 1998

Described Content conditions:
■ 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 dictionaries:
- UK Keywords
- UK Electoral Roll Number Words
- UK NIN Keywords
- UK Tax ID Number Keywords
- UK Passport Keywords

**EU Data Protection Directives**

Structured Content conditions:
- 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.

**Human Rights Act 1998**

Described Content conditions:
- 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.

Structured Data conditions:
- UK Data Protection Act, Personal Data – 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.

Included dictionaries:
- UK Personal Data Keywords
- UK Keywords
UK Electoral Roll Number Words

PIPEDA

Described Content conditions:

- 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.

Structured Data conditions:

- 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

Included dictionaries:

- Canadian Social Ins. No. Words
- ABA Routing Number Keywords
- Credit Card Number Keywords

Page settings for adding a compliance folder

This section describes the Compliance Folder page settings.

See “About compliance folders” on page 346.

Table B-15  Add Compliance Folder page settings

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
Table B-15  Add Compliance Folder page settings (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send from</td>
<td>Specify the from header for incident notification messages.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specify the subject header for incident notification messages.</td>
</tr>
<tr>
<td>Notification</td>
<td>Edit the text of the notification. Symantec Brightmail Gateway will replace the variable <code>%NEW_COMPLIANCEMESSAGES%</code> with a list of incident numbers and the policies that triggered those incidents. You can type text before or after this variable, or you can delete the variable if desired. For example, you could type the following text to precede variable, replacing Name with the folder name: A new incident has been created. Please access the Name Compliance Folder for incident details.</td>
</tr>
<tr>
<td>Default</td>
<td>Click to restore the default notification settings.</td>
</tr>
<tr>
<td>OK</td>
<td>Save your changes to this incident notification template.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancel your changes to this incident notification template and return to the Add Compliance Folder page.</td>
</tr>
</tbody>
</table>

Compliance Conditions

This section describes the conditions that can be used with compliance policies and the corresponding filter tests.

See “About compliance policy conditions” on page 286.

Table B-16  Compliance conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Test against</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any part of the message</td>
<td>Dictionary</td>
<td>Profanity</td>
</tr>
<tr>
<td></td>
<td>Regular expression</td>
<td>ABA Routing Numbers</td>
</tr>
<tr>
<td></td>
<td>Pattern</td>
<td>Social Security number</td>
</tr>
<tr>
<td></td>
<td>Record resource</td>
<td>Customer phone numbers</td>
</tr>
<tr>
<td>Attachment content</td>
<td>Text within an attachment file</td>
<td>Find all attachments that contain the word &quot;discount&quot; more than three times.</td>
</tr>
<tr>
<td>Attachment type</td>
<td>An attachment list, file name, or MIME type</td>
<td>script.vbs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>application/octet-stream</td>
</tr>
<tr>
<td>Condition</td>
<td>Test against</td>
<td>Examples</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bcc: address</td>
<td>Bcc: (blind carbon copy) message header</td>
<td>jane example.com <a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Body</td>
<td>Contents of the message body. This component test is the most processing intensive, so you may want to add it as the last condition in a filter to optimize the filter.</td>
<td>You already may have won</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cc: address</td>
<td>Cc: (carbon copy) message header</td>
<td>jane example.com <a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Envelope HELO</td>
<td>SMTP HELO domain in message envelope</td>
<td>example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Envelope recipient</td>
<td>Recipient in message envelope</td>
<td>jane example.com <a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Envelope sender</td>
<td>Sender in message envelope</td>
<td>jane example.com <a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From: address</td>
<td>From: message header</td>
<td>jane example.com <a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From/To/Cc/Bcc Address</td>
<td>From: To:, Cc:, and Bcc: message headers</td>
<td>jane example.com <a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message header</td>
<td>Message header specified in the accompanying text field. A header is case-insensitive. Do not type the trailing colon in a header.</td>
<td>Reply-To reply-to Message-ID</td>
</tr>
<tr>
<td>Condition</td>
<td>Test against</td>
<td>Examples</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subject</td>
<td>Subject: message header</td>
<td>$100 FREE. Please Play Now!</td>
</tr>
<tr>
<td>To: address</td>
<td>To: message header</td>
<td>jane</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td>To/Cc/Bcc Address</td>
<td>To:, Cc:, and Bcc: message headers</td>
<td>jane</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td>Recipient</td>
<td>Email addresses, domain names, and country codes in dictionaries</td>
<td>jane</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td>Sender</td>
<td>Email addresses, domain names, and country codes in dictionaries</td>
<td>jane</td>
</tr>
<tr>
<td></td>
<td></td>
<td>example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:jane@example.com">jane@example.com</a></td>
</tr>
<tr>
<td>Message size</td>
<td>Size of the message in bytes, kilobytes, or megabytes, including the header and body is less than or greater than the specified value.</td>
<td>2000 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>200 KB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 MB</td>
</tr>
<tr>
<td>Is in the attachment list</td>
<td>Archive files</td>
<td>fy1998.arc</td>
</tr>
<tr>
<td></td>
<td>Document files</td>
<td>mystorysofar.msw</td>
</tr>
<tr>
<td></td>
<td>Executable files</td>
<td>startmeup.exe</td>
</tr>
<tr>
<td></td>
<td>Image files</td>
<td>lookatme.jpg</td>
</tr>
<tr>
<td></td>
<td>Multimedia files</td>
<td>seenontv.mov</td>
</tr>
<tr>
<td></td>
<td>If you have the Premium Content Compliance module licensed and enabled, you can also choose a premium attachment list.</td>
<td></td>
</tr>
</tbody>
</table>
### Table B-16  Compliance conditions (continued)

<table>
<thead>
<tr>
<th>Condition</th>
<th>Test against</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has the filename</td>
<td>Use DOS wildcard characters if needed to allow for variations</td>
<td>Find all attachment filenames that include attach*.exe (attached.exe, attachment.exe, attachments.exe)</td>
</tr>
<tr>
<td>Is MIME type</td>
<td>Filters attachment according to Multipurpose Internet Mail Extension type for non-US ASCII characters sets, non-textual message bodies, and multipart message bodies</td>
<td>MIME-type begins with video/</td>
</tr>
<tr>
<td>contains/does not contain a filename from dictionary</td>
<td>Dictionaries</td>
<td>ABA Routing Number Keywords</td>
</tr>
<tr>
<td>contains/does not contain a file extension from</td>
<td>Dictionaries</td>
<td>California Keywords</td>
</tr>
<tr>
<td>For all messages</td>
<td>Flags all email not filtered by another compliance policy.</td>
<td>(Not applicable)</td>
</tr>
</tbody>
</table>

### Table B-17  Filter tests

<table>
<thead>
<tr>
<th>Test type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains</td>
<td>Tests message content against words found in selected dictionary.</td>
</tr>
<tr>
<td>Matches regular expression/Does not match regular expression</td>
<td>Tests message content against user-specified regular expressions. Regular expressions combine alphanumeric characters with metacharacter variables to identify pattern variations.</td>
</tr>
<tr>
<td>Matches pattern/Does not match pattern</td>
<td>Tests message content against known regular-expression patterns such as those found in Social Security numbers or credit card numbers patterns</td>
</tr>
<tr>
<td>Contains/does not contain</td>
<td>Tests for the supplied text within the component specified. Sometimes called a substring test. You can in some cases test for frequency - the number of instances of the supplied text that appear.</td>
</tr>
<tr>
<td>Matches data in the Record resource</td>
<td>Compares message content with the data defined by the selected Record resource.</td>
</tr>
</tbody>
</table>
Table B-17  Filter tests (continued)

<table>
<thead>
<tr>
<th>Test type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starts with/does not start with ends with/does not end with matches exactly/does not match exactly</td>
<td>Equivalent to &quot;text.&quot; wildcard test using matches exactly. Equivalent to &quot;text.$&quot; wildcard text using matches exactly. Exact match for the supplied test.</td>
</tr>
<tr>
<td>Exists/does not exist</td>
<td>Tests whether the specified message header exists. For example, messages that include unwanted or nonstandard headers can trigger appropriate actions, such as Delete message or Create an incident. Similarly, messages that do not include standard or expected headers can trigger other actions that you determine for the policy.</td>
</tr>
<tr>
<td>Is equal to/Is greater than/Is less than</td>
<td>Compares message size with the specified number of bytes, kilobytes (KB), or megabytes (MB)</td>
</tr>
</tbody>
</table>

Notes:
All text tests are case-insensitive.
Some tests are not available for some components.

Attachment characteristics for attachment lists

This section describes the attachment list characteristics.
See “About attachment list resources” on page 311.

Table B-18  Attachment characteristics for attachment lists

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>True file type</td>
<td>Specifies an attachment type based on direct inspection of the type of file. You can use this to match files whose extensions may not accurately reflect their true file types. Each file type is a member of a specific file class.</td>
<td>Microsoft Word for Windows</td>
</tr>
<tr>
<td>True file class</td>
<td>Specifies an attachment type based on the class of file. You can use this to match files whose extensions may not match their true file classes.</td>
<td>Word Processor Document</td>
</tr>
</tbody>
</table>
Table B-18  Attachment characteristics for attachment lists (continued)

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>Part or all of a filename. A partial match for a file will match a file, such as “oxy” for “oxygen.txt”.</td>
<td>oxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>oxygen</td>
</tr>
<tr>
<td></td>
<td></td>
<td>oxygen.txt</td>
</tr>
<tr>
<td>Extension</td>
<td>A period followed by usually three letters at the end of a file that, by convention, indicates the type of the file.</td>
<td>.txt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.exe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.text</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.zip</td>
</tr>
<tr>
<td>MIME-type</td>
<td>The MIME type of the attachment in the email message. MIME is a standard for email attachments.</td>
<td>text/plain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>image/gif</td>
</tr>
<tr>
<td></td>
<td></td>
<td>application/msword</td>
</tr>
<tr>
<td></td>
<td></td>
<td>application/octet-stream</td>
</tr>
</tbody>
</table>

Email notification variable attributes

This section describes the variables available for use in email notifications.

See “About notifications” on page 294.

Table B-19  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 will be 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 will be 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 will be 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 will be replaced with a comma separated list of top-level attachments from the original message.</td>
</tr>
</tbody>
</table>
Compliance condition categories

This section describes the categories of compliance conditions provided by Symantec Brightmail Gateway.

See “About compliance policy conditions” on page 286.

Table B-20 Compliance condition categories

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Text in the Subject, Body or Attachments | Applies any of the following rules to match words, expressions, patterns, or structured data in the message subject, body, or attachments:  
- Contains n or more words from dictionary specified in the drop-down list.  
- matches/does not match regular expression that you enter in the text box.  
- matches/does not match pattern with pattern selected from the drop-down list.  
- Matches data in the Record Resource specified in the drop-down list according to the View and the Minimum number of occurrences required that you specify. |
Table B-20  Compliance condition categories *(continued)*

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Text in this specific part of the message | The policy condition applies one of the following rules to the specified message part and uses it to match the word, expression, or pattern that you specify:  
  - Text in the part of the message selected from the drop-down list.  
  - contains/does not contain *n* or more occurrences of the text string that you specify in the text box.  
  - starts with/does not start with/matches exactly/does not match exactly /ends with/does not end with the string that you enter in the text box.  
  - Regular expressions are designed to match on a line-by-line basis when configured to match against a message headers, but only match against the entire body text when configured to match against the message body or attachments.  
  - matches/does not match regular expression that you enter in the text box.  
  - matches/does not match pattern that select from the drop-down list.  
  If you select Message header from the Text in this specific part of the message drop-down list, you have the option to enter the header name and select exists/does not exist from the message header drop-down list. |
| Text in the specific part of the message header | Matches messages that contain or do not contain an email address, domain, or country code from a specific dictionary to either the envelope recipient or the envelope sender.  
  - Text in the part of the header selected from the drop-down list  
  - contains Email address selected from drop-down list  
  - from dictionary selected from drop-down list |
| Message size                        | Applies policy according to whether the size of the message and its attachments are less than, greater than, or equal to the specified number of bytes, kilobytes, or megabytes.  
  - Message size/Attachment size  
  - is equal/is greater then/is less than  
  - the number entered in the text box  
  - bytes/KB/MB |
Table B-20  Compliance condition categories (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File metadata</td>
<td>This condition applies the policy to attachments whose filenames match one of the specified criteria.</td>
</tr>
<tr>
<td></td>
<td>■ Is in the Attachment List selected from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>■ Has the filename that you enter in the text box</td>
</tr>
<tr>
<td></td>
<td>■ Is MIME type that you enter in the text box</td>
</tr>
<tr>
<td></td>
<td>■ contains/does not contain a file name from dictionary selected from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>■ contains/does not contain a file extension from dictionary selected from the drop-down list.</td>
</tr>
<tr>
<td>For all messages</td>
<td>For all messages not filtered by a higher-precedence policy.</td>
</tr>
<tr>
<td>Add Condition</td>
<td>Click this button to add this condition to the policy and return to the Email Content Compliance Policy page.</td>
</tr>
</tbody>
</table>

**Record system patterns**

This section describes the record patterns provided by Symantec Brightmail Gateway.

See “About creating a record resource for compliance policies” on page 318.
<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 beginning with 5 and whose second digit is a number from 1 to 5, separated into 4 groups of 4 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 beginning with 4 and separated into 4 groups of 4 digits separated by a space or hyphen, or any 12-digit number beginning 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 beginning with 34 or 37 and separated into 3 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 beginning with 30, 36, or 38 and separated into 3 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 beginning 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 beginning 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>Credit Card number</td>
<td>3123 4567 8901 1234</td>
<td>JCB: Any 16-digit number separated into 4 groups of 4 by a space or hyphen, beginning with 3; or any 15-digit number beginning with 2131 or 1800 and 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 B-21  Record system patterns (continued)

<table>
<thead>
<tr>
<th>System pattern</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
</table>
| Email          | jabberwocky@symantec.com  
mister_smith@senate.gov  
tom.swift@gadgetsarpa  
t-rex9@museum  
harry@hogwarts.edu.uk | Any alphanumeric string, which can be 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 Brightmail 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 will not validate harry@hogwarts.edu.uk or bilbo@canterbury.ac.Nz. However, Symantec Brightmail Gateway will validate mister_smith@senate.GOV. |
| IP address     | 1.2.3.4  
10.0.0.0  
18.255.30.41  
10.0.10.0/24  
10.0.10.0/1  
10.0.10.0/0 | Any grouping of four 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 Brightmail Gateway does not parse any terminal characters other than a 1- or 2-digit numeral preceded by a forward slash. Thus, 10.113.14.10a is not interpreted as a valid IP address. |
<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 Brightmail Gateway recognizes European-style numbers, where the comma serves as decimal point and periods separate groups of 3 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. This avoids the possibility that commas in numbers will be mistaken as field delimiters. Numbers that are larger than 8 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 Brightmail Gateway recognizes European-style numbers, where the comma serves as decimal point and periods separate groups of 3 digits. Fractions of a percent must be preceded by a numeral, including zero (0) if necessary, and expressed as a decimal. Only numbers adjacent to the percent sign (%) (no space) are regarded as valid percentages. The following patterns will not produce a match:</td>
</tr>
<tr>
<td></td>
<td>23.4%</td>
<td>.32</td>
</tr>
<tr>
<td></td>
<td>56.78%</td>
<td>32 percent</td>
</tr>
<tr>
<td></td>
<td>-1.089,01%</td>
<td>32per</td>
</tr>
<tr>
<td></td>
<td>-0.32%</td>
<td>5 3/4%</td>
</tr>
</tbody>
</table>
Table B-21  Record 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 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) 832-5555</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 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 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>

Perl-compatible regular expressions

This section describes the Perl-compatible regular expressions that can be used in compliance policies.

See “About using regular expressions in conditions” on page 327.

Table B-22  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>
</tbody>
</table>
Table B-22  Regular expression metacharacters *(continued)*

<table>
<thead>
<tr>
<th>Metacharacter/construct</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>$</td>
<td>Dollar sign: Represents the end of the input line. For example, A$ 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</td>
</tr>
<tr>
<td>*</td>
<td>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).</td>
</tr>
<tr>
<td>?</td>
<td>Question mark: Matches zero or one instance of the string to the immediate left of the question mark.</td>
</tr>
<tr>
<td>+</td>
<td>Plus sign: Matches one or more instances of the string to the immediate left of the plus sign.</td>
</tr>
<tr>
<td>\</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>[string]</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table B-22  Regular expression metacharacters *(continued)*

<table>
<thead>
<tr>
<th>Metacharacter/construct</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(string)</td>
<td>Parentheses: Groups parts of regular expressions, which gives the string inside the parentheses precedence over the rest.</td>
</tr>
<tr>
<td>(string)</td>
<td></td>
</tr>
</tbody>
</table>


Table B-23 describes the methods you can use to refine your search.

Table B-23  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$n</td>
</tr>
<tr>
<td>..</td>
<td>Match any two characters</td>
<td>jo..</td>
<td>john, josh, jo4#</td>
</tr>
<tr>
<td>.*</td>
<td>Match zero or more characters</td>
<td>sara.*</td>
<td>sara, sarah, sarahjane, saraabc%123</td>
</tr>
<tr>
<td>.*</td>
<td>s.<em>m.</em></td>
<td>sm, sam, simone, s321m$xyz</td>
<td></td>
</tr>
<tr>
<td>.*</td>
<td>sara.+</td>
<td>sara, sarahjane, saraabc%123</td>
<td></td>
</tr>
<tr>
<td>.+</td>
<td>s.+m.+</td>
<td>simone, s321m$xyz</td>
<td></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^*</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>
Perl-compatible regular expressions
Administering your product through the command line

This appendix includes the following topics:

■ About administering your product through the command line

About administering your product through the command line

Each appliance has a set of commands that you can use to configure, optimize and administer your system. Access these commands by logging into the system either through SSH or via the VGA or serial connections on the appliance. Help is available for all commands by typing `help command_name`.

**Note:** Square brackets ([ ]) indicate an optional statement. The pipe character (|) indicates that one of two statements can be specified. Text in greater- and less-than characters (<>) should be replaced with text that you specify.

The following commands are available:

■ agentconfig
■ cat
■ cc-config
■ clear
■ crawler
■ date
- db-backup
- db-restore
- deleter
- diagnostics
- dn-normalize
- dns-control
- eula
- grep
- help
- http
- ifconfig
- install
- iostat
- ldapsearch
- ls
- mallog
- malquery
- more
- mta-control
- mta-stats
- netstat
- nslookup
- passwd
- pause-mode
- ping
- reboot
- rebuildrpmdb
- rm
- route
- service
agentconfig

The `agentconfig` command allows you to 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 Scanner to re-allow the new Control Center IP to connect to the Scanners. The `agentconfig` command exits with a return value of zero if successful and non-zero if unsuccessful. The utility restarts the Agent when you add or delete an IP address to or from the allowed IP list unless the `-norestart` parameter is included in the command.

The `agentconfig` command has the following syntax:

```
agentconfig [-option] <ip>
```

where:

- `option` can be any of the actions listed in See Table C-1 on page 593.
- `ip` is the IP address to be acted upon as instructed by the value of the command provided.

Table C-1 lists the available actions for `agentconfig`.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-list or -l</td>
<td>Displays the allowed IP list.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-add or -a</td>
<td>Places a new entry in the allowed IP list. Validation is performed on the IP address.</td>
</tr>
<tr>
<td>-del or -d</td>
<td>Deletes an entry from the allowed IP list. A warning is displayed unless the -f parameter is used on the command line.</td>
</tr>
<tr>
<td>-norestart or -n</td>
<td>Indicates that the agent is not to be restarted after the allowed IP is changed.</td>
</tr>
<tr>
<td>-force or -f</td>
<td>Used with the -del option to bypass the deletion warning</td>
</tr>
<tr>
<td>-help or -h</td>
<td>Displays the usage for the agentconfig command.</td>
</tr>
</tbody>
</table>

**cat**

The `cat` utility reads files sequentially, writing them to the standard output. This command is part of the standard Linux command set, but has been modified in this implementation.

The `cat` command has the following syntax:

```
cat [files]
```

Type `help cat` from the appliance for online assistance.

**cc-config**

The `cc-config` lets users modify the maximum file size for the Control Center log and the time of retention for the Compliance Audit log. When applied to the Control Center log, `cc-config` writes command line parameters to the log4j properties file, and then restarts the Control Center.

The `cc-config` command has the following syntax:

```
cc-config <log> [level|days]
```

where:

- **log** is either `controlcenter` or `complianceaudit`.
- **level** is the logging level the Control Center log uses. Acceptable values are: `trace`, `debug`, `info`, `warn`, `error`, or `fatal`.
- **days** is the number of days to retain the Compliance Audit Log.

Type `help cc-config` from the appliance for online assistance.
The `clear` command removes logs, configuration information and other data as specified in a set of associated classes, and restarts the Brightmail Engine.

The `clear` command has the following syntax:

```
clear <class class ...>
```

where `class` can be any combination of the classes in Table C-2.

Table C-2 lists the available classes for the `clear` command.

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scannerlogs</td>
<td>Clears Scanner logs.</td>
</tr>
<tr>
<td>bcclogs</td>
<td>Clears the Control Center logs.</td>
</tr>
<tr>
<td>synclogs</td>
<td>Clears the LDAP synchronization logs.</td>
</tr>
<tr>
<td>mallog</td>
<td>Clears the message audit logs.</td>
</tr>
<tr>
<td>oslogs</td>
<td>Clears the operating system logs.</td>
</tr>
<tr>
<td>imlogs</td>
<td>Clears the IM logs.</td>
</tr>
<tr>
<td>alllogs</td>
<td>Clears Scanner and operating system logs.</td>
</tr>
<tr>
<td>scannerconfig</td>
<td>This command removes the on-disk configuration files for your Scanner. It does not affect the Scanner configuration information stored in the Control Center. Running this command restarts the appliance on which the command is run. After running this command, 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 prior to saving this information to disk. To do either of these actions, access Administration &gt; Hosts &gt; Configuration in the Control Center, select the Scanner, and click Edit. To recommit the information unchanged click the Save button, or edit any settings for this Scanner as necessary to correct improper configuration and then click Save. If you are manipulating the Scanner configuration of an independent Scanner appliance (not the appliance on which the Control Center is also running), you can delete the Scanner configuration completely and re-add it using the Add Scanner Wizard. This option is not available for an appliance that hosts both a Control Center and Scanner.</td>
</tr>
<tr>
<td>bccconfig</td>
<td>Clears Control Center configuration files.</td>
</tr>
</tbody>
</table>
### Table C-2 Classes for the clear command (continued)

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>osconfig</td>
<td>Clears operating system configuration files.</td>
</tr>
<tr>
<td>imconfig</td>
<td>Clears IM configuration files.</td>
</tr>
<tr>
<td>clearsockets</td>
<td>Clears all socket files in /var/tmp.</td>
</tr>
<tr>
<td>allconfig</td>
<td>Clears Scanner and operating system configuration files.</td>
</tr>
<tr>
<td>scannerdata</td>
<td>Clears all Scanner data and deletes any messages in any queues.</td>
</tr>
<tr>
<td>keystore</td>
<td>Restarts the Control Center and sets the Control Center to use the original demo certificate for HTTPS communication. This may be necessary if you can't log into the Control Center after setting a different user interface HTTPS certificate.</td>
</tr>
<tr>
<td>bccdata</td>
<td>Clears all Control Center data, including any license files.</td>
</tr>
<tr>
<td>sudata</td>
<td>Clears all software update cache data.</td>
</tr>
<tr>
<td>syncdata</td>
<td>Clears all LDAP synchronization data.</td>
</tr>
<tr>
<td>imdata</td>
<td>Clears all IM data.</td>
</tr>
<tr>
<td>ipfreq.db</td>
<td>Clears the IP database containing information about the quality of mail from given IPs.</td>
</tr>
<tr>
<td>alldata</td>
<td>Clears Scanner, operating system, and software update cache data.</td>
</tr>
<tr>
<td>password</td>
<td>Resets the password for the admin user.</td>
</tr>
<tr>
<td>bcchostacl</td>
<td>Clears the host access controls made on the Administration &gt; Settings &gt; Control Center page to allow access from all hosts.</td>
</tr>
<tr>
<td>oldqueuedata</td>
<td>Clears all old postfix queue data.</td>
</tr>
<tr>
<td>all</td>
<td>Clears all logs, configuration, password, synchronization and Scanner data, restoring your appliance to the original factory configuration.</td>
</tr>
<tr>
<td>help</td>
<td>Displays help.</td>
</tr>
</tbody>
</table>

Type `help clear` from the appliance for online assistance.

**crawler**

The crawler command searches the appliance file system for core dumps. Under normal circumstances, core dumps are accounted for in the standard clean-up process on each appliance. However, it is possible for occasional core dumps to be deposited in irregular locations. The crawler command examines the appliance
file system to find such instances. If it finds core dumps, they are compressed and moved into an area where they can be managed appropriately. An email about the existence of these files and their location is sent to the system administrator. A sample email might look like this:

Subject: found core

The following core files have been found:

/data/scanner/jobs/other/2007.06.30-00:44:00

/data/scanner/jobs/other/2007.02.14-09:22:00

Times are in GMT.

The crawler command has the following syntax:

crawler

For additional related information see deleter. Type help crawler from the appliance for online assistance.

date

The date command displays the date and time. This command is part of the standard Linux command set but has been modified in this implementation. Type help date from the appliance for online assistance.

Note: You cannot use this command to set the system date and time.

db-backup

The db-backup command backs up Symantec databases such as configuration settings, report data, log data, and incidents. You can store backups on the appliance or on a remote server. Only one instance of db-backup can be run at a time, as a lock file is created during command execution.

Backup files are compressed before they are written to disk to maximize disk space. The db-backup script calculates the amount of disk space the backup file requires and exits if at least twice this amount is not available on the /data partition.

If any part of the operation fails, db-backup fails and an explanatory message is displayed on the command line.
The `db-backup` command has the following syntax:

\[
\text{db-backup [options]}
\]

Table C-3 describes the syntax for the `db-backup` command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-f <file>` | Saves a backup. If you do not specify a file, the backup is saved to the appliance as `db-backup.brightmail.<Mon-Day-Year-Hour-Min>.full.manual.tar.bz2`. If you type a different filename for a backup to the appliance, you can only restore this backup using the `db-restore` command, not the Control Center restore facility. Use one of the following two protocols to save the backup to a remote server:
  - `scp` – Temporarily stores database dumps on the local appliance, checking files for data integrity, before copying them remotely using SCP (secure copy protocol). A username is required when using SCP as a transport, and the administrator is prompted for a password. Return codes are checked to ensure that the entire dump was copied to the remote host.
  - `ftp` – Temporarily stores database dumps on the local appliance, checking files for data integrity, before copying them remotely using FTP (file transfer protocol). Login will be attempted using the username and password 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 (`"`). Passwords containing single and double quotes are not valid. If no user name and password are specified, an anonymous login is used. Error checking ensures that the dumps and copies are complete.

If the file path ends with `/` the backup is stored in that directory using the default filename. If the file path ends with a file name the backup is saved with that name in the specified path.

| `-n` | Does not compress the backup file before writing it to disk. By default, backup files are compressed with bzip2. |
| `-l` | Lists existing backups on the appliance. |
| `-g` | Uses gzip file compression instead of bzip2. |
| `-t <type>` | The type of backup to perform. The following backup types are available:
  - `full` – Perform a full backup. Instead of full, you can type f or 1 instead.
  - `config-incidents` – Back up configuration and incident data. Instead of config-incidents, you can type ci or 2 instead.
  - `config-incidents-reports-logs` – Back up configuration, incident, report and log data. Instead of config-incidents-reports-logs, you can type cirl or 3 instead.

The default is full.
Table C-3  

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| -s <schedule> | The schedule name to include in the backup file name. Specifying a schedule name does not create automatic backups at that interval. Use the backup facility in the Control Center to create automatic scheduled backups. Use this option to separate backup files for retention purposes. See -b for more information. Specify one of the following schedule names:  
- manual  
- daily  
- weekly  
- monthly  
The default is manual. |
| -b <number> | Specifies the number of backups to keep on the appliance. Each unique combination of type and schedule is retained separately. The default is 5 for each type and schedule combination. |
| -d         | Purge old backups, retaining only the number of backups specified with the -b option. To remove all backups of a type and schedule combination, specify '-b 0'. If specified with -f, delete the specific named backup only. |
| -h         | Displays help for command usage. |

Table C-4  

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save a full backup on the appliance</td>
<td>db-backup</td>
</tr>
<tr>
<td></td>
<td>The oldest backup copy is deleted if it exceeds the number specified for db-backup -b &lt;number&gt; or 5 if db-backup -b has not been run.</td>
</tr>
<tr>
<td>Save a full backup on a remote server using SCP</td>
<td>db-backup -f scp://support@192.168.2.42/tmp/</td>
</tr>
<tr>
<td></td>
<td>The database backup file in the format db-backup.brightmail.&lt;date-time&gt;.full.manual.tar.bz2 is copied to 10.160.248.128 in the /tmp directory, using SCP. The support user account was specified.</td>
</tr>
<tr>
<td>Save a full backup on a remote server using FTP</td>
<td>db-backup -f ftp://jmuir:<a href="mailto:secret@host.symantecs.org">secret@host.symantecs.org</a>/user/jmuir/</td>
</tr>
<tr>
<td></td>
<td>The database backup file in the format db-backup.brightmail.&lt;date-time&gt;.full.manual.tar.bz2 is copied to host.symantecs.org in the /user/jmuir directory, using FTP. The jmuir user account and secret password were specified.</td>
</tr>
</tbody>
</table>

Type help db-backup from the appliance for online assistance.
db-restore

The db-restore command restores Symantec databases to an appliance from previously created backups located by default in your local backup store, or from remote locations via FTP, SCP, and HTTP. Only one instance of db-restore can run at a time, as a lock file is created during command execution. db-restore expects compressed backup files created by db-backup.

If you want to restore system policies in addition to system databases, you must use the Control Center. If any part of the operation fails, db-restore fails with a non-zero status and an explanatory message on the command line.

Note: After you restore an appliance that functions as your Control Center from a different IP address than the original IP address, you must reboot the appliance. If that appliance also hosts a Scanner, you should stop the Scanner first.

See “Restarting an appliance” on page 468.

See “Stopping and starting Scanners” on page 127.

The db-restore command has the following syntax:

db-restore [options] <filename>

where:

- **filename** is the name of the file used to restore your database information. Use the -l option to see a list of available files. The filename can be prefixed with SCP, FTP, or HTTP. Otherwise, it is assumed that the file resides in the local backup store.

  The syntax for a local filename is **filename**.

  In addition, you can prefix the path of the file as described in Table C-5.

Table C-5 lists the syntax for paths included in the db-restore command.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scp://user@host/path</td>
<td>Copies the backup file from its remote location using SCP (secure copy protocol). A complete path and filename, along with username, are required when using SCP as a transport. The administrator is prompted for a password. Return codes are checked to ensure that the entire dump was copied from the remote host, and the script exits with non-zero status on failure.</td>
</tr>
</tbody>
</table>
Table C-5  db-restore remote path syntax (continued)

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp://user:password[:port]/path</td>
<td>Copies files from their remote location using FTP (file transfer protocol). Login will be attempted using the username and password credentials 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 (&quot;'). Passwords containing single and double quotes are not valid. If no credentials are specified, anonymous login is used. Error checking ensures that the copies are complete.</td>
</tr>
<tr>
<td><a href="http://host%5B:port%5D/path">http://host[:port]/path</a></td>
<td>Allows for web-based transfer of a restore file from the Control Center. Using this mode, backups stored on your local appliance can be retrieved at either of the following addresses: <a href="http://host.domain.com:41080/brightmail/backups/file.bz2">http://host.domain.com:41080/brightmail/backups/file.bz2</a> <a href="https://host.domain.com/brightmail/backups/file.bz2">https://host.domain.com/brightmail/backups/file.bz2</a> 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 (&quot;'). Passwords containing single and double quotes are not valid. <strong>Note:</strong> If you are using Internet Explorer, be certain that Do not save encrypted pages to disk is unchecked. This option can be found in the Internet Explorer Tools menu, Internet Options menu, expanded Security view.</td>
</tr>
</tbody>
</table>

Table C-6 shows the syntax for the db-restore command.

Table C-6  db-restore options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>Forces a restore even when the version of appliance software in the backup file differs from the software running on the appliance.</td>
</tr>
<tr>
<td>-l</td>
<td>Lists existing backups in the local backup store</td>
</tr>
<tr>
<td>-h</td>
<td>Displays help for command usage</td>
</tr>
</tbody>
</table>

Type `help db-restore` from the appliance for online assistance.
deleter

The deleter command removes core files that you have been informed about via email. If not deleted, these files can be picked up by the diagnostics command and used in compiling system data as described in diagnostics.

The deleter command has the following syntax:

deletex <pathname/filename>

where:

- <pathname/filename> is the path and filename provided in email via crawler to the system administrator.
- list finds core memory dumps from crashes and lists them.
- -all deletes all the core files it finds.

An example of using deleter based on the first file shown in the sample email message from the crawler command would appear as follows:

deletex /data/scanner/jobs/other/2007.04.20-00:44:00

Times are in GMT.

See “crawler” on page 596.

Type help deleter from the appliance for online assistance.

diagnostics

The diagnostics command takes a snapshot of key elements on the appliance and sends it to the designated location via SCP or FTP.

The diagnostics command has the following syntax:

diagnostics [options] <url>

where:
Item | Description
--- | ---
**options** | ■ **--help** displays a help message showing command usage information  
■ **--verbose** turns on verbose reporting for command execution  
■ **--config** gathers only configuration data  
■ **--cores n** gathers only specified number of core files per component (the default is 9999)  
■ **--logs n** specifies the number of lines per log file to retrieve (the default is 20000)  
■ **--rules** gathers the rules directory (minus EDM data)  
■ **--edm** gathers EDM record sets from the rules directory  
■ **--ldap** gathers the active LDAP sync service addr.db file  
■ **--snmp** gathers the SNMP exec cache file  
■ **--include-old-queues** gathers queue data from old postfix queues

**Note:** With no options, `diagnostics gatherings --config --cores 9999 --logs 20000 --snmp`.

**url** | The location where the package of information is transmitted via SCP or FTP. Prefix the URL as described in Table C-7.
If file path ends with `/` then a directory is assumed and the default file name is appended to URL; otherwise the full path to the file is assumed.

Table C-7 shows the syntax for paths referenced by this command.

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>scp://user@host/path</strong></td>
<td>Copies the diagnostics package remotely using SCP. A username is required when using SCP as a transport, and the administrator is prompted for a password.</td>
</tr>
<tr>
<td><strong>ftp://user:password@host[:port]/path</strong></td>
<td>Copies the diagnostics package remotely using FTP. Login will be attempted using the username and password credentials 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 (&quot;'). Passwords containing single and double quotes are not valid. If no credentials are specified, anonymous login is used.</td>
</tr>
</tbody>
</table>
Table C-8  diagnostics sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a diagnostics file on an SCP server</td>
<td><code>diagnostics scp://'support'@10.160.248.128/tmp/</code></td>
</tr>
<tr>
<td></td>
<td>The diagnostics file (in the format, diagnostics.yy-mmm-dd-hh-mm.tar.gz) is copied to the 10.160.248.128 SCP server in the /tmp directory using the support account.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> &quot;Month&quot; is expressed in standard three-letter format, and not two-digit format.</td>
</tr>
</tbody>
</table>

Type `help diagnostics` from the appliance for online assistance.

**dn-normalize**

Some LDAP servers do not correctly/consistently apply whitespace and quote rules to the 'distinguished name' (dn). This can result in rejected groups due to mismatching of member entries. When dn normalization is enabled, a normalization function is applied to the data coming in from the LDAP server, which resolves mismatch problems.

**Note:** This process is not recommended for most customers; you should only apply normalization if you are experiencing a problem with LDAP synchronization resulting from non-normalized data in the LDAP source.

The `dn-normalize` command has the following syntax:

```
dn-normalize [options]
```

where option can be any of the following:

- **enable** stops ldapsync, enables dn normalization, and runs a utility to retroactively normalize any distinguished names already in MySQL, then restarts ldapsync. Depending on the size of your dataset, the normalization can take up to five minutes.
- **disable** stops ldapsync, disables dn normalization, starts ldapsync, and prints a message advising that you perform a 'full sync' on any existing LDAP Sync sources.
- **status** reports whether dn normalization is enabled ('YES') or disabled ('NO').

Type `help dn-normalize` from the appliance for online assistance.
dns-control

The `dns-control` command manages local caching for the name server. The command has the following syntax:

```
dns-control <command>
```

where command is any of the following:

- `start` starts the local caching name server.
- `stop` stops the local caching name server.
- `restart` restarts the local caching name server.
- `status` displays the status of the local caching name server.
- `flush` flushes the cache.
- `list` lists the locally configured name servers for the resolver.
- `trace` increments the tracing (debug) level by +1.
- `notrace` disables tracing (debug).

Type `help dns-control` from the appliance for online assistance.

eula

The `eula` command displays the End User License Agreement.

grep

The `grep` command searches within redirected output from any other command available in the appliance. This command is part of the standard Linux command set but has been modified in this implementation. Type `help grep` from the appliance for online assistance.

help

The `help` command displays a list of available commands on the appliance.

The `help` command has the following syntax:

```
help
```
http

The `http` command enables or disables HTTP access for your appliance. By default, each appliance has the HTTPS Web server enabled and the HTTP Web server disabled. Using the `http` command has no effect on HTTPS access. After executing the command, the Control Center must be restarted with the service command for the change to take effect.

The `http` command has the following syntax:

```
http <on|off>
```

where `on` enables HTTP access and `off` disables HTTP access.

Type `help http` from the appliance for online assistance.

Note: HTTP access is available only from localhost.

ifconfig

The `ifconfig` command displays the status and configuration of network interfaces and can make temporary changes to interface configurations. This command is part of the standard Linux command set, but has been modified in this implementation.

Type `help ifconfig` from the appliance for online assistance.

install

The `install` command loads the designated version of software as an upgrade to the appliance.

Warning: Installing earlier versions of the appliance software is not supported.

The `install` command has the following syntax:

```
install <version>
```

where `<version>` is an available version of Symantec Brightmail Gateway appliance software.

Type `help install` from the appliance for online assistance.
iostat

The `iostat` command monitors system input/output device loading by observing the time devices are active in relation to their average transfer rates.

The `iostat` command has the following syntax:

```bash
iostat <flags>
```

Type `help iostat` from the appliance for online assistance.

ldapsearch

The `ldapsearch` command allows you to perform LDAP logon authentication and see your Query Base DN messages in full form.

The syntax for the `ldapsearch` command is as follows:

```bash
ldapsearch [options] [filter [attributes...]]
```

where:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>options</td>
<td>Specifies search options</td>
</tr>
<tr>
<td>filter</td>
<td>Specifies an RFC-2254-compliant LDAP search filter</td>
</tr>
<tr>
<td>attributes</td>
<td>Specifies a list of attribute descriptions separated by white space and that can include:</td>
</tr>
<tr>
<td></td>
<td>■ 1.1 - No attributes</td>
</tr>
<tr>
<td></td>
<td>■ * - All user attributes</td>
</tr>
<tr>
<td></td>
<td>■ + - All operational attributes</td>
</tr>
</tbody>
</table>

This syntax corresponds to the following:

```bash
ldapsearch -x -h 'customers ldapsearch hostname' -p 'ldap server port' -D 'bind name (dn)' -w 'password' -b 'query start' 'query filter' 'Email alias attribute' 'Transport attribute'
```

where:

- options are: -x -h 'customers ldapsearch hostname' -p 'ldap server port' -D 'bind name (dn)' -w 'password' -b 'query start'
- filter is: 'query filter'
- attributes are: 'Email alias attribute' 'Transport attribute'
Options are divided into search options and common options. Search options can be any of the following:

<table>
<thead>
<tr>
<th>Search Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a deref</td>
<td>One of never, always, search, or find. The default is never.</td>
</tr>
<tr>
<td>-A</td>
<td>Retrieve attribute names only (no values).</td>
</tr>
<tr>
<td>-b basedn</td>
<td>Specifies the base dn to be used for the search. This can include the query start, query filter, email alias attribute, and transport attribute.</td>
</tr>
<tr>
<td>-F prefix</td>
<td>URL prefix for files. The default URL prefix is file:///temp/.</td>
</tr>
<tr>
<td>-l limit</td>
<td>Specifies the allowable time limit for the search in seconds.</td>
</tr>
<tr>
<td>-L</td>
<td>Specifies that responses are printed in LDIFV1 format.</td>
</tr>
<tr>
<td>-LL</td>
<td>Specifies that responses are printed in LDIF format without including comments.</td>
</tr>
<tr>
<td>-LLL</td>
<td>Specifies that responses are printed in LDIF format without including comments or version information.</td>
</tr>
<tr>
<td>-s scope</td>
<td>Specifies a scope for the search which can be one of base, one, or sub.</td>
</tr>
<tr>
<td>-S attr</td>
<td>Requests that the search results be sorted by the specified attribute.</td>
</tr>
<tr>
<td>-t</td>
<td>Writes binary values to files in a temporary directory.</td>
</tr>
<tr>
<td>-tt</td>
<td>Writes all values to files in a temporary directory.</td>
</tr>
<tr>
<td>-T path</td>
<td>Writes files to the specified directory. The default is /tmp.</td>
</tr>
<tr>
<td>-u</td>
<td>Includes user-friendly names in the search output.</td>
</tr>
<tr>
<td>-z limit</td>
<td>Specifies the number of entries returned from the search.</td>
</tr>
</tbody>
</table>

Common options include:

<table>
<thead>
<tr>
<th>Common option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d level</td>
<td>Sets the LDAP debugging level.</td>
</tr>
<tr>
<td>-D</td>
<td>Specifies the bind name (dn) for the user. For example: -D &quot;user_4&quot;.</td>
</tr>
<tr>
<td>-f filename</td>
<td>Reads operations from the specified file.</td>
</tr>
<tr>
<td><strong>Common option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>-h</td>
<td>Specifies the host name for an LDAP server at your site. For example: <code>-h 'ldap_server_1'</code>.</td>
</tr>
<tr>
<td>-H URI</td>
<td>Specifies LDAP Uniform Resource Identifiers.</td>
</tr>
<tr>
<td>-I</td>
<td>Uses SASL interactive mode.</td>
</tr>
<tr>
<td>-k</td>
<td>Uses Kerberos authentication.</td>
</tr>
<tr>
<td>-K</td>
<td>Uses Kerberos authentication, but only step 1 of the Kerberos bind is performed.</td>
</tr>
<tr>
<td>-M or -MM</td>
<td>Enables Manage DSA IT control. Using -MM makes this critical.</td>
</tr>
<tr>
<td>-n</td>
<td>Shows what would be done but does not perform a search.</td>
</tr>
<tr>
<td>-O props</td>
<td>Specifies SASL security properties.</td>
</tr>
<tr>
<td>-p</td>
<td>Specifies the port for the LDAP server to be used in the query. For example: `-p &quot;389&quot;.</td>
</tr>
<tr>
<td>-P version</td>
<td>Specifies a protocol version. The default is 3.</td>
</tr>
<tr>
<td>-Q</td>
<td>Invokes SASL quiet mode.</td>
</tr>
<tr>
<td>-R realm</td>
<td>Specifies an SASL realm.</td>
</tr>
<tr>
<td>-U authcid</td>
<td>Specifies an SASL authentication identity.</td>
</tr>
<tr>
<td>-v</td>
<td>Set verbose mode. Diagnostics are written to the standard output.</td>
</tr>
<tr>
<td>-w</td>
<td>Specifies the password for the given bind name (dn). This can be used for simple authentication.</td>
</tr>
<tr>
<td>-W</td>
<td>Prompts for the bind password.</td>
</tr>
<tr>
<td>-x</td>
<td>Specifies the use of simple authentication and voids the use of SASL authentication.</td>
</tr>
<tr>
<td>-X authzid</td>
<td>Specifies an SASL Authorization identity: dn:&lt;dn&gt; or u:&lt;user&gt;.</td>
</tr>
<tr>
<td>-Y mech</td>
<td>Specifies an SASL mechanism.</td>
</tr>
<tr>
<td>-Z or -ZZ</td>
<td>Starts a TLS request. Use -ZZ to require a successful response.</td>
</tr>
</tbody>
</table>
Table C-9  ldapssearch sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
</table>
| Get a list of attributes for a user in Active Directory   | ldapsearch -v -h 10.160.248.32 -D "CN=Administrator,CN=Users,DC=bmi,DC=qa" -w <password> -x -b "CN=Users,DC=bmi,DC=qa" "(sAMAccountName=guest)"
|                                                           | A list of attributes for the user guest located in Users container is displayed from the ldapssearch 10.160.248.32, using the administrator account ("CN=Administrator,CN=Users,DC=bmi,DC=qa") for the bmi.qa domain. |
| Get a list of all objects in the Active Directory         | ldapsearch -v -h 10.160.248.32 -D "CN=Administrator,CN=Users,DC=bmi,DC=qa" -w <password> -x -b "DC=bmi,DC=qa"
|                                                           | All objects, starting from the top-level search base (DC=bmi,DC=qa), are displayed from the ldapsserver 10.160.248.32, using the administrator account ("CN=Administrator,CN=Users,DC=bmi,DC=qa") for the bmi.qa domain. |

ls

The `ls` command lists directory contents. This command is part of the standard Linux command set but has been modified in this implementation. Type `help ls` from the appliance for online assistance.

mallog

The `mallog` command lists, backs up, and restores message audit log data residing on the appliance.

The `mallog` command has the following syntax:

```
mallog [--list|--help]
mallog [--backup|--restore] <url>
```

where:

- `--list` lists individual message audit logs on the file system, including their timestamps and sizes as returned by `stat()`.
- `--backup` creates a backup of the message audit logs in tar format and uploads the resulting file to the specified URL. Supported upload schemes are scp and ftp.
- `--restore` restores message audit logs from the specified URL. Existing logs are overwritten. The `mallog` command attempts to ensure that the backup
specified by url is a valid message audit log backup and the backup is not corrupt.

- url is the location to which the package of information is transmitted by SCP or FTP. Prefix the URL as described in Table C-7.

**Note:** Running `mallog --backup` or `mallog --restore` stops email processing 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.

Available log files include:

- /data/logs/scanner/audit_bmengine_log*
- /data/logs/scanner/audit_hub_log*
- /data/logs/scanner/audit_mte_log*
- /data/logs/scanner/audit_mta_log*

Message audit log data is stored in binary format in the log files. To view message audit log data, use the `malquery` command or the Message Audit Logs status page in the Control Center.

See “malquery” on page 612.

See “About message audit logging” on page 418.

Message audit log data can be logged to a remote syslog.

See “Configuring remote logging to syslog” on page 412.

**Table C-10** mallog sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>List all available message audit log files</td>
<td>mallog --list</td>
</tr>
<tr>
<td>Back up all log files using scp</td>
<td>mallog --backup scp://jmuir@10.160.240.161/home/jmuir/</td>
</tr>
<tr>
<td>Restore all log files using scp</td>
<td>mallog --restore scp://jmuir@10.160.240.161/home/jmuir/mallog.Nov-06-08-16-09.tar.gz</td>
</tr>
</tbody>
</table>
**malquery**

You can track messages in the Control Center using Message Audit Logs on the Status menu. Alternatively, you can use the `malquery` command to track messages. Use `malquery` instead of the Control Center for complex queries or queries where you expect voluminous data.

`malquery` only returns data for the Scanner on which it is run.

**Scalability of message audit logging**

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.

**malquery syntax**

The syntax for `malquery` is as follows:

```
malquery -l <start time YYYYMMDDHHMM>,<end time YYYYMMDDHHMM>|-g <start time epoch>,<end time epoch> -u <uid> [-u <uid> ...] | -e <event name[,arg #]>=|*><string> [-e <event name[,arg #]>=|*><string> ...] [-m #] [-o <filename>] [-d] [-v]
```

Table C-11 describes the options available for `malquery`.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l &lt;start time&gt;,&lt;end time&gt;</td>
<td>Local time range to search. Specify the start and end time in the following format (local time - 24 hour format): yyyymmddhhmm.</td>
</tr>
<tr>
<td>-g &lt;start time&gt;,&lt;end time&gt;</td>
<td>GMT time range to search. Specify the start and end time in UNIX epoch time, a 10-digit number which is the number of seconds since January 1, 1970, 00:00 o'clock.</td>
</tr>
<tr>
<td>-e &lt;event name[,arg #]&gt;=</td>
<td>*&gt;&lt;string&gt;</td>
</tr>
<tr>
<td>-u &lt;UID&gt;</td>
<td>Unique audit IDs to return results for.</td>
</tr>
</tbody>
</table>
Table C-11  malquery options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-o &lt;filename&gt;</td>
<td>Output XML results to the specified filename.</td>
</tr>
<tr>
<td>-m &lt;number&gt;</td>
<td>Used to control the number of results returned from malquery. This is not a precise throttle.</td>
</tr>
<tr>
<td>-d</td>
<td>When specified with multiple -e arguments, the -e arguments are connected by the OR logical operator rather than by the default AND operator.</td>
</tr>
<tr>
<td>-v</td>
<td>Verbose mode.</td>
</tr>
</tbody>
</table>

The following query would list all messages for the recipient pietro@symantecs.org between May 1, 2006 and May 31, 2006.

```
malquery -l 200605010000,200605312359 -e RCPTS="pietro@symantecs.org"
```

malquery output format

The output from malquery is in .xsd format, for example:

```
<malResults count="message result count">
  <message UID="uid">
    <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>
```

Format of audit logs

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.

Table C-12 describes the audit log parameters.

Table C-12  Format of audit logs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTC time stamp</td>
<td>The current time in UTC, encoded in UNIX epoch time format</td>
</tr>
</tbody>
</table>
Table C-12  Format of audit logs *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>The unique audit ID for the message (not UNIX user identifier). The format of the audit ID is: <code>&lt;First IP address in hex&gt;-&lt;ThreadID &amp; ProcessID in hex&gt;-&lt;Protected 2 digit counter&gt;-&lt;UTC Time in hex&gt;-&lt;Random number, seeded with millisecond timer, in 8 character padded hex&gt;</code>. The audit ID is always 41 bytes in length. The audit ID is stored in the message in a X-AuditID: header.</td>
</tr>
<tr>
<td>Event ID</td>
<td>The type of audit event being logged. Some event IDs are followed by parameters. See “Audit log events” on page 614.</td>
</tr>
</tbody>
</table>

**Note:** The order of events for a given UID in the audit log is not relevant. The data is intended to be gathered and interpreted independent of any implied order.

**Audit log events**

These audit log events can be queried using the Control Center or `malquery`.

**ACCEPT**

An inbound or outbound mailflow has accepted the message.

- **Logging module:** Accepting MTA
- **Parameters:** `<IP address>:<port>`
- **Count:** One ACCEPT per audit ID
- **State:** The message is at least in the inbound or outbound queue

**Example:**

```
UTC|UID|ACCEPT|10.240.190.2:25
```

**ATTACH**

The viruses or worms found in the message attachments.

- **Logging module:** Brightmail engine
- **Parameters:** The filenames of one or more attachments
- **Count:** Potentially multiple ATTACH events per audit ID
The message has been filtered, and is at least in the delivery queue.

Example:

UTC|UID|ATTACH|virus.exe|internal.doc

**DELIVER**

Message was handed off to another MTA.

**Note:** There may be more than one DELIVER event for a single audited message, or recipient, as delivery can succeed or fail per recipient, and per target destination.

**Logging module**

MTA or Brightmail Engine

**Parameters**

- The IP address and port of the MTA the message was to, in the form of `<IP address>:<port>`
- One or more email addresses to which the message was successfully delivered

**Count**

Multiple DELIVER events per audit ID; potentially multiple DELIVER events per recipient

**State**

The message has been filtered and is at least in the delivery queue; some or all recipients have been delivered to the next hop

Example:

UTC|UID|DELIVER|10.240.190.45:25|recip@domain.tld|recip1@domain.tld

**IRCPTACTION**

The actions taken per recipient after distribution list expansion.

Specify `-e IRCPTACTION="search string"` to search for IRCPTACTION by itself or specify `-e RCPTS ="search string"` to search for both IRCPTACTION and ORCPTS

**Logging module**

Message transformation engine

**Parameters**

- The recipient’s email address
- One or more action summaries for the recipient
Count
Multiple IRCPTACTION events per audit ID; potentially multiple IRCPTACTION events per recipient.

State
Message has been filtered, and is at least in the delivery queue

Example:
UTC|UID|IRCPTACTION|user2@domain.com|Subject Markup|Forward

MSGID
The contents of the Message-ID header, not the unique message ID added for the message audit logs.

Logging module
Brightmail engine

Parameters
The RFC822 Message-ID header

Count
One per audit ID

State
The message has been filtered, and is at least in the delivery queue

Example:
UTC|UID|MSGID|200607052345.LBB05394@symantecs.org

ORCPTS
The original recipients of a message before alias, distribution list, or masquerading changes as received by the accepting MTAs.

Specify -e ORCPTS="search string" to search for ORCPTS by itself or specify -e RCPTS ="search string" to search for both IRCPTACTION and ORCPTS

Logging module
Accepting MTA

Parameters
One or more RFC821 recipient addresses

Count
One per audit ID

State
The message is at least in the inbound or outbound queue

Example:
UTC|UID|ORCPTS|user1@example.com|user2@example.com
**SENDER**
The original sender of a message as received by the accepting MTAs.

Logging module       Accepting MTA
Parameters           One RFC821 sender address
Count                One per audit ID
State                Message is at least in the inbound or outbound queue

Example:

UTC|UID|SENDER|muir@symantecs.org

**SOURCE**
The origin, internal or external, of the accepting MTAs. Example:

Logging module       Accepting MTA
Parameters           The string "external" or the string "internal"
Count                One per audit ID
State                If "external," the message is at least in the inbound queue; if "internal," the message is at least in the outbound queue

Example:

UTC|UID|SOURCE|external

**SUBJECT**
The message subject line.

Logging module       Brightmail engine
Parameters           The subject line of the message
Count                One per audit ID
State                Message has been filtered, and is at least in the delivery queue

Example:

UTC|UID|SUBJECT|Make $$$ Fast!!!
VERDICT
The verdict, group policy, and filtering policy that was triggered on the message per recipient.

Logging module
Brightmail engine

Parameters
- The intended recipient
- The verdict for the intended recipient
- The group policy used to determine the filtering policy
- The filtering policy used

Count
Multiple VERDICT events per message

State
Message has been filtered and is at least in the delivery queue

Example:
UTC|UID|VERDICT|user1@domain.tld|spam|default|Default Spam Policy

VIRUS
The viruses or worms found in the message.

Logging module
Brightmail engine

Parameters
One or more virus or worm identification strings

Count
One per audit ID

State
Message has been filtered and is at least in the delivery queue

Example:
UTC|UID|VIRUS|sobig|notsobig.win32

Audit log retention
Audit logs older than the current day are rolled over to a filename appended with the local date in the form yyyyMMdd. Audit logs older than the default retention period of 30 days are deleted.
### Table C-13  
malquery sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get tracking info for messages sent between 10:00am and 4:00pm on June 18, 2007</td>
<td><code>malquery -l 200706181000,200706181600 -e ORCPTS*</code></td>
</tr>
<tr>
<td>Get tracking info for messages sent to a recipient between 10:00am and 4:00pm on June 18, 2007</td>
<td><code>malquery -l 200706181000,200706181600 -e ORCPTS=user@org.qa</code></td>
</tr>
<tr>
<td>Get tracking info for messages quarantined between 10:00am and 4:00pm on June 18, 2007</td>
<td><code>malquery -l 200706181000,200706181600 -e IRCPTACTION=quarantine</code></td>
</tr>
<tr>
<td>Get tracking info for messages that received a spam verdict between 10:00am and 4:00pm on June 18, 2007</td>
<td><code>malquery -l 200706181000,200706181600 -e VERDICT=spam</code></td>
</tr>
</tbody>
</table>

### more

The `more` command displays output, one screen at a time, for redirected output from any other appliance command. This command is part of the standard Linux command set but has been modified in this implementation. Type `help more` from the appliance for online assistance.

### mta-control

The `mta-control` command allows you to run additional instances of the MTA, query MTA instances, and control specific elements within MTA message processing, such as flushing message queues.

See “MTA and message queue behavior” on page 111.

**Note:** When specifying output filenames and paths, passwords, email addresses, and user names (for exporting), the ~ (tilde) character must not be used—specify the full pathname.

The `mta-control` command has the following syntax:

```
mta-control <instance> <command>
```

where:
- **instance** is one of the following MTA queues:
  - inbound
  - outbound
  - delivery
  - all

- **command** is one of the following:
  - start – Starts the instance
  - stop – Stops the instance
  - status – Displays the current status. The status can be: running, not running, enabled or disabled.
  - restart – Restarts the instance
  - flush – Reattempts delivery for all queued messages
  - delete-msgs-by-sender <regexp> – Deletes from the queue all messages with Envelope Sender that matches the given Perl regexp (case insensitive).
  - delete-msgs-by-rcpt <regexp> – Deletes from the queue all messages with an Envelope Recipient that matches the given Perl regexp (case insensitive). Note that this deletes the entire *msg* not just the recipient.
  - delete-msg-by-id <queue-ID> – Deletes the message with the given queue-ID from the queue.
  - delete-all-msgs – Deletes all messages from the queue
  - export-msg-by-id <queue-ID> [URL] – Export the message with the given queue-ID from the queue, saving it at the specified URL. If the URL is missing, print the message data to the screen. When the username or password is part of URL it should be taken in quotes if it has any special shell characters in it. If the transport and path specified ends with / then it is assumed to be a directory and a default file name is appended to it. Otherwise a full path to the file is assumed.
    **URL syntax:** scp://'user'@host/path
    (User is prompted for password)
    ftp://'user':'password'@host[:port]/path
  - query-queue – Queries the message queue based on one or more provided parameters. The following optional parameters are available: sender_match=<perl regexp>, rcpt_match=<perl regexp>, deferred, include_subject, start=N, limit=N, format=<neat|xml>.
sender_match, rcpt_match and deferred are logically ANDed together if present. The intermediate result set after applying these matches is sorted by date, and then the start and limit are applied: $start-1 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.

**Note:** For the following bad message queue commands, use **all** instead of a **<queue-ID>** to apply the command to all bad messages in the queue.

- **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 <instance> bad-msg-export <queue-ID>`. If the username or password is part of the URL, enclose it in quotes if it has any special shell characters in it. If the URL and path specified ends with /, it is assumed to be a directory and a default filename is appended to it. Otherwise a full path to the file is assumed.
- **bad-msg-delete <queue-ID>** – Delete the message.
- **bad-msg-bypass <queue-ID>** – Submit the message for delivery to the original recipients, bypassing scanning.
- **bad-msg-forward <queue-ID> <address>** – Submit a copy of the message for delivery to the given address, bypassing 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.

**Note:** Do not attempt to rescan the offending message until a hotfix has been implemented.

<table>
<thead>
<tr>
<th>Table C-14</th>
<th>mta-control sample usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td>Get the queue-id of messages in delivery queue</td>
<td><code>mta-control delivery query-queue</code></td>
</tr>
</tbody>
</table>
### mta-control sample usage (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>View a raw message in the delivery queue using a message queue-id</td>
<td><code>mta-control delivery export-msg-by-id 00/00-25597-EFD46794</code></td>
</tr>
<tr>
<td>Export a specific message from the delivery queue a message queue-id</td>
<td><code>mta-control delivery export-msg-by-id 00/00-25597-EFD46794 scp://'support'@10.160.248.128/tmp/</code></td>
</tr>
<tr>
<td></td>
<td>In this example, the message with queue-id 00/00-25597-EFD46794 is exported to the 10.160.248.128 SCP server in the /tmp directory, using the support account.</td>
</tr>
</tbody>
</table>

### Providing bad message information to Symantec

The information required to diagnose an issue can vary widely depending on the nature of the problem being encountered. If your system experiences a content-related failure (meaning that the content of a particular message caused a crash), you can provide the message and other data to Symantec to assist in preventing this issue from occurring in the future.

If you choose to do this, please provide as much of the following data as possible:

- The maillog file, found at /data/logs/maillog
- The Brightmail Engine log, found at /data/logs/scanner/bmsrver_log
- If possible, a copy of the offending mail message.
- If a Brightmail Engine crash was involved, a tar file containing the contents of the directory generated at the time of the crash:
  
  /data/scanner/jobs/bmserver/<date-time>
  
  This directory, if it exists, should include a compressed core file, a back trace from the time of the crash, and an emitted message.
- The output of the `diagnostics` command.

These items will usually give Symantec enough information to begin the triage process.

### mta-stats

The `mta-stats` command reports MTA statistics.

```
mta-stats <key> <key> <...
```

where `key` can be any of the following MTA elements:

- inbound_listener_connections
outbound_listener_connections
- delivery_connections
- inbound_queued_msgs
- outbound_queued_msgs
- delivery_queued_msgs
- inbound_deferred_msgs
- outbound_deferred_msgs
- delivery_deferred_msgs
- inbound_queue_size
- outbound_queue_size
- delivery_queue_size
- inbound_listener_data_rate
- inbound_listener_msg_rate
- outbound_listener_data_rate
- outbound_listener_msg_rate
- delivery_data_rate
- delivery_msg_rate

If you do not specify a key, mta-stats displays MTA statistics for all available keys.

Type help mta-stats from the appliance for online assistance.

netstat

The netstat command prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. This command is part of the standard Linux command set but has been modified in this implementation.

The netstat command has the following syntax:

netstat <flags>
### Table C-15  netstat sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display network connections</td>
<td>netstat -an</td>
</tr>
<tr>
<td>Display routing table</td>
<td>netstat -r</td>
</tr>
</tbody>
</table>

**Type** `help netstat` from the appliance for online assistance.

### nslookup

The `nslookup` command performs a DNS lookup of the given hostname or IP address. This command is part of the standard Linux command set, but it has been modified for this implementation.

The `nslookup` command has the following syntax:

```
nslookup <hostname|IP address>
```

**Table C-16  nslookup sample usage**

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup MX records for a domain (yahoo.com, for example)</td>
<td>nslookup -querytype=mx yahoo.com</td>
</tr>
</tbody>
</table>

**Type** `help nslookup` from the appliance for online assistance.

### passwd

The `passwd` command changes the password for the admin login and is part of the operating system.

The `passwd` command has the following syntax:

```
passwd
```

**Type** `help passwd` from the appliance for online assistance.

### pause-mode

Holds messages in the queue for future delivery. This mode can be particularly useful if you want to pause incoming messages while waiting for new virus definitions.

The pause-mode command syntax is as follows:
pause-mode <normal|pause|reject|status>

where:
- normal accepts and processes mail normally.
- pause accepts inbound and outbound messages; holds messages in queues for future scanning and delivery.
- reject rejects incoming messages; scanning and delivery of already received messages continues. This selection is particularly 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 \texttt{service not available (450)} error message. Once this option is selected, all previously received messages are processed, but no new messages are accepted.
- status views the current mode.

See “MTA and message queue behavior” on page 111.

**ping**

The \texttt{ping} command tests, via data packet, the transfer of that data between the issuing machine and the given hostname or IP address. All arguments are permitted. This command is part of the standard Linux command set, but it has been modified in this implementation. Type \texttt{help ping} from the appliance for online assistance.

The \texttt{ping} command has the following syntax:

\texttt{ping <hostname|IP address>}

**reboot**

The \texttt{reboot} command reboots the appliance and is part of the operating system.

The \texttt{reboot} command has the following syntax:

\texttt{reboot}

Type \texttt{help reboot} from the appliance for online assistance.

\textbf{Note:} Depending on your deployment, migration can take up to several hours to complete. Do not reboot your computer during this time; doing so can result in database corruption.
To force the system to reboot, type `reboot -f`. This command reboots the system and deletes all files owned by user `mailwall` in the following directories:

- /temp
- /var/temp

**Warning:** Because rebooting your system during migration can cause database corruption, use caution when issuing this command.

**rebuildrpmdb**

The `rebuildrpmdb` command recreates the RPM database for the appliance. The `rebuildrpmdb` command has the following syntax:

```
rebuildrpmdb
```

Type `help rebuildrpmdb` from the appliance for online assistance.

**rm**

The `rm` command attempts to remove the non-directory type files specified on the command line. This command is part of the standard Linux command set, but it has been modified in this implementation. Type `help rm` from the appliance for online assistance.

**route**

The `route` command allows you to view routing tables or to add entries to a routing table temporarily. Its primary use is for viewing the routing tables. Type `help route` from the appliance for online assistance.

**service**

The `service` command allows you to change the status of various services. The `service` command has the following syntax:

```
service <component_name> <command>
```

where:

- `component_name` can be any one of the following:
  - `afasnmpd`
controlcenter

ldapsync

agent

connector

mta

imrelayd

mysql

osconfig

percnmpd

snmpd

lsisnmpd

stunnel

smsswapfile

command can be any one of the following:

- start
- stop
- restart
- status
- condrestart

**Note:** Issuing `service <component_name> condrestart` restarts the component only if it is currently running.

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop the Brightmail Engine and MTA</td>
<td><code>service mta stop</code></td>
<td>Notice that Brightmail Engine is part of MTA service.</td>
</tr>
<tr>
<td>Stop the Conduit and LiveUpdate</td>
<td><code>service connector stop</code></td>
<td>Also applies to jlu-controller</td>
</tr>
</tbody>
</table>

Type `help service` from the appliance for online assistance.
set-control-center-port-443

The `set-control-center-port-443` command enables or disables Web access to the Control Center using port 443. When port 443 access is enabled, you can use the default HTTPS port of 443 to access to the Control Center with your Web browser. When port 443 access is disabled, you must use port 41443 to access the Control Center. You may want to enable port 443 access if you have configured your firewall to allow HTTPS through that port only.

The `set-control-center-port-443` command has the following syntax:

```
set-control-center-port-443 <option>
```

### Table C-18 Options for set-control-center-port-443

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| disable | Disable Web access to the Control Center using port 443. When port 443 access is disabled, you must specify :41443 in the URL to access the Control Center. For example, you would need to type a URL in the following form to access the Control Center:  

|https://appliance.symantecexample.com:41443|

If you attempt to access the Control Center without including :41443 in the URL, errors such as the following are displayed in your Web browser:  
■ The page cannot be displayed  
■ Data Transfer Interrupted  

If port 443 access is disabled, ensure that your network allows access to the Control Center using port 41443. |
| enable | Enable Web access to the Control Center using port 443. For most Web browsers, when port 443 access is enabled, you do not need to specify the port number to access the Control Center. For example, a URL of the following form would be valid to access the Control Center:  

|https://appliance.symantecexample.com|

Some Web browsers may require that you append :443 to the URL. If port 443 access is enabled, you can also access the Control Center using port 41443. That is provided that your network allows access to the Control Center over port 41443. |
| status | Display the status of port 443 access. |

You can enable HTTP access to the Control Center.

See “http” on page 606.
shutdown

The `shutdown` command shuts down the appliance.

Shutdown occurs immediately and email remains in the queues.

The `shutdown` command has the following syntax:

```
shutdown
```

Type `help shutdown` from the appliance for online assistance.

**Note:** Depending on your deployment, migration can take up to several hours to complete. Do not shut down your computer during this time; doing so can result in database corruption.

Shut down an appliance

Before shutting down, it is strongly recommended that you stop the flow of mail to and from the appliance.

**To stop the flow of mail**

1. Suspend the acceptance of new mail.
   
   You can do this either by modifying your network setup such that the inbound and outbound appliance ports are blocked, or by issuing the following commands:
   
   ```
   mta-control inbound suspend-accept
   
   mta-control outbound suspend-accept
   ```

2. Let the mail drain from the system until it is free of messages.

3. As a precaution, you might also want to flush your inbound, outbound and delivery email queues.
   
   You can flush the queues by going to Status > Message Queues in the Control Center and clicking **Flush** or by issuing the following command:
   
   ```
   mta-control all flush
   ```

sshdctl

The `sshdctl` command lets you designate machines from which an administrator can connect to an appliance with the `ssh` command. This command alters entries
to the appliance's **allow** and **deny** lists. An entry on the **allow** list always takes precedence over **deny**. If a machine is matched with both lists, access is allowed. If a machine is unmatched on either list, access is allowed.

**Note:** These lists are not the same as the Good and Bad Senders lists

The `sshdctl` command has the following syntax:

```
sshdctl [option] <parameter> ...
```

as described in Table C-19.

Table C-19 provides the syntax for the `sshdctl` command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a [allow</td>
<td>deny] [rule]</td>
</tr>
<tr>
<td></td>
<td>A rule restricts access to an appliance via ssh connection and can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Host name or IP address – Designates a specifically allowed or denied location. A host name can be prefixed with a period (.) to include subdomains. An IP address can be terminated with a period (.) to include subdomains. Net masks can also be used to designate groups of IP addresses. An expression of the form n.n.n.n/m.m.m.m is interpreted as a net/mask pair. An IPv4 host address is matched if net is equal to the bitwise AND of the net address and the mask. For example, the net/mask pattern 131.155.72.0/255.255.254.0 matches every address in the range 131.155.72.0 through 131.155.73.255. You can also use wildcards of ? and * to include multiple IP address or host name entries for a rule. Wild cards cannot be used with any of the abbreviated forms described above.</td>
</tr>
<tr>
<td></td>
<td>■ ALL – Matches all hosts.</td>
</tr>
<tr>
<td></td>
<td>■ LOCAL – Matches any host name not containing a dot.</td>
</tr>
<tr>
<td></td>
<td>■ UNKNOWN—Matches any host with an unknown host name or IP address. Use this pattern with care as host names can be unavailable due to temporary name server problems. A network address is unavailable when the software cannot determine the type of network being accessed.</td>
</tr>
<tr>
<td></td>
<td>■ KNOWN – Matches any host with a known host name or IP address. Use this pattern with care as host names can be unavailable due to temporary name server problems. A network address is unavailable when the software cannot determine the type of network being accessed.</td>
</tr>
<tr>
<td></td>
<td>■ EXCEPT – Modifies entries from another list using the form list_n EXCEPT list_n.</td>
</tr>
<tr>
<td>-d [allow</td>
<td>deny] &lt;#&gt;</td>
</tr>
</tbody>
</table>
Table C-19  sshdctl command syntax (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Lists the active rules. The utility displays the full list of restrictions, including both the allow and deny list. If either list has no entries, the word empty is displayed for that list.</td>
</tr>
<tr>
<td>-h</td>
<td>Displays help for this command.</td>
</tr>
</tbody>
</table>

Type help sshdctl from the appliance for online assistance.

Table C-20  sshdctl sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a rule allowing ssh access to an appliance for your_domain.com</td>
<td>sshdctl -a allow .your_domain.com</td>
</tr>
<tr>
<td>Delete rules from a list</td>
<td>sshdctl -d deny 3 -d deny 1</td>
</tr>
<tr>
<td>Allow your_domain.com (but not its subdomains) and my_domain.com (and its subdomain addresses) access to an appliance via ssh. Also eliminate access to any other domain</td>
<td>sshdctl -a allow your_domain.com -a allow .my_domain.com -a deny ALL</td>
</tr>
</tbody>
</table>

sshdver

Run sshdver to allow or prohibit access to the Symantec Brightmail Gateway command line with SSH version 1 (SSH-1). You can also display the current setting. SSH-1 has documented security vulnerabilities so requiring access only with SSH-2 is recommended. If you change the allowable SSH version, your current SSH session to Symantec Brightmail Gateway exits. If you have difficulty logging in to the command line, ensure that your SSH client is set to match the allowable SSH protocols.

The sshdver command has the following syntax:

sshdver <option>

Table C-21  sshdver command syntax

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Displays help for this command.</td>
</tr>
<tr>
<td>-v</td>
<td>Displays the current setting.</td>
</tr>
</tbody>
</table>
Table C-21  sshdver command syntax (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Allows SSH access to the Symantec Brightmail Gateway command line with SSH-1 or SSH-2. This is the default setting.</td>
</tr>
<tr>
<td>2</td>
<td>Requires SSH access to the Symantec Brightmail Gateway command line with SSH-2 only. Access with SSH-1 is denied. If your SSH client is set to SSH-1 only, the SSH client may print an error if you attempt to access the command line.</td>
</tr>
</tbody>
</table>

sys-info

Run `sys-info` to display hardware information for an appliance or allocated resources for a virtual machine.

The `sys-info` command has the following syntax:

```bash
sys-info
```

Table C-22  Description of sys-info characteristics

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Display for appliance</th>
<th>Display for virtual machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Number</td>
<td>The Symantec model number for the appliance.</td>
<td>The text &quot;VM&quot; is displayed.</td>
</tr>
<tr>
<td>Service Tag</td>
<td>The Dell service tag for the appliance hardware. The Dell service tag is unique to each appliance like a serial number.</td>
<td>Nothing is displayed.</td>
</tr>
<tr>
<td>System CPU(s)</td>
<td>The CPU model and the CPU's speed. If the appliance has multiple CPUs, each CPU is displayed.</td>
<td>The speed of the CPU allocated to the virtual machine. If the virtual machine has multiple CPUs, each CPU is displayed. The CPU model is displayed as &quot;Unknown.&quot;</td>
</tr>
<tr>
<td>CPU cores</td>
<td>The total number of processor cores including single and multi-core CPUs. For example, an appliance with two dual-core CPUs counts as four processor cores.</td>
<td>The total number of processor cores allocated to the virtual machine, including single and multi-core CPUs. For example, a virtual machine with two dual-core CPUs counts as four processor cores.</td>
</tr>
</tbody>
</table>
Table C-22 Description of sys-info characteristics (continued)

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Display for appliance</th>
<th>Display for virtual machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory (MB)</td>
<td>The amount of physical RAM.</td>
<td>The amount of RAM that is allocated to the virtual machine.</td>
</tr>
<tr>
<td>Disk Size (GB)</td>
<td>The capacity of the hard disk. This number may be slightly smaller than expected due to manufacturer hard disk calculations and reserved space. If the appliance has multiple hard disks, the size of each hard disk is displayed. If the appliance has a RAID disk array, the capacity available for use is displayed excluding any redundant disks.</td>
<td>The amount of hard disk space that is allocated to the virtual machine.</td>
</tr>
</tbody>
</table>

**system-stats**

The system-stats command displays system statistics.

The system-stats command has the following syntax:

```
system-stats <key>
```

where `key` can be blank, in which case all available values are returned, or one or more of the following:

- **cpu_idle** – Displays CPU idle time as a percentage of CPU activity
- **cpu_iowait** – Displays input/output wait time as a percentage of CPU activity
- **cpu_usage** – Displays the CPU usage as a percentage
- **disk_used** – Displays the disk used in KB
- **disk_free** – Displays the disk free in KB
- **mem_used** – Displays the memory used in KB
- **mem_free** – Displays the memory free in KB
- **swap_used** – Displays the amount of swap in use
- **swap_free** – Displays the amount of free swap
- **eth_in** – Displays the current incoming data rate in KB if the interface is defined and enabled
- **eth_out** – Displays the current outgoing data rate in KB if the interface is defined and enabled
- disk_in – Displays the current rate of disk writes in KB
- disk_out – Displays the current rate of disk reads in KB

Type `help system-stats` from the appliance for online assistance.

**tail**

The `tail` command shows the last 50 lines of the named log file. This command is part of the standard Linux command set, but it has been modified in this implementation. Type `help tail` from the appliance for online assistance.

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`.

The `tail` command has the following syntax:

```
tail <log_name>
```

where `log_name` can be any of the following:

- `agent_log`
- `bmclient_log`
- `bmserver_log`
- `boot.log`
- `BrightmailLog.log`
- `cron`
- `conduit_log`
- `db-migration.log`
- `dmesg`
- `bmserver_log`
- `jlu-controller_log`
- `liveupdt.log`
- `maillog`
- `messages`
- `named.run`
- `secure`
- `imrelay_log`
**telnet**

The `telnet` command allows you to connect from the appliance to your network. This command is part of the standard Linux command set but has been modified in this implementation. Type `help telnet` from the appliance for online assistance.

**traceroute**

The `traceroute` command traces the network route to the given hostname or IP address and is part of the operating system. All arguments are permitted. This command is part of the standard Linux command set, but it has been modified in this implementation. Type `help traceroute` from the appliance for online assistance.

The `traceroute` command has the following syntax:

`traceroute <hostname|IP address>`

**update**

The `update` command:

- Checks for new packages
- Downloads new packages
- Installs new packages
- Lists available update package versions for download or installation

Before using update to install a new version of appliance software, be sure to familiarize yourself with the procedure described below for performing a software update.

The `update` command has the following syntax:

`update <option>`

where option can be any of the following:

- `check` – Performs a dry run of what will happen if you choose to update your software.
- `download` – Fetches new packages for future installation.
install – Installs the most recent software version to your appliance.

list – Shows a list of available updates and which version you are currently using.

### Table C-23 update sample usage

<table>
<thead>
<tr>
<th>Task</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fetch new packages for future installation.</td>
<td>update download</td>
</tr>
</tbody>
</table>

Type `help update` from the appliance for online assistance.

## Installing software updates

Use `update install` to download and install the most recent version of software to the appliance. If you are running separate appliances for the Control Center and Scanners, be sure to update every appliance before running updated software.

Before updating the software, be certain your appliance is not performing tasks that, if disrupted, could cause problems after resetting the system. Such tasks include but are not necessarily limited to the following:

- A running synchronization cycle
- A Scanner replication cycle

### To install software with the `update` command

1. Make a backup of your database information using the `db-backup` command.
   For information on doing this, see `db-backup`.
2. Use the `update install` command to install the new software.
   Be sure to update all appliances if more than one is being used.

**Note:** When you have finished updating the Control Center appliance, either click your browser's refresh button or close and re-open it to ensure that cached versions of graphics are redisplayed correctly.

## version

The `version` command displays the version of the software that is installed on the appliance. The `version` command also displays the date and time at which the current version was installed.

The `version` command has the following syntax:
**version**

Type `help version` from the appliance for online assistance.

**watch**

The `watch` command displays the last ten lines of the specified log file when issued, and then displays any messages written to the log. Output is sent to the screen for monitoring. Type `help watch` from the appliance for online assistance.

The watch command has the following syntax:

```
watch <log_name>
```

where `log_name` can be any of the following:

- agent_log
- bmcclient_log
- bmserver_log
- boot.log
- BrightmailLog.log
- cron
- conduit_log
- db-migration.log
- dmesg
- bmsserver_log
- imrelay_log
- imlinkage_log
- jlu-controller_log
- liveupdt.log
- maillog
- messages
- named.run
- secure
- update.log
Administering your product through the command line

About administering your product through the command line
adware
Programs that secretly gather personal information through the Internet and relay it back to another computer. This is done by tracking browsing habits, generally for advertising purposes.

Agent
A component that facilitates communicating configuration information between the Control Center and each Scanner.

annotation
A phrase or paragraph 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 groups of recipients. You can use this feature to automate email disclaimers.

archive
An action that can be performed on email messages which consists of forwarding the messages to a specific SMTP address.

attachment list
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), or on the true type of each file, or you can use a pre-filled list.

Audit ID
A unique identifier included as a message header in all processed messages.

authentication
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.

bad sender
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.

bounce
An action that can be performed on an email message by an email server, which consists of returning the message to its From: address with a custom response.

Bounce Attack Prevention
A feature of Symantec Brightmail Gateway that eliminates bounced messages that are a result of redirection, while still allowing legitimate bounce message notification.

Brightmail Engine
The component of Symantec Brightmail Gateway that scans email and attachments, instant messages, and file transfers for viruses, spam, and content compliance according to polices that you configure.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<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>CA (Certificate Authority)</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>certificate</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>Certificate Authority-signed SSL</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>CIDR (classless interdomain routing)</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 would include 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>clean</td>
<td>An action that consists of deleting unreparable virus infections and repairing repairable virus infections.</td>
</tr>
<tr>
<td>Conduit</td>
<td>A component that retrieves new and updated filters from Symantec Security Response through secure HTTPS file transfer. Once retrieved, the Conduit authenticates filters, and 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>Content Compliance</td>
<td>A set of features that enable administrators to enforce corporate email policies, reduce legal liability, and ensure compliance with regulatory requirements. These features include annotations, streamlined filter creation using multiple criteria and multiple actions, flexible sender specification, dictionary filters, and attachment management.</td>
</tr>
<tr>
<td>Control Center</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>
<tr>
<td>defer</td>
<td>An action that an MTA receiving an email message can take, which consists of using a 4xx SMTP response code to tell the sending MTA to try again later.</td>
</tr>
<tr>
<td>DMZ (de-militarized zone)</td>
<td>A network added between a protected network and an external network to provide an additional layer of security. Sometimes called a perimeter network.</td>
</tr>
</tbody>
</table>
| dictionary | A list of words and phrases against which email messages can be checked for non-compliant content. Symantec Brightmail Gateway allows you to create Content
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance filters</td>
<td>Filters 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>Directory harvest attack</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 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>DNS (Domain Name Server) proxy</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>DNS (Domain Name System)</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>DNS server</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>Downstream</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>Email virus attack</td>
<td>A series of virus-infected emails from a specific domain. Symantec Brightmail Gateway allows you to choose an action to perform on these messages; by default messages received from violating senders are deferred.</td>
</tr>
<tr>
<td>Encrypted attachment</td>
<td>A message attachment that has been converted into a form that is not easily understood by unauthorized persons. Symantec Brightmail Gateway does not scan encrypted attachments, but allows you to choose an action to take when an encrypted attachment is detected.</td>
</tr>
<tr>
<td>Expunger</td>
<td>A component of Spam Quarantine, which resides on the Control Center computer in Symantec Brightmail Gateway. Expunger can be configured to periodically remove older or unwanted messages from the Spam Quarantine database.</td>
</tr>
<tr>
<td>False positive</td>
<td>A piece of legitimate email that is mistaken for spam and classified as spam by Symantec Brightmail Gateway.</td>
</tr>
<tr>
<td>Fastpass</td>
<td>A feature of Symantec Brightmail Gateway that lets most 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 required for messages from legitimate sources.</td>
</tr>
</tbody>
</table>
filter  A method for analyzing email messages, used to determine what action to take on each message. Symantec Brightmail 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 Brightmail Gateway, a set of actions that apply to a category of messages. The actions specified in a filter policy are only applied to users who are members of a group that includes the filter policy. There are three types of filter policies: spam, virus, and content compliance policies. Filter policies can also make use of policy resources. See also group, policy resources.

firewall  A program that protects the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet will want 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.

group  In Symantec Brightmail Gateway, a group of users to which you can apply a unique set of filter policies. Users can be specified by email address or domain. See also filter policy.

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.

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, which consists of the network ID, plus a unique host ID assigned by the network administrator. 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 Brightmail Gateway, a feature that allows you to block or allow messages written in a specified language. 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. Administrators can set language...
identification for groups of users, or allow users to specify their own settings. See also Symantec Outlook Spam Plug-in.

**LDAP (Lightweight Directory Access Protocol)**
A software protocol that enables anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a lightweight (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.

**LDIF (LDAP Data Interchange Format)**
An Internet Engineering Task Force (IETF) standard format for representing directory information in a flat file, specified in RFC 2849.

**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 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 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.

**messaging gateway**
The outermost point in a network where mail servers are located. All other mail servers are downstream from the mail servers 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 Brightmail 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.

Each Scanner MTA has the following queues for the temporary storage of email:

- **Delivery queue**
  The queue that temporarily holds inbound and outbound messages that have already been filtered before the MTA delivers the messages to their required destinations

- **Inbound queue**
  The queue that temporarily holds inbound messages before the MTA forwards them to the Brightmail Engine for processing
Outbound queue
The queue that temporarily holds outbound messages before the MTA forwards them to the Brightmail Engine for processing.

name server
A computer running a program that converts domain names into appropriate IP addresses and vice versa.

notification
1. In Symantec Brightmail Gateway, a separate email that can be automatically sent to the sender, recipients, or other email addresses when a specified condition is met. For example, if you have a policy that strips .exe attachments from incoming messages, you may want to also notify the sender that the attachment has been stripped. 2. In Symantec Brightmail Gateway, a periodic email summary sent by Spam Quarantine to users, listing the newly quarantined spam messages, and including links for users to immediately release messages to their inbox or to log in to their personal quarantines. See also Notifier.

Notifier
A component of Spam Quarantine, which resides on the Control Center in Symantec Brightmail Gateway. Notifier sends periodic email messages to users, providing a digest of their spam. The Notifier message (notification) is customizable; it can contain a list of the subject lines and senders of all spam messages.

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, designed to mimic the site of a legitimate business and entice the recipient to provide information that can be used for identity theft or online financial theft.

policy
A set of message filtering instructions that Symantec Brightmail Gateway implements on a message or set of messages. See also filter policy, group.

policy resources
In Symantec Brightmail Gateway, sets of data that enable customization of email filtering and the actions taken on filtered email. You can employ policy resources when you create filter policies. Policy resources include annotations, archive, attachment lists, dictionaries, and notifications. See also filter policy, annotation, archive, attachment list, dictionary, and notification (definition 1).

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 accounts**
Email addresses assigned to Symantec by our Probe Network Partners, and used by Symantec Security Response to detect spam.

**Probe Network**
A network of email accounts provided by Symantec’s Probe Network Partners. Used by Symantec Security Response for the detection of spam, the Probe Network has a statistical reach of over 300 million email addresses, and includes over 2 million probe accounts.

**Probe Network Partners**
ISPs or 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, which consists of using a 5xx SMTP response code to tell the sending MTA that the message is not accepted.

**release**
In Symantec Brightmail Gateway, an action that end users or administrators can take on messages in the Spam Quarantine database. Releasing removes the message from the Spam Quarantine database and returns the message to the end user's inbox. See also Spam Quarantine.

**replication**
In Symantec Brightmail Gateway, the process of duplicating configuration data from the Control Center to Scanners.

**Scanner**
The component in Symantec Brightmail Gateway that filters mail. Each site can have one or many Scanners. The configuration of each Scanner is managed via the Control Center.

**sender group**
A category of email senders that Symantec Brightmail 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 group.
Sender ID  
A set of standard practices for authenticating email. If the sender's domain owner participates in Sender ID, the recipient MTA can check for forged return addresses. Symantec Brightmail Gateway allows you to specify an action for messages that fail Sender ID authentication.

signature  
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 can also be 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 is more precisely referred to as signature data.

SMTP (Simple Mail Transfer Protocol)  
The protocol that allows email messages to be exchanged between mail servers. Then, clients retrieve email, typically via the POP or IMAP protocol.

spam  
1. Unsolicited commercial bulk email. 2. An email message identified as spam by Symantec Brightmail Gateway, using its filters.

Spam Quarantine  
A database that stores email messages separately from the normal message flow, and allows access to those messages. In Symantec Brightmail 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.

spam scoring  
The process of grading messages when filtering email for spam. Symantec Brightmail Gateway assigns a spam score to each message that expresses the likelihood that the message is actually spam. See also suspected spam.

SSH (Secure Shell)  
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 information sent over the network.

SSL (Secure Sockets Layer)  
A protocol that allows mutual authentication between a client and server and the establishment of an authenticated and encrypted connection, thus ensuring the secure transmission of information over the Internet. See also TLS.

SPF (Sender Policy Framework)  
A set of standard practices for authenticating email. If the sender's domain owner participates in SPF, the recipient MTA can check for forged return addresses. Symantec Brightmail Gateway allows you to specify an action for messages that fail SPF authentication.

spyware  
Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay the information back to another computer.
subnet mask

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 “mask” a portion of an IP address so that TCP/IP can determine whether any given IP address is on a local or remote network. Each computer configured with TCP/IP must have a subnet mask defined.

suspected spam

A message that Symantec Brightmail Gateway deems could potentially be spam based on scores 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.

Suspect Virus Quarantine

In Symantec Brightmail Gateway, a database that temporarily holds messages suspected of containing viruses. Messages with suspicious attachments can be held in Suspect Virus Quarantine for a number of hours, then filtered again, with updated filters, if available. This processing delay capability enables Symantec Brightmail Gateway to more effectively deal with new virus threats as they emerge.

suspicious attachment

A message attachment that Symantec Brightmail Gateway has determined may contain a virus. You can choose what action to take when a suspicious attachment is detected.

Symantec Global Bad Senders

A list of IP addresses collected by Symantec, based on global spam data from mail servers protected by Symantec. One of the sender groups in Symantec Brightmail Gateway.

Symantec Global Good Senders

A list of IP addresses collected by Symantec, based on global legitimate sender data from mail servers protected by Symantec. One of the sender groups in Symantec Brightmail Gateway.

Symantec Outlook Spam Plug-in

An application that makes it easy for Outlook users to submit missed spam and false positives to Symantec. Depending on how you configure the plug-in, user submissions can also be sent automatically to a local system administrator. The Symantec Outlook Spam Plug-in also gives users the option to administer their own Allowed Senders List and Blocked Senders List, and to specify their own language identification settings. See also language identification.

Symantec Security Response

Symantec Security Response is a team of dedicated intrusion experts, security engineers, virus hunters, threat analysts, and global technical support teams 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 to 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, 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 & statistics for the entire security community, placing 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 as 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 located around the world.

**synchronize**

To copy files between two folders on host and remote computers to make the folders identical to one another. Copying occurs in both directions. If there are two files with the same name, the file with the most current date and time is copied. Files are never deleted during the synchronization process.

**Third Party Bad Senders**

A sender group in Symantec Brightmail Gateway that allows administrators to add multiple lists of bad senders compiled by third-party services.

**Third Party Good Senders**

A sender group in Symantec Brightmail Gateway that allows administrators to add multiple lists of good senders compiled by third-party services.

**threat**

A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

**TLS (Transport Layer Security)**

A protocol that provides communications privacy over the Internet by using 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 Brightmail 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 Brightmail 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 Brightmail Gateway, a message can be unscannable for viruses for a variety of reasons. For example, if it exceeds the maximum file size or maximum scan depth configured on the Scanning Settings page, or if it contains malformed MIME attachments, it may be unscannable. Compound messages such as zip 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.

**Vontu Network Prevent**
A component of Vontu Data Loss Prevention which discovers, monitors, and protects confidential data wherever it is stored or used. Symantec Brightmail Gateway integrates with Vontu Network Prevent to deliver, route, hold, or block email traffic.

**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.
Index
bad sender groups  (continued)
   configuring LDAP settings for 490
   deleting senders 149
   editing members 149
   enabling, disabling groups 147
   enabling, disabling members 149
   end user lists 74
   exporting data 153
   impact of Connection Classification on 134
   import file formats 151
   importing data 150
   LDAP synchronization for 481
   overview 132, 143
   sender identification methods 154
   use case 143
blacklists. See third party sender lists
Blocked Sender Lists. See bad sender groups
Bloodhound settings 171, 189
bounce attack prevention
   configuring 161
   creating a seed value 161
   overview 159
   spam policies 162
Brightmail
   ARM (Adaptive Reputation Management) 132
   engine
      about 107
      enabling, disabling 108, 394
   IQ Services 132
C
CA (Certificate Authority). See Certificate Authority
cat command 594
cc-config command 594
certificate
   assigning 457, 464
   assigning user interface HTTPS 465
   Certificate Authority signed 457, 459–463, 465
      configuring 457
   Control Center 466
   deleting 464
   HTTPS 457, 465
   MTA TLS 457, 464
   self-signed 457–463, 465
   viewing 463
Certificate Authority (CA)
   about 457, 464
   backing up 463
   changing name 462
Certificate Authority (CA)  (continued)
Control Center, for 465
importing 461
PEM format 460
replacing 462
requesting 459
user interface certificate 465
change-based synchronization 481
clear command 595
command line interface 591
commands
agentconfig 593
cat 594
cc-config 594
clear 595
crawler 596
date 597
db-backup 597
db-restore 600
delete 602
diagnostics 602
dn-normalize 604
dns-control 605
eula 605
grep 605
help 605
http 606
ifconfig 606
install 606
iostat 607
ldapsearch 607
ls 610
mallog 610
malquery 612
more 619
mta-control 619
mta-stats 622
netstat 623
nslookup 624
passwd 624
pause-mode 624
ping 625
reboot 625
rebuildrpmdb 626
rm 626
route 626
service 626
set-control-center-port-443 628
shutting down 629
commands  (continued)
sshdctl 629
sshdver 631
sys-info 632
system-stats 633
tail 634
telnet 635
traceroute 635
update 635
version 636
watch 637
compliance.  See content compliance
compliance folders 346
See also  content compliance
adding 348
default folder 346
deleting 350
notification template 297
settings 346, 348, 351
components, Symantec Brightmail Gateway
about 24
hardware 28
software 27
Conduit
about 107
starting, stopping 108, 394
Connection Classification
configuring 136
default settings 138
disabling 136
enabling 136
how it works 134
impact on sender groups 134
learning mode 134, 136
overview 132
connection time processing 132
container limit 170, 189
content compliance 351
See also incident management compliance
adding policy conditions 286, 289
attachment list 311
basic resources for policies 300
creating a policy 282
creating compliance policies 280
creating conditions 286
creating dictionaries 305
described content templates 302, 522
dictionaries 305, 537
disabling 285
content compliance  (continued)
   enabling 285
   filtering, language-based 75
   filters 300
   folders 346
   for filter all messages 583
   incident archive tag 348
   incident management 346, 351–352
   match tests 579
   multiple policies 63
   notification 348
   notification template 297
   patterns 314, 536
   Perl regular expressions 329
   policy
      assigning to groups 72
      order 286
      resources 300
      verdicts and actions 56
   premium
      attachment list 311
      dictionaries 305
      resources 311, 536–537
      templates 302
   record resource 317
   regular expressions 327, 536
   reports 359
   status 347
   structured data templates 302, 525
   templates 302
   types of filter tests available 579
content filtering attachment settings 474
Control Center
   bounce attack prevention 161
   certificate for 457, 465–466
   component 27
   DNS 451
   error log 435
   host access 451–452
   licensing 436–437
   listener port 456
   logs 403
   replicating 395, 400, 402
   security warning 465
   simultaneous access 434
   user logon help 453
crawler command 596
custom filters.  See content compliance

D
Dashboard
   contents 389
   system status 390
   threat categories 391
data loss prevention 24
date command 597
day-zero protection 171
db-backup command 597
db-restore command 600
DBCS 453
defaults
   Connection Classification 138
   inbound SMTP connection settings 39
   inbound SMTP session phase settings 41
   internal hosts list 124
   message filtering actions 43, 48
   outbound SMTP connection settings 45
   outbound SMTP session phase settings 46
   policy actions
      email virus 68
      IM virus 68
      spam 71
      spim 71
definitions
   disabling automatic updates 194
   emerging threats 196
   on demand 194
   platinum 195
   scheduling 193
   source
      LAN host 195
      Symantec 195
   status 193
   updating 171, 191
deleter command 602
delivery
   settings overview 51
   Spam Quarantine
      misidentified messages 228
      undeliverable messages 246
   starting, stopping 108
   Suspect Virus Quarantine 199
denial-of-service attack
   bounce attack prevention 159
   container limits 189
deployment
   advantages at gateway 123
   non-gateway 123
deployment (continued)
   sender group policies 124, 143
diagnostics command 602
dialers 180
dictionaries
   about 305
   adding new 308
   custom 305
   editing 309
   enabling, disabling keyword or keyphrase 310
   importing keywords 308
   premium 302, 305
directory harvest attacks
   configuring recognition 140
   overview 132
directory types. See LDAP directory types
disk space 454
distribution list, LDAP directory
   expansion 490
   query 481
   resolution 490
distribution lists. See aliases and distribution lists
dn-normalize command 604
dns-control command 605
documentation, product 34
does Not Match and Match tests 329
Domain Name System (DNS) servers 113
domains
   deleting 86
   for outbound mail acceptance 105
   importing 85
   local 81
      See also local domains
   adding, editing 81
   specifying routing for 83
   non-local
      adding, editing 84
   overview 79
   sender authentication 76
   specifying for sender groups 154
   specifying which to accept 79
Domino 477, 481
double-byte character sets 453
duplicate messages, Spam Quarantine 246

E
email 170, 209
   See also spam
   See also virus
email addresses, identifying for groups 154
email aliases. See aliases and distribution lists
email filtering 170, 209
   See also spam
   See also virus
   inbound 43
   inbound diagram 36
   outbound 45, 48
   overview 35, 53
   phases 36
email message flow
   inbound diagram 36
   outbound 45
   overview 35
   phases 36
email virus attack
   configuring recognition 138
   overview 132
Enable distribution list expansion 493
encoding 60, 453
encrypted attachment 170
encryption 79
   See also TLS encryption
End User License Agreement. See eula command
end user settings
   configuring 74
   enabling, disabling 74
   requirements for 75
errors
Spam Quarantine
   cannot release mail 246
   cannot release the message 246
   disk or work directory full 246
   distribution list 246
   large spam messages 246
   no disk space 246
   the operation cannot be performed 246
Ethernet settings 115
eula command 605
Exchange 5.5 477, 481
Expunger
   log 408
   reports 383
   Spam Quarantine 245
   Suspect Virus Quarantine 207

F
factory defaults, restoring 468
fallback encoding 453
false positive spam messages 228, 236
Fastpass
  configuring 157
  enabling, disabling 157
  how it works 155
  overview 132
favorite reports
  canceling scheduled 379
  copying 371
  creating 370
  deleting 372
  editing 370–371
  generating automatically 377
  printing 381
  running on demand 377
  saving to file 382
features, product 31
file attachment 311
file transfer, instant messaging 272
filters 170, 209
  See also spam
  See also virus
  assigning policies 68
  attachment list 312
  changing policy order 286
  disabling 285
  editing 285
  email categories for 53
  enabling 285
  end user 74–75
  for all messages 583
  group precedence 67
  IM categories for 53
  inbound 43
  language-based 74–75
  outbound email 45, 48
  overview 35, 53
  regular expressions in 329
  searching compliance incidents 351
  sender authentication 76
  test types 579
  types 53
  verdicts 53
full synchronization. See synchronization

G

gateway
  about 24
  deployment considerations 123
Global Intelligence Network 132
global reputation 143
good sender groups
  adding members 148
  choosing actions 147
  deleting senders 149
  editing members 149
  enabling, disabling groups 147
  enabling, disabling members 149
  end user lists 74
  exporting data 153
  impact of Connection Classification on 134
  import file formats 151
  importing data 150
LDAP
  authentication for 480
  configuring source for 490
  overview 132, 143
  reasons to use 145
  sender identification methods 154
Google Talk
  blocking or allowing access to 269
  connection status 432
grep command 605
Group Query, LDAP synchronization 481
groups
  assigning filter policies 68
  assigning policies
    spam 71
    spim 71
    virus 68
  deleting 67
  disabling 67
  editing 66
  enabling 67
  end user settings 74–75
  managing 66
  members
    adding 64
    creating 64
    deleting 64
    editing 64
    exporting 65
    importing 65
  outbound, inbound effects of 63
  overview 63
  policies, assigning
    compliance 72
    IM Network Access Control 73
groups (continued)
policies, assigning (continued)
    language 75
    precedence 63, 67
    user, finding 67

H
hacking tools 180
hardware
    components 28
    information about 393
    status 392
headers
    Spam Quarantine
        searching 230
        viewing 233
    Suspect Virus Quarantine
        searching 203
help
    command-line command 605
    Symantec Brightmail Gateway 34
    user logon help 453
heuristics 171, 189
hosts
    accessing the Control Center 452
    adding 125
    configuration settings 115
    disabling 126
    enabling 126
    internal mail hosts 123
    modifying 126
    services 107
    SMTP settings 454
    starting 127
    status 394
    stopping 127
    turning off 466
HTML text, annotating to messages 291
HTTP command 606
HTTPS
    Control Center 465
    user interface certificate 457, 465–466

I
ifconfig command 606
IM. See instant messaging
IM filtering. See instant messaging
IM Network Status 432

IM Relay
    about 107
    starting, stopping 108
inbound SMTP settings
    about 98, 100
    changing 100
    delivery 102
    processing details 39, 41
    restricting acceptance 101
incident
    acting upon 352
    archive tag 348
    exporting history 352
    status overview 346
    updating the status 352
incident management compliance 351
install command 606
instant messaging
    about 251
    configuring 254
    enabling 254
    file transfer, scanning 272
IM network access
    allowing 269
    blocking 269
    status 432
    overview 251
policies
    assigning to groups 73
    creating spim policies 274
    creating virus policies 272
    default 271
    Network Access Control 73
    verdicts and actions 60
reports 359
searching for active IM users 429
spim
    about 256
    about detecting 257
    configuring detection 274
    disabling detection 259
    enabling detection 259
suspected spim 258
troubleshooting 432
user registration
    about 259–260
    as an administrator 265
    deleting 267
    editing 267
instant messaging (continued)
user registration (continued)
editing registration text 261
enabling 260
self-registering 266
viewing active IM users 429
internal mail hosts 123
internal mail servers 143
invalid recipient
accepting all 88
configuring LDAP settings for 490
dropping 88
overview 87
rejecting 88
iostat command 607
IP address
modifying 115
researching reputation 163
specifying for sender groups 154
virtual 115
IP connections reports 359
iPlanet. See Sun Directory Server

J
Java directory server. See Sun Directory Server
joke programs 180

L
LAN host 195
language encoding 60, 201, 233
language identification
about 74
configuring 75
tagging messages based on 215
LDAP 221
See also Spam Quarantine
adding directory server 477
adding source definition 493
administrator credentials 477
configuring source 477
deleting an LDAP source 503
dn normalization 604
editing a source definition 501
logs 403
object classes 481
postmaster mailbox 225
Scanner replication 401
LDAP (continued)
synchronization
about 395
cancelling 399
initiating 398, 485
status 396
troubleshooting 400
LDAP directory types
Active Directory 477
Domino 477
Exchange 5.5 477
OpenLDAP 477
other directories 477
Sun Directory Server 477
LDAP Server Usage 477
See also LDAP services
LDAP services
authenticating 477, 480
recipient validation 477, 488
routing 477, 485
synchronizing 477, 481
LDAP settings
authentication 480
routing service 485
source 490
synchronization 481
ldapsearch command 607
license 436–437
Linux 27
listener port 456
lists
aliases and distribution lists
about 92
adding 93
details, examples 94
editing 93
importing 93
attachment list 312
importing local routes/domains list 81
LiveUpdate
about 107, 191
on demand 194
scheduling 193
service
disabling 394
enabling 394
source 195
starting, stopping 108
local domains 86
See also domains
adding 83
configuring 81
importing 85
overview 79
specifying routing for 83
specifying which to accept 79
local reputation 143
local routes list 81
locale 453
log on issues, Spam Quarantine 246
login query, LDAP authentication 480
logs
about 403
backing up 435
Control Center 435
database size 408
deleting 410
local Scanners 410
logging levels 410
message audit 418
purging 408
remote Scanners 410
remote syslog 412
saving 407
settings 412
syslog 412–417
system performance 410
types 403
viewing 406
Lotus Domino. See Domino
ls command 610

M
mail flow 427
See also MTA
about 28
inbound diagram 36
managing 111
omitted verdicts 512
outbound 45
overview 35
phases 36
starting, stopping 108, 111
stopping 427, 629
mail hosts, internal 123
mail transfer agent. See MTA
malicious attack
denial-of-service 189
detecting 170–172
zip bomb 189
mallog command 610
malquery command 612
malware 180
Management Information Base (MIB) 451
masquerade list
adding, editing 90
importing 90
mass-mailer worm 170
matches exactly and does not match tests 329
message audit logging
about 418
size 612
message flow
delivery phase 51
inbound diagram 36
managing 111
omitted verdicts 512
outbound email 45
overview, email 35
phases 36
reducing volume 132
routing phase 50
starting, stopping 108, 111
Message ID 230, 421
message queues
about 424
bad message queue 475
deleting 425
flushing 426
mail flow 427
managing 111
searching 425
starting, stopping 111
status 428
viewing 425
message reports 359
messages
annotating 291–292
audit logging 418
delivery 51
dropping invalid recipients 88
routing 50
Spam Quarantine
duplicate 246
false positives, who to notify of 236
messages (continued)
Spam Quarantine (continued)
maximum allowed 246
message retention period 245
misidentified 228
navigating 226
postmaster mailbox 225
retention period 245
searching 230, 232
thresholds 234
viewing 223
starting, stopping 111
108
Suspect Virus Quarantine
navigating 202
releasing 206
retention period 207
searching 203–204
viewing 200
tracking 418
MIB (Management Information Base) 451
misidentified spam messages 236, 246
more command 619
MSN Messenger
blocking or allowing access to 269
connection status 432
MTA
about 107
component 24, 27
managing 111
message queue behavior 111
operations 108
starting 108, 394, 427, 619
stopping 108, 394, 427, 619
TLS certificate 457, 464
viewing the service status 394
mta-control command 619
mta-stats command 622
MX lookup
enabling 299
LDAP routing 485
new features 22
non-local domains. See domains, non-local
notification
creating 295
Spam Quarantine
choosing the format 243
editing the template 240
frequency of 239
template
choosing the format 243
compliance folder 297
e-mail 294
IM 294
incident 297
spam 240
variables 580
nslookup 436
nslookup command 624
O
object classes, LDAP directory 481
OpenLDAP 477
outbound SMTP settings
about 98, 104
changing 104
connection phase processing 45
delivery 106
domains to accept mail from 105
processing details 46
P
passwd command 624
password
best practices 438
resetting 446
strong 438–439
patterns
filter tests 579
premium 302
pause-mode command 624
PEM, format requirements 460
performance, vs. effectiveness 155
Perl-compatible regular expressions 329
permissions, Active Directory
ADAM Administration Tools 490
ping 436, 625
plain text, annotating to messages 291
platinum virus definitions. See definitions

N
netstat command 623
Network Access Control policy 73, 269
Network Time Protocol (NTP) servers 114
network utilities 436
network, sender group policy considerations 124, 143
Registered Users (continued)
deleting 267
ing editing 267
registering users as an administrator 265
self-registering 266
registration
Control Center 436–437
Scanner 436–437
regular expressions
filter tests 579
in compliance policy templates 302
in content compliance policies 329
premium content compliance 327
use in content compliance policies 327, 536
regulatory compliance
data-protection templates 562
mitigation 280, 552
policy templates 542
templates 302
release, message
from Spam Quarantine 228
from Virus Quarantine 206
remote access programs 180
replication
about 395
canceling 402
check status of 505
enabling, disabling 108
resolve errors 506
Scanners 402, 455
status 400–401
reports
about 356
canceling scheduled 379
configuring data retention period 383
content compliance 359
copying 371
creating 357
data tracking
deleting 384
purging 384
retention 383
what to track 357
deleting 372
editing 370–371
emailing 379–380
Expunger 383–384
favorites
canceling scheduled 379
reports (continued)
favorites (continued)
copying 371
creating 370
deleting 372
editing 370–371
generating automatically 377
printing 381
running on demand 377
saving to file 382
generating automatically 377
generating on demand 377
graphs 372
instant messages reports 377
IP connections 359
layout 372
message 359
printing 381
purging 383–384
running on demand 377
saving to file 382
spam 359
summary 359
tables 372
troubleshooting 385
types 359
virus 359
Vontu Network Prevent integration 341
reputation
global 143
local 143
researching 163
resources
attachment lists for policies 311
conserving 132, 157, 512
policy 300
premium dictionaries 537
premium patterns 536
regular expressions 327, 536
resources, conserving 132, 157, 512
restore
factory defaults 468
from local backup 472
retention
Spam Quarantine
message retention period 245
retention period 245
Suspect Virus Quarantine
retention period 207
rm command 626
route command 626
routing
  configuring LDAP settings for 490
  LDAP 477, 485
  overview, settings 50
  specifying for local domains 83

S
Scanners
  adding 125
  certificate for 457
  certificates, assigning 464
  component 27
  defining role 99
  deleting 127
  disabling 126
  DNS 113
  See also settings, Scanners
  enabling 126
  Ethernet 115
  IP address 115
  licensing 436–437
  logs 403
  managing mail flow 111
  modify SMTP settings for 99
  modifying 126
  NTP time servers 114
  proxy 114
  replicating 108, 401–402, 455
  See also replication
  services
    about 107
    starting, stopping 108
  SMTP advanced settings 118
  SMTP settings
    about 98
    inbound 100
    inbound delivery 102
    outbound 104
    outbound delivery 106
    restricting acceptance 101
  starting 127
  stopping 127
  time settings 114
  turning off 466
search
  compliance incidents 351
  search (continued)
    Spam Quarantine
      criteria and tips 232
      headers 230
      messages 230
    Suspect Virus Quarantine
      criteria and tips 204
      headers 203
      messages 203
  security risks 180
  self-signed certificate
    adding 458
    changing name 462
  sender authentication 76
  sender groups
    adding members 148
    choosing actions 147
    deleting senders 149
    editing members 149
    enabling, disabling groups 147
    enabling, disabling members 149
    end user lists 74
    exporting data 153
    impact of Connection Classification on 134
    import file formats 151
    importing data 150
    overview 132, 143
    sender identification methods 154
  Sender ID 76
  sender policies
    choosing actions 147
    overview 132
  Sender Policy Framework 76
  senders
    adding to sender groups 148
    bad sender groups 143
    deleting from sender groups 149
    editing lists 149
    enabling, disabling 149
    exporting from senders groups 153
    importing into sender groups 150
    sender identification methods 154
  service command 626
  services
    about 107
    proxy 114
    Scanner 108
    status 394
  set-control-center-port-443 command 628
settings 209
See also spam
Domain Name System (DNS) 113
e-mail message delivery 51
e-mail message routing 50
end user 74–75
hosts 118
inbound SMTP connection phase 39
inbound SMTP session phase 41
message filtering
  inbound 43
  outbound 48
Network Time Protocol (NTP) 114
outbound SMTP connection phase 45
outbound SMTP session phase 46
proxy 114
Scanners 113, 115, 118
Scanners, e-mail
  about 98
  inbound 100
  inbound delivery 102
  outbound 104
  outbound delivery 106
  outbound mail acceptance 105
  restricting acceptance 101
sender authentication 76
SMTP
  about 98
  advanced 118
  inbound 100
  outbound 104
shut down command 629
SMTP (continued)
  message queues 424
  outbound connection phase settings 45
  outbound mail acceptance 105
  outbound Scanner settings
    about 98
    configuring 104
    delivery 106
  outbound session phase settings 46
SNMP 450–451
software
  components 27
  installing updates 636
  licensing 436–437
  updating 474
  version 473
spam 209
See also groups
See also policies
See also Spam Quarantine
  about 209–210
  bypassing scanning 157
  directory harvest attacks 140
  exempting senders from spam scanning 155
  language-based filtering 74–75
  policies
    assigning to groups 71
    bounce attack prevention 162
    copying 214
    creating 211
    default actions 71
    deleting 215
    enabling and disabling 213
    modifying 213
    pre-configured 210
    verdicts and actions 56
  reports 359
  sender authentication 76
  suspected spam threshold, configuring 216
  tagging specific languages 215
spam filters 209
  See also spam
  inbound 43
  outbound 48
Spam Quarantine 220
  See also spam
  about 220
  access quarantine problems 246
  administrator-only access 222
Spam Quarantine (continued)
aliases and distribution lists 238
before you use 220
differences between administrator and user
pages 224
distribution lists, aliases 238
duplicate messages 246
effects 246
false positives 228
language encoding 233
LDAP authentication for 480
logs 403
messages
  deleting 229
  false positives, who to notify of 236
  headers, viewing 233
  language encoding 233
  maximum number of 246
  misidentified 228
  number of entries on message list page 227
postmaster mailbox 225
searching 230, 232
searching tips 232
sorting 227
viewing 223
misidentified messages 228
navigating 226
non-existent addresses 221
notification
  about 237
  enabling 243
  false positives, who to notify of 236
  modifying the template 240
  selecting the format 243
  to users 239
  variables 242
number of entries on message list page 227
postmaster mailbox 225
purging 245
retaining messages 245
thresholds 234–235
troubleshooting 246
undeliverable messages 246
user logon help 453
viewing 223, 226
SPF 76
spim. See instant messaging
policies
  assigning to groups 71
spim (continued)
policies (continued)
  default actions 71
spyware 170, 180
sshdct1 command 629
sshdver command 631
status
  about 387
  compliance 347
  Control Center replication 400, 402
  Dashboard 389
  hardware information 393
  hardware status 392
  IM 387, 429, 432
  LDAP synchronization 395
  logs 403
  message queue size 428
  queued messages 424
  replicating the Control Center 395
Scanners
  canceled synchronization 399
  replication 401
  synchronization 396
  synchronizing manually 398
services 394
SMTP 387
system 387
structured data 317
  See also content compliance
  about 302
  record resource 318
summary reports 359
Sun Directory Server 477
SunONE 477, 481. See Sun Directory Server
Suspect Virus Quarantine
  about 199
  language encoding 201
  messages
    deleting 206
    language encoding 201
    number of entries on message list page 201
    releasing 206
    searching 203–204
    searching tips 204
    sorting 203
    viewing 200
  navigating 202
  number of entries on message list page 201
  purging 207
Suspect Virus Quarantine  (continued)
retaining messages 207
size, maximum 207
viewing 200
suspicious attachment 170, 178
Symantec Brightmail Gateway
about 21
architecture 28
components
    about 24
    hardware 28
    software 27
features 31
feedback 622
how viruses are detected 171
information, where to get 34
licensing 436–437
logs 403
new features 22
product documentation 34
software
    updating 474
    version 473
status 387
Symantec Mail Security. See Symantec Brightmail
Gateway
Symantec Security Response 132
synchronization
    configuring LDAP settings for 490
    full synchronization 481
    LDAP 400, 477
    status 396
    synchronizing changes 481
    troubleshooting procedure 505
    verify completion of 505
synchronize changes. See synchronization
sys-info command 632
syslog. See logs, syslog
system
    administrator. See administrator
    locale 453
    statistics 633
system-stats command 633

T

tail command 634
telnet command 635
templates
    best practices 302
    (continued)
    premium content control 302
    quarantined notification message 237
    regulatory compliance 302
tests, content compliance filters 329
third party sender lists
    specifying for sender groups 154
    using to block messages 143
threat categories 391
threshold
    Spam Quarantine 234–235
    Suspect Virus Quarantine 207
TLS certificate 457, 463–464
TLS encryption
    inbound Scanner settings for 100
    outbound Scanner settings 104
    per domain for routing, delivery 79
    specifying per local domain 83
    specifying per non-local domain 84
traceroute 436
trace route command 635
troubleshoot
    IM network connection 432
    replicating 504
    reports 385
    Spam Quarantine 246
    synchronization 505
true file types 311

U

undeliverable spam messages 246
unresolved email addresses 246
untested verdict 422
update
    definitions 191
    software, installing 636
update command 635
UPS monitoring 467
user groups. See groups
user interface certificate, HTTPS 457, 465
User Query, LDAP synchronization 481
user, find groups a user belongs to 67

V

variables, notification messages 242
verdicts
about 53
filtering actions available
email 56
IM 60
multiple actions per 61
omitted from processing 512
spyware or adware verdict 180
untested 422
verdict and action combinations 62
version command 636
virtual IP address 115
virus
Bloodhound settings 171, 189
container limits 189
definitions
for emerging threats 196
LiveUpdate 191
on demand 194
platinum 195
Rapid Response 191
source 195
status 193
updating 191
detecting 170, 172
exclude files from scanning, list
creating 184
deleting 187
disabling 187
enabling 187
exporting 188
modifying 186
heuristic settings 171, 189
policies
assigning to groups 68
copying 183
creating 179
default 175
default actions 68
deleting 183
disabling 182
enabling 182
modifying 181
verdicts and actions 56
reports 359
technologies that detect 171
virus attack recognition (continued)
   enabling 138
   how viruses are detected 171
   overview 132
virus filters. See virus
Vontu Network Prevent
delivering messages 51
routing messages to 50
Vontu Network Prevent integration
about 329
blocking messages 331
bypass mode 337–338, 340
configuring 334–336, 340
forwarding 332
maintenance 342
message queues 337–338
multiple Scanners 330
performance 333
policies 336, 340
ports 330–331, 334–335
preference 333
redirecting messages 331
reflecting 332
tagging, message 331
troubleshooting 333, 337–338, 342

W
watch command 637

Y
Yahoo IM
   blocking or allowing access to 269
   connection status 432
   using Standard vs. Japanese 254

Z
zip bomb. See container limit