

# SOPHOS

 email **security and data protection**

Reviewer's Guide

PureMessage for UNIX





# CONTENTS

<b>1: Product overview</b>	<b>4</b>
PureMessage management features	4
PureMessage benefits	5
PureMessage architecture	6
• PureMessage engine	
• PureMessage quarantine	
• PureMessage Manager	
• PureMessage administrative interface	
Email policy enforcement	7
Spam protection	8
Virus protection	10
Perimeter protection	11
Summary	11
<b>2: End-user interfaces</b>	<b>12</b>
Quarantine digest	12
End-user web interface	13
• On-demand quarantine review	
• End-user allow and block lists	
• End-user preferences	
<b>3: Managing PureMessage for UNIX</b>	<b>15</b>
Email filter policy management	15
• Tests and actions	
• Allow lists	
• Anti-spam rules	
Quarantine management	18
• Quarantine searches	
• Quarantine digests	
Reporting	20
Server administration	23
• Central server management	
• Delegated administration	
<b>Appendix I: PureMessage system requirements</b>	<b>28</b>
<b>Appendix II: PureMessage default configuration</b>	<b>29</b>
<b>Appendix III: PureMessage modules – tests and actions</b>	<b>30</b>

# 1: PRODUCT OVERVIEW

Sophos PureMessage® for UNIX is a secure email gateway solution providing integrated anti-virus, anti-spam, data loss prevention, policy enforcement and email management. It delivers scalable, reliable and proactive protection against inbound and outbound email-borne threats through a highly flexible and easy-to-use administrative interface.

Award-winning technology protects the enterprise network from email-borne viruses, Trojans, worms, and malicious spyware. By countering the rapid evolution of new spam techniques, PureMessage also keeps inboxes free of unsolicited bulk email and helps maintain network performance and employee productivity.

Automated tuning technology constantly balances a range of detection techniques to prevent protection failures. Genotype® technology blocks families of spam campaigns and viruses, ensuring that organizations are protected against previously unseen threats even before specific detection is available. PureMessage automatically receives the latest anti-virus updates and new spam rules created by expert analysts in SophosLabs™. In addition, administrators can implement email policies that further reduce the risk of customer privacy, intellectual property, and compliance regulations being compromised.

The powerful technologies which enable this high-level messaging security are complemented by a range of tools that simplify the administrative task. A centralized quarantine and powerful web-based management console enable single-point control of multi-server systems, while the end-user interface and digests allow end users to review quarantine contents easily. Delegated administration enables decentralized email management for defined groups, departments or completely separate organizations, placing the visibility and power to make decisions where they have the greatest impact.

## *Comprehensive gateway security*

Organizations of all sizes can benefit from the security offered by PureMessage against email-borne threats and policy infringements.

## PureMessage management features

- Automatically updated virus and spam protection powered by SophosLabs™.
- A web-based graphical user interface to manage the overall policies that drive the PureMessage filter.
- Flexible message-filtering policy management to define the handling of virus, spam and other email.
- Delegated administration of policy, reporting, quarantine and other features to sub-administrators.
- Quarantine digests to provide end users with scheduled quarantine review and a web-based end-user interface to manage their personal quarantine, allow lists and other spam-filtering preferences on-demand.
- Administrative quarantine management capabilities to query, analyze and maintain the organization's message quarantine.

- Global and per-user allow and block lists and configurable actions help organizations optimize spam protection to their unique needs.
- Comprehensive logging and reporting provides administrators with detailed feedback on filtering activity.
- Central server management to ensure multiple servers remain synchronized with the same rules and configurations.

### PureMessage benefits

<b>Unrivalled threat detection</b>	Detects over 99% of spam and protects against email scams, including phishing attacks. Detects, disinfects, deletes or quarantines viruses, Trojans, worms, and malicious spyware in incoming and outgoing email.
<b>Proactive protection</b>	Employs Genotype, Behavioral Genotype®, and Sender Genotype technology to catch evolving threats and dangerous applications.
<b>High accuracy</b>	Automatically balances a range of spam detection techniques to deliver consistent accuracy, minimizing false positives.
<b>Data loss prevention</b>	Provides powerful message and attachment content scanning controls to protect against confidential information leakage.
<b>Regulatory compliance</b>	Incorporates a rich policy environment to support complex security or regulatory compliance requirements.
<b>Global protection</b>	Protects global organizations from spam and viruses in multiple language message streams, including those that use double-byte characters.
<b>Automatic updating</b>	Updates automatically with the latest protection from SophosLabs™ – a global network of threat analysis centers.
<b>Delegated administration</b>	Group, department or customer-based management of policy, quarantine, reports, and more.
<b>End-user controls</b>	Provides end-user quarantine review, allow lists, and block lists.
<b>Mail system integration</b>	Integrates with popular mail transfer agents (MTAs), including Sendmail, Postfix, and Sun Java™ System Messaging Server. Other platforms can be supported via a relay configuration.
<b>Comprehensive support</b>	Includes unlimited 24-hour telephone, email, and online support, 365 days a year.

## PureMessage architecture

PureMessage is built around four major components:

- PureMessage high-performance filtering engine
- PureMessage administrative interface
- PureMessage quarantine
- PureMessage end-user interfaces.

### PureMessage engine

PureMessage’s filtering engine is split into two levels. Sender Genotype advanced connection control provides proactive botnet detection and reputation filtering at the connection level, rejecting up to 90% of connections and improving overall throughput and performance.

The PureMessage policy engine then performs policy-level filtering on the message stream. The policy engine:

- Intercepts messages at the email gateway level (using built-in or external MTA)
- Scans the messages for spam, viruses and other conditions as defined by the overall message filtering policy
- Applies policy actions to the messages
- Passes the message back to the MTA for delivery to the intended recipient or quarantines the message for review in the PureMessage quarantine.

The order of the tests, test conditions and actions applied to the message are all managed by configuring the overall PureMessage inbound and outbound message-filtering policy using the graphical PureMessage Manager interface.

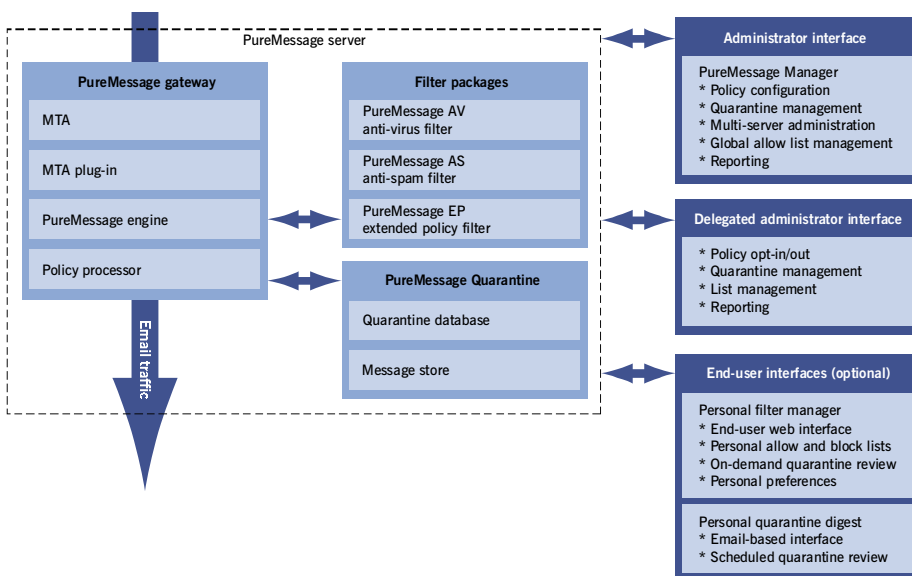


Figure 1: Principal PureMessage components

As shown in Figure 1 on the previous page, the PureMessage filters – anti-virus, anti-spam, and extended policy – scan the message for the particular threats or policy concerns, as driven by the overall message-filtering policy.

### PureMessage administrative interface

PureMessage administrative interface provides the administrative interface to the PureMessage engine, filters and quarantine, providing administrators with the ability to:

- Manage the overall filtering policy
- Configure the parameters governing the anti-spam, anti-virus and extended policy filters
- Manage the PureMessage quarantine
- Access the PureMessage reporting tools
- Manage the local server settings
- Synchronize multiple server configurations
- Delegate administrative responsibilities and control end-user interface capabilities.

The PureMessage Groups interface (also referred to as the delegated administration GUI) provides an alternative administrative interface. In addition to providing improvements to reporting and quarantine management, it can be used for domain and group-based or role-based delegation.

PureMessage also provides command-line access for advanced configuration and management.

### PureMessage quarantine

The database-driven PureMessage quarantine provides a highly scalable message store capable of managing tens of millions of messages distributed over multiple server quarantines. The quarantine provides a safe mechanism to store suspect messages temporarily at the gateway while enabling users to review their quarantined messages if necessary.

### PureMessage end-user interfaces

The optional end-user web interface and quarantine digests provide localized interfaces to enable users to manage their personal quarantined messages, allow lists and spam protection preferences in their preferred local language. These are described further in section 2 (pages 12 to 14).

### Email policy enforcement

Confidentiality breaches, legal liability, lost productivity, and damage to reputation can cost companies millions of dollars each year. Complex and evolving regulatory environments require organizations to protect themselves by establishing, monitoring, and enforcing appropriate use, receipt and regulatory compliance policies and procedures, at both the end-user and infrastructure levels.

### *Flexible email policy*

Using PureMessage's flexible policy framework, organizations can take complete control of inbound and outbound messages.

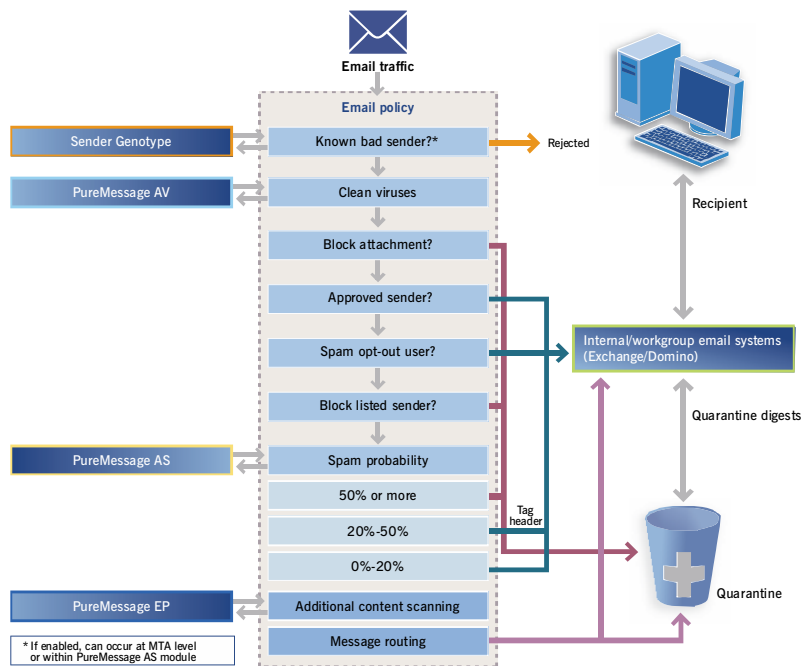


Figure 2: Typical inbound email flow

Sophos PureMessage’s RFC 3028-compliant policy framework is the most flexible available. As shown in Figure 2 above, it enables organizations to establish and enforce a clear policy governing the messages they will allow into and out of their gateway. The rules and actions that comprise this policy are configured using the PureMessage Manager.

PureMessage ships with a default policy governing spam and virus protection. Additional policies may be configured to meet an organization’s exclusive filtering requirements. By combining ready-to-implement tests, administrators can configure an overall policy decision tree that determines the tests processed by PureMessage, the test order, and which actions are applied based on test results. Using the policy repository, proactive administrators can prepare policies in advance ready for rapid deployment to deal with particular email events.

Common content policies that organizations enforce are:

- Discard messages containing a virus.
- Reject messages from known bad senders
- Quarantine messages containing harassing or offensive language
- Add disclaimers to outbound messages from specific departments
- Route or archive messages based on message content
- Quarantine and review messages with specific attachments to protect against leakage of intellectual property or sensitive content
- Monitor and log suspicious traffic for system abuse detection.

### Spam protection

Sophos’s unique email deconstruction and analysis process features the most advanced detection technology in the industry, complemented by 24/7 global

*Increased efficiency,  
lower overall costs*

PureMessage extends the life of your network infrastructure, delivering greater efficiency and lower total cost of ownership.

threat monitoring by SophosLabs. PureMessage's anti-spam technology employs a "cocktail" filtering methodology, combining hundreds of different tests of the sender IP address, message headers, structure and content that test for thousands of different conditions. For example, one test looks for common spam products – within that test PureMessage looks for more than 5.6 billion different ways spammers spell the word Viagra. If a spam indicator is detected, that result contributes to the message's overall spam probability.

The first line of defense is at the connection level. Sender Genotype advanced connection control provides proactive botnet detection and reputation filtering prior to content scanning. As much as 90% of inbound spam can be eliminated this way, substantially increasing message throughput without the need for added infrastructure investments. PureMessage can also perform a reputation filter at the policy level before scanning (see below). Identified at this stage, spam from known bad senders can be redirected or quarantined according to customized security preferences.

PureMessage analyzes message traffic and content for spam techniques and current spam campaigns, employing multiple spam detection techniques:

- Genotype campaign analysis identifies complex spam campaigns by recognizing characteristics common to a series of messages.
- Behavioral Genotype analysis identifies and blocks malicious code before it executes.
- Blocking of known bad URLs/domains by analyzing the message's call to action
- Advanced checksums of message content, attachments, and images by analyzing known spam content
- Obfuscation detection identifies techniques spammers use to obfuscate, or hide, their messages from spam filters
- Scam detection protects against phishing attacks and other fraudulent schemes that trick users into submitting personal or financial information or passwords.

A weighted scoring system combines the results of the individual tests to create an actionable, overall probability that a message is spam. Combining tests in this fashion maximizes the overall benefits of strong spam indicators, while mitigating the risks associated with individual techniques.

SophosLabs continually analyzes spam, automatically updating PureMessage customers with the latest protection every five minutes as new threats arise. This allows customers to maintain protection from the latest spammer activity without incurring substantial administrative effort. Sophos SXL technology delivers real-time anti-spam protection via online lookup, providing instant access to the latest anti-spam intelligence.

### Handling spam

Combining the results of all of the spam detection tests into an overall spam probability enables administrators to define spam handling actions based on the spam probability percentage.

### *Highly efficient spam filtering*

PureMessage for UNIX employs multiple anti-spam techniques to ensure protection against increasingly sophisticated spam campaign.

The optimum method for deploying PureMessage, and building end users' confidence in the filtering, is to adjust the anti-spam policy actions over time, increasing the aggressiveness as users become more familiar with the filters.

Typical steps in the process of adjusting the way spam is handled:

- 1 Before engaging the filters, create feedback mechanisms to ensure administrators can fine tune the system to eliminate false positives. A PureMessage implementation normally starts with the default Tag and Deliver mode, allowing users to see which messages would be blocked once quarantining is enabled.
- 2 Once end users are comfortable with the filtering process, the administrator can start quarantining spam messages above a certain probability, and then reduce this probability over time. When quarantining mail, most organizations choose to provide end users with the ability to review their quarantined messages using either the quarantine digest feature, the end-user web interface or both.
- 3 Finally, once the organization has total confidence in PureMessage's accuracy, it may choose to discard high-probability spam from the message stream completely.

A common production setup for spam probability thresholds is:

Spam probability	Action
91-100%	Discard the spam message
51-90%	Quarantine the message
41-50%	Add the spam score to the message subject and forward to the recipient
21-40%	Add a hidden x-spam header to that includes the spam score and forward to the recipient
0-20%	Deliver the message as normal

Sophos recommends allowing 2-3 weeks for optimizing PureMessage's spam threshold to your organization's requirements.

## Virus protection

The email gateway is a major route by which businesses are infected by viruses. Protection at the gateway provides an important first level of security, safeguarding the entire organization at a single point and enabling continued protection with one simple update. PureMessage incorporates Sophos's industry-leading virus detection engine to protect organizations from viruses entering the organization through email.

PureMessage checks all email traffic passing through the email server in real time, providing protection against mass-mailing worms and viruses, including the latest multi-faceted attacks that combine virus, spam, and DoS (denial of service) attacks. Viruses are stopped at the gateway before they can proliferate within a corporate network.

## Key protection

PureMessage protects an organization from virus infection at the email gateway.

Sophisticated threat-reduction technology provides a powerful ability to prevent even new, unknown email-aware worms from entering the business without having to update the anti-virus solution. PureMessage automatically checks executable content and files in email messages and attachments for malicious code and applies the appropriate policy to handle the message actions for fast and reliable protection.

When a virus outbreak occurs, PureMessage provides immediate protection against the new threat. Genotype® technology uses approximation methods to detect new variants of families of viruses, providing pre-emptive protection even before specific detection is available. With the option to set up attachment blocking and policy enforcement, organizations are also able to respond to email-aware worms, thereby protecting their internal email systems.

Behavioral Genotype technology provides proactive protection against malicious code before it can execute, providing the benefits of real-time Host Intrusion Prevention System (HIPS) without the need for a separately installed and administered application.

### *Proactive protection*

During a virus outbreak, PureMessage proactively protects organizations' email systems.

### Perimeter protection

Denial of service (DoS) and directory harvest attacks (DHA) are security threats that result in overloaded internal and gateway systems. To protect against these threats, PureMessage measures message velocity to detect anomalous traffic patterns that exceed the organization's typical legitimate mail volumes from all or specific senders. This monitoring enables organizations to detect and respond appropriately to DoS and DHA attacks.

### Summary

Sophos PureMessage provides the ideal mix of control and automation to support enterprise email management needs. It combines automated management and anti-spam updating with comprehensive tuning, feedback and management capabilities across multiple servers. This combination of facilities minimizes the day-to-day administrative load while providing the precise control that administrators need.

PureMessage also benefits from the complete insight SophosLabs has into email-borne threats. This enables proactive protection through faster analysis of new threats, multiple detection/update techniques (virus updates, spam updates, or policy updates) and complete management of the entire threat lifecycle.

Using PureMessage, organizations benefit from:

- Reliable protection against virus variants and evolving spam campaigns
- Proactive protection against new threats through SophosLabs and multiple detection approaches
- Powerful management tools to automate routine administrative tasks and complex message handling scenarios.

## 2: END-USER INTERFACES

With the ever-increasing threat, sophistication and volume of spammer activity, organizations are seeking the benefits of scalable, centrally managed gateway spam protection. Preferences vary over how to address a particular spam problem. The enforcement of a single spam policy can be managed exclusively by the administrator, with little or no end-user interaction. However, a global organization with multilingual message streams might want a solution that embraces its end users' preferences for localized interfaces, quarantine review and personal approved sender lists. The PureMessage end-user web and digest interfaces provide the unique ability to meet the full spectrum of these needs, from the simplest to the most complex.

The PureMessage end-user interfaces:

- Match the organization's needs and end users' preferences, with optional web-based and email-based interfaces and administrator-configurable end-user features
- Provide users with interfaces in their preferred languages
- Fit the spam protection to the organization's and the individual end-user's personal preferences, with both global and per-user allow lists and block lists
- Can exempt certain accounts with per-user opt-out control and organizational opt-out policy
- Provide ongoing visibility of the spam protection through scheduled quarantine review using email-based **Personal Quarantine Digests**
- Respond to urgent end-user needs with on-demand quarantine review through the end-user web interface
- Fit quarantine management to the end-users' real world schedules, with temporary hold features to maintain quarantined messages during extended absences.

Organizations planning to quarantine spam messages can implement either the quarantine digest or the end-user web interface functionality, or both. The end-user web interface enables users to review their message quarantines on demand, while the quarantine digest enables a scheduled review of the quarantine by emailing users a summary of the messages in their quarantine. Used together, these features provide simple mechanisms for users to manage their quarantine, either by scanning the message summary on a regular basis or by directly searching their quarantine if an urgent need arises.

### Quarantine digest

PureMessage provides end users with scheduled quarantine review capabilities through a **Personal Quarantine Digest** (see Figure 3). On a scheduled basis, end users receive via email a listing of new quarantined messages. They can quickly scan through this digest and retrieve any messages needed from the quarantine, eliminating the business impact of false positives.

### *Versatile interfaces*

Interfaces give users the choice of on-demand and scheduled reviews of their quarantined messages.

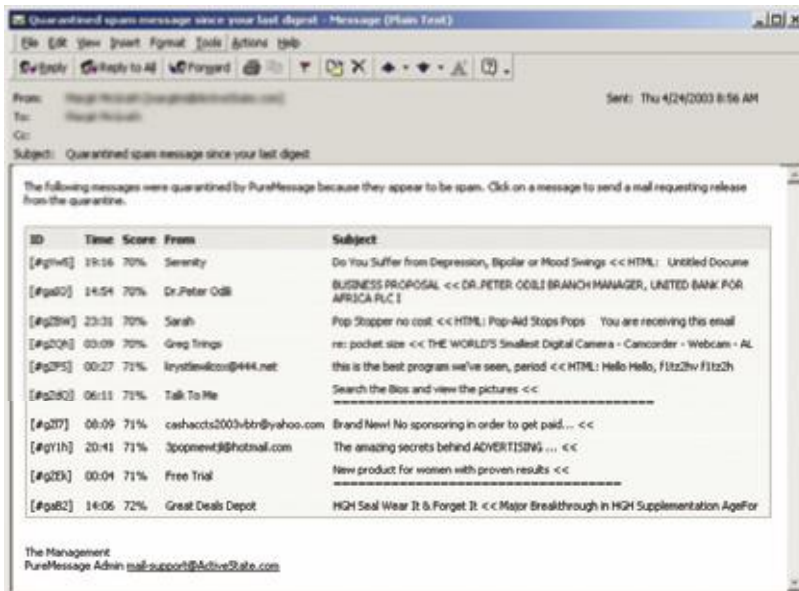


Figure 3: A sample quarantine digest sent to an end user

### End-user web interface

The end-user web interface enables organizations to provide their users with direct control over personal spam filtering preferences. End users can respond to immediate concerns through the ability to review their quarantine on demand, define their approved sender list, and configure their personal email filtering preferences.

### On-demand quarantine review

The end-user web interface provides users with an on-demand quarantine review mechanism, enabling them to check for new messages if they suspect an expected message has been quarantined. End users can access their list of quarantined messages via the interface, review their messages, and release them from the quarantine if necessary.



Figure 4: Blocked messages in an end user's quarantine

## End-user allow and block lists

Combining end-user and global allow lists and block lists lets end users control who they receive email from, while enabling the administrator to define organization-wide approved and blocked senders. This combination ensures low administrative effort to manage the lists, matching the spam protection to the differences in end users' preferences.



Figure 5: Approved senders in an end user's allow list

## End-user preferences

End-user mail-filtering preferences enable users to control how they interact with the spam filtering. By setting their preferences, users can choose to opt out of filtering, choose whether to receive **Personal Quarantine Digest** messages, and hold all the messages in their quarantine during an extended absence (see Figure 6).

- The PureMessage opt-out lets users with a specific need to receive their email unfiltered, such as a complaint desk, to opt out of all spam filtering and other filtering tests according to the organization's opt-out policy.
- The temporary hold facility enables end users, for the duration of an extended absence, to protect all their quarantined messages that could otherwise be expired during a quarantine clean-up.



Figure 6: Setting an end user's personal preferences

## 3: MANAGING PUREMESSAGE FOR UNIX

Administrators can manage PureMessage using either the web-based graphic user interface (**PureMessage Manager**) or the command line. This guide focuses on the PureMessage Manager.

Once logged in to the PureMessage Manager, the Dashboard screen provides a quick view of the system status, basic reports on mail activity, and quick links to tools supporting common tasks.

### *Graphic user interface*

PureMessage's easy-to-use web-based interface gives administrators access to system status, reporting and management tools.



Figure 7: PureMessage Dashboard

### Email-filter policy management

The rules that govern the overall message-filtering process are controlled via the **Policy** tab. This shows the overall message-filtering policy and provides complete control over how messages are handled.

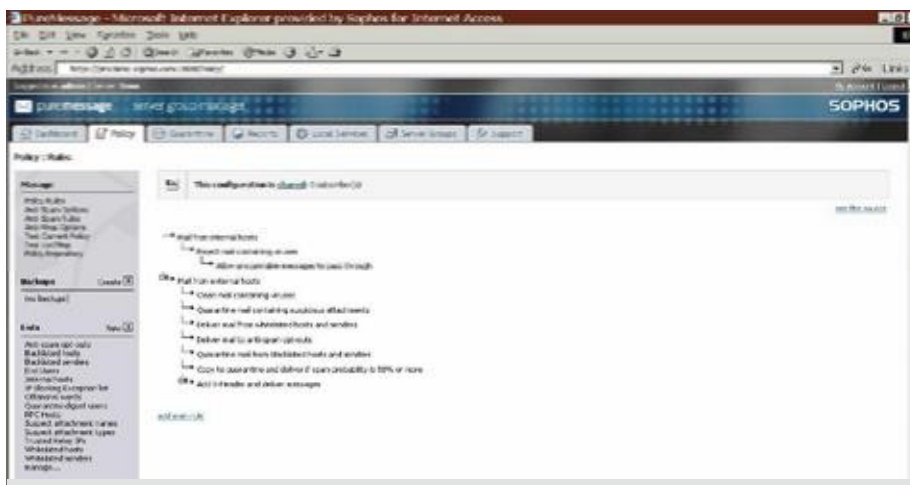


Figure 8: PureMessage Policy Manager

In addition to spam and virus protection, PureMessage functionality includes:

- Blocking large attachments or attachments of certain types by granular true file type detection, regardless of extension or content type header
- Adding disclaimers to outbound mail
- Checking for keywords, phrases and credit card numbers
- Encrypting messages using TLS or routing messages to third-party end-to-end encryption solutions.

The **Policy Manager** is typically used for:

- Email filter policy management
- Setting the spam disposition thresholds and policy
- Managing allow lists, block lists, and opt-out lists.

PureMessage allows you to create dynamic policies that use information stored in LDAP systems. This can simplify the ongoing maintenance of complex policies. Extensible architecture also allows you to integrate PureMessage with existing archiving, encryption or access control systems.

### Tests and actions

The rule-editing panel lists all the available test and action options, and defines the specific tests and actions to take when a certain rule is applied. For example, the **Quarantine and Deliver** rule applies two actions to the message if PureMessage assigns a spam probability greater than 50%:

- A hidden x-header is added to the message, listing the spam probability and rules that were hit
- A copy of the message is placed in the quarantine.

This configuration allows administrators to see which messages would be quarantined, without interfering with the message delivery.

### Managing policy

The Policy Manager is key to defining spam and controlling how messages are handled.

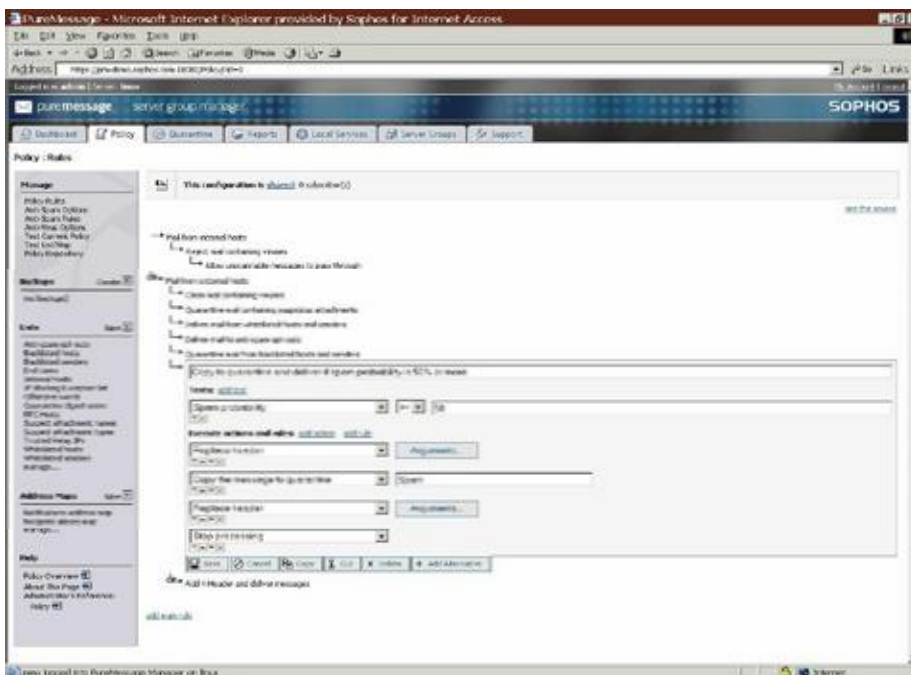


Figure 9: Configuring a spam-probability test

## Allow lists

The first step in all spam filter tuning is to add known, legitimate senders to the allow list. This is a simple mechanism for tuning the system and will allow all mail from the listed senders to bypass the spam filter. PureMessage offers both global and per-user allow lists, that:

- Enable administrators to define trusted senders for the entire organization, minimizing user burden
- Enable end-users to manage a list of the senders that they wish to receive mail from, embracing personal preferences.

## *Tuning the spam filter*

Creating an allow list is fundamental to tuning the system to accept all mail from approved addresses.

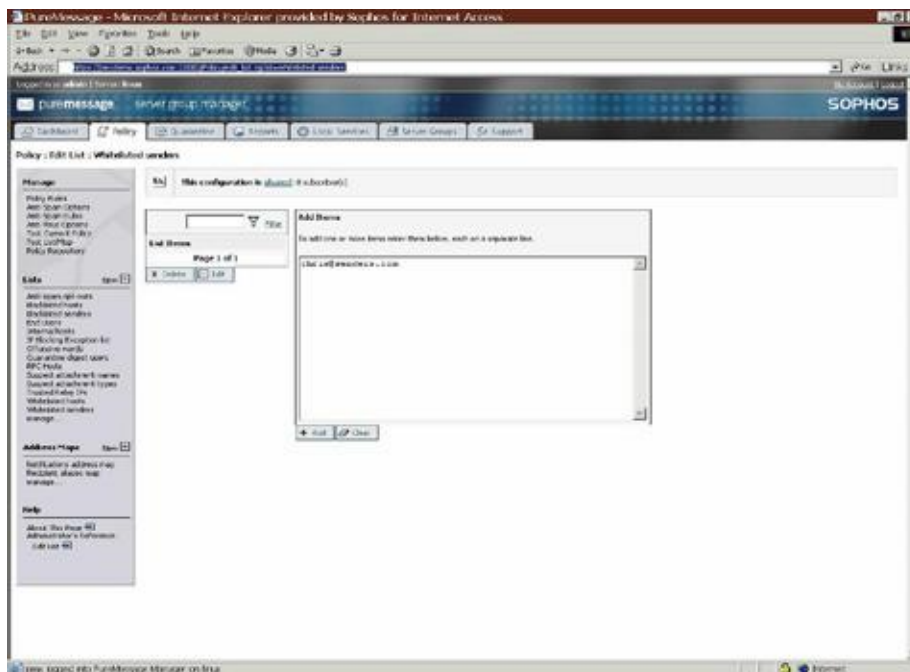


Figure 10: Adding an allow list entry

## Block lists

In addition to allow lists, global and personal block lists can also be created, discarding messages from unwanted domains without scanning or quarantining.

## Anti-spam rules

For organizations requiring more customized mail filtering, the **Policy** tab allows administrators to control how the filter operates. Using either the management console or the command line, administrators can easily create new rules, adjust existing rules, and edit specific tests to enforce email policy rules unique to their organization.

## Quarantine management

The **Quarantine Summary** page shows the basic quarantine reports, as shown in the lefthand tool bar in Figure 11. These provide information on the current status of the quarantine. There are two main elements to quarantine management:

- Querying the contents for specific messages through the **Manage Quarantine** option (see Figure 12), and
- Configuring the quarantine digests through the **Quarantine Digest** links.

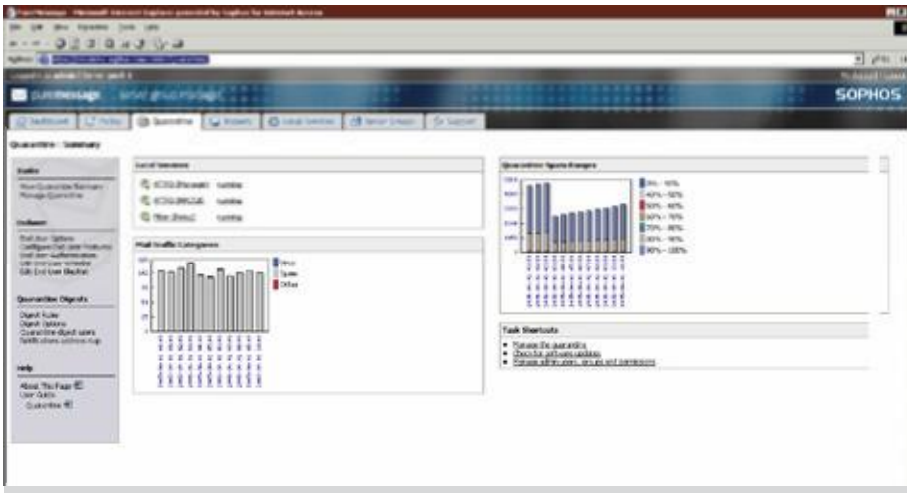


Figure 11: The Quarantine Summary page

## Quarantine searches

The administrator uses the quarantine query page to search the quarantine for messages, based on either simple or advanced query parameters.



Figure 12: Advanced queries using the Manage Quarantine option

The message review screen in Figure 13 lists the quarantined messages that match the parameters entered via the **Manage Quarantine** option above. It shows the content of messages and detailed information on why they were

quarantined, including all the rules that were hit. This powerful and unique feature gives administrators exceptional visibility into both the quarantine and the spam filtering.

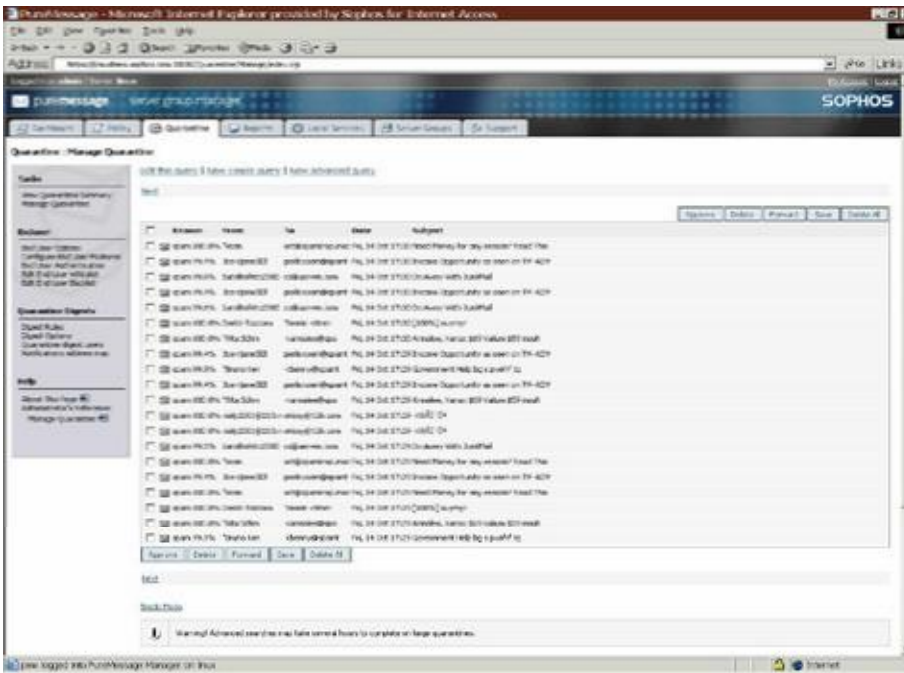


Figure 13: A list of quarantined messages

### Quarantine digests

PureMessage allows end users to review their quarantined messages through a personal quarantine digest delivered to them via email. They can quickly scan through and click to retrieve any message they want from the quarantine.

All users configured in the **Quarantine digest users** list will receive a scheduled notification if they have new items addressed to them in the quarantine. The user list can include specific users, or wildcards that enable an entire domain of users to be quickly added. This is a powerful way to minimize the administrative effort required to manage the entire quarantine, while helping end users manage their own quarantined messages effectively.

### Quarantine digest

PureMessage's quarantine digest eases the burden, both for end users managing their messages and for administrators managing the quarantine.

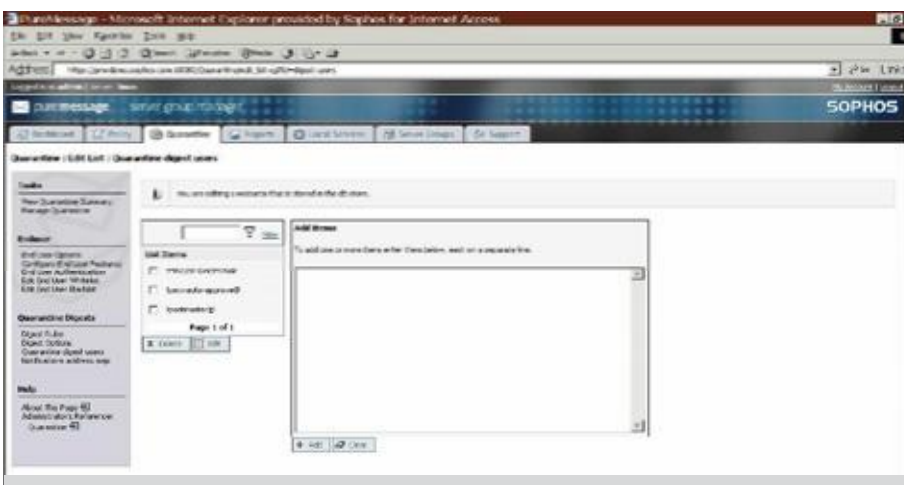


Figure 14: Editing the list of Quarantine Digest recipients

Administrators have full control over what features are available to their end users to provide users with the appropriate level of control for the organization. Access to quarantine digests, on-demand quarantine review, allow lists, block lists, or opting out are all under the administrator's control.

When the administrator enables the end-user web interface (see Figure 15), it gives users an on-demand quarantine review mechanism. This allows them to check for new messages if they suspect an expected message has been quarantined. The end user can access and review the message through the interface, and release it from the quarantine if required.

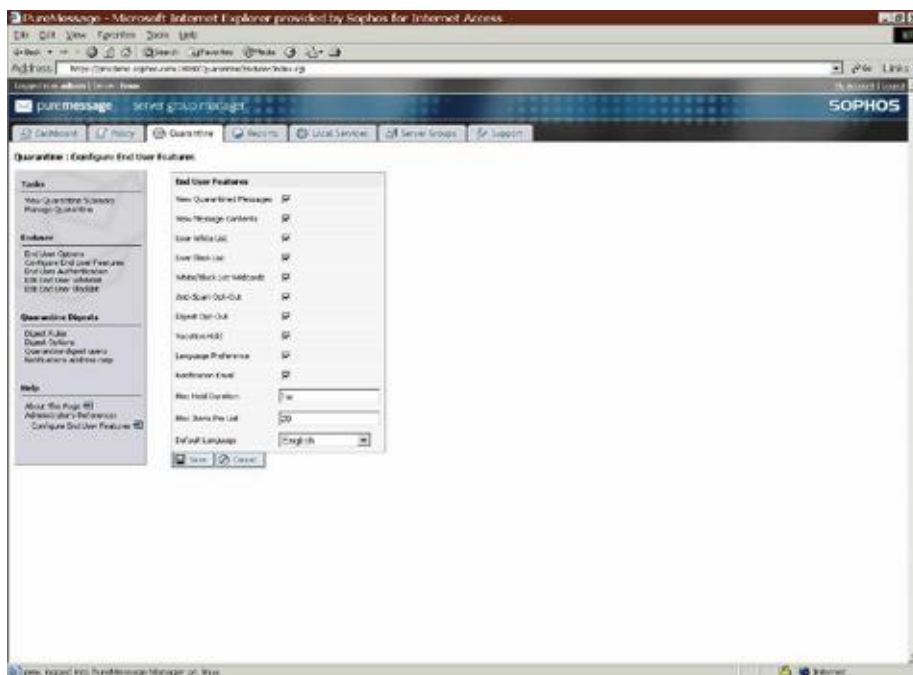


Figure 15: Enabling the end-user web interface

## Reporting

PureMessage offers extensive reporting and logging options, including administrator-controlled test logging, to ensure that PureMessage records exactly the information administrators need to analyze their message traffic and filter actions. Built on top of this logging framework is an enhanced reporting system that offers graphical and exportable tabular reports. These are available either on demand or delivered via email to administrators on a scheduled basis. When used with the **Central Server Management** option, PureMessage can aggregate and generate reports for single servers or for an entire server group.

## Comprehensive reporting

PureMessage provides a wide range of reports in a variety of formats, giving administrators a comprehensive view of system effectiveness.

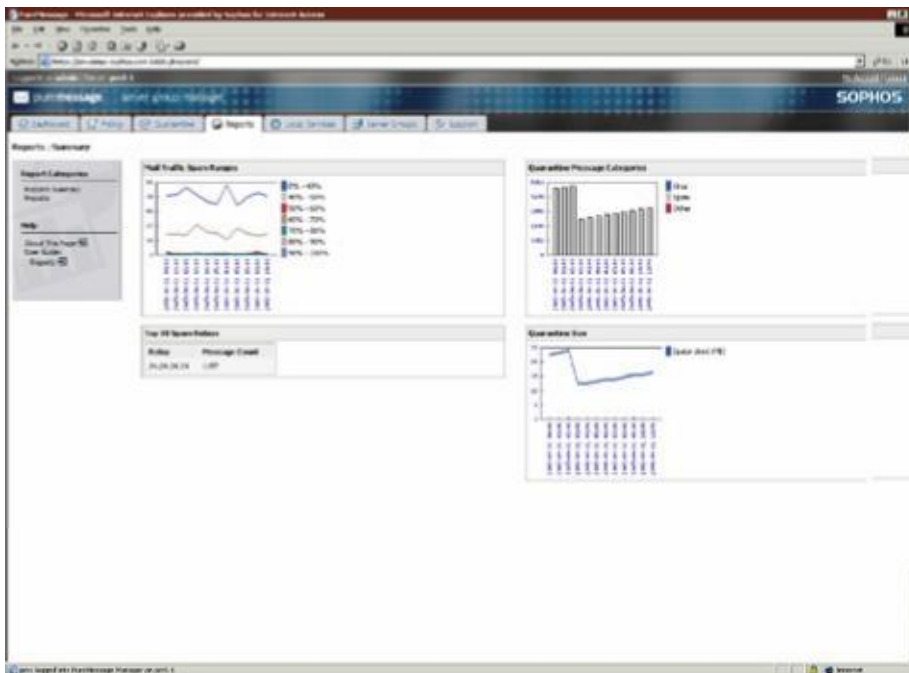


Figure 16: PureMessage Reports

Sophos PureMessage provides administrators with a broad range of reports on all aspects of system performance, message handling, and quarantine activity:

- Attachment Sizes shows the overall ratio of attachment sizes.
- Attachment Types shows the overall ratio of attachment types.
- Disc Usage shows the amount of disk space (KB) used by PureMessage.
- Memory Usage shows the amount of memory (KB) used by PureMessage.
- Message Categorizations shows the number of messages detected as spam, virus or other. If PureMessage determines that a message contains spam and also contains a virus, the message counts toward the virus total only. The spam threshold is 50% probability by default.
- Messages from Blocked IPs in Policy.
- OS Health shows the CPU (%), load average (\*100).
- Overall Spam Count shows the total number of spam messages received.
- Overall Virus Count shows the total number of infected messages received.
- Quarantine Size shows the size and number of messages in the quarantine.
- Number of Releases shows the number of messages released.
- Rejected MTA Connections
- Rule Hit Rates shows the frequency of spam rule matches.
- Spam Range Volumes shows the number of messages by spam probability range, which is shown as a percentage.
- Top Other Relays shows the top spam relays by number of other messages.
- Top Relays shows the top relays by number of messages.
- Top Releasers shows the top releasers of messages.

- Top Spam Recipients shows the top spam recipients by number of detected spam messages.
- Top Spam Relays shows the top spam relays by number of detected spam messages.
- Top Spam Senders shows the top spam senders by number of detected spam messages.
- Top Virus Relays shows the top spam relays by number of detected virus messages.
- Top Virus Types shows the virus types (categorized by virus name) found in messages.

Report-display options include:

- Report type (chart v table)
- Report timeframe (e.g. past 24 hours, past 7 days, past 30 days)
- Custom start and end dates
- Grouping options (all servers or by individual servers).

Report-handling options include:

- Print
- Export underlying data
- Schedule to run and be emailed automatically.

The **Reports** tab of the **PureMessage Manager** interface (see Figure 17) provides quick access to reports on mail filtering, quarantine contents, quarantine size, and other information used to monitor the effectiveness of the PureMessage system.

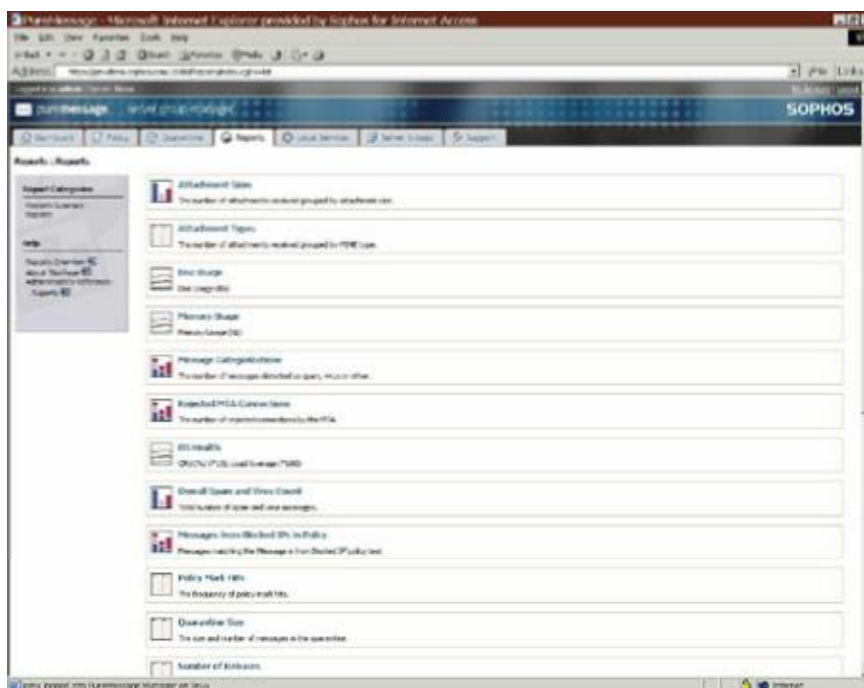


Figure 17: Report categories

Within a specific report there are further options to define the format and timeframe of the report, as well as print, export, or schedule the report for regular automatic email delivery.

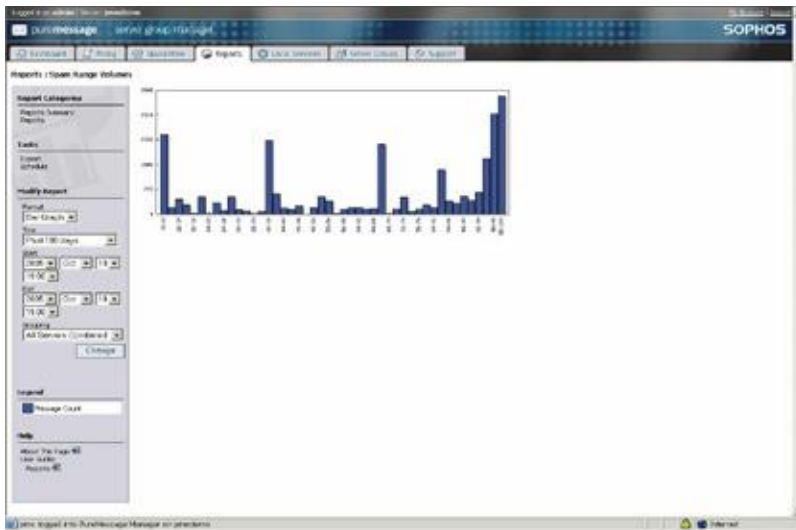


Figure 18: A Message Category report

## Server administration

The **Local Services** and **Server Groups** tabs are used to manage the individual server properties and to synchronize multiple servers to the same set of policies.

## Central server management

The **Central Server Management** module (see Figure 19) makes it easy for administrators to share configuration information and lists (grouped into **Publications** – see Figure 20) across multiple PureMessage servers. It also allows reporting on one or more servers in the group from a central console.



Figure 19: Central server management

## Reporting

Powerful reporting options enable administrators to monitor and analyze email traffic and filtering, both for individual servers and server groups.

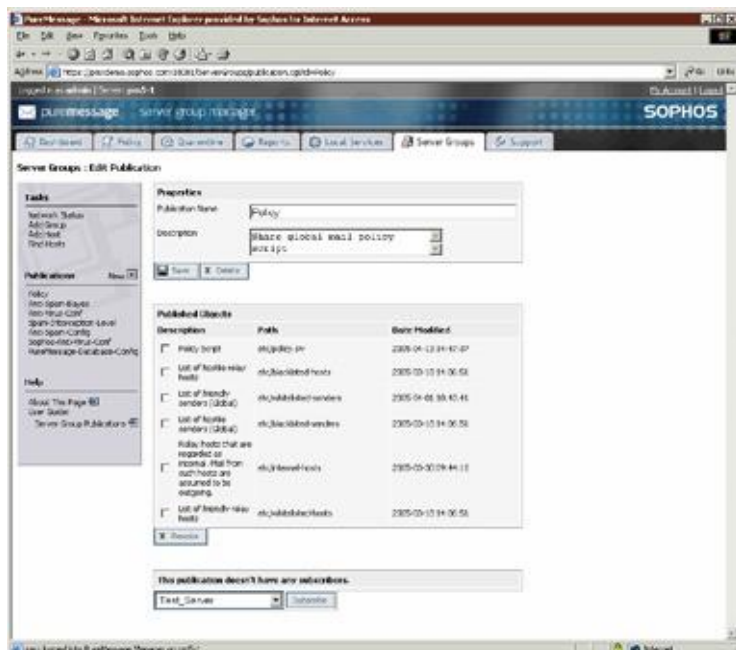


Figure 20: Managing the publications of shared server configuration

## Delegated administration

PureMessage for UNIX includes powerful management tools that enable shared administrative control of messaging systems. Designed for organizations with decentralized or fragmented email administration requirements, these tools allow policy decisions to be delegated beyond the central administrator, optimizing administrative effort by enabling control where it matters most. For example, the master PureMessage administrator can expose different policy rules to email administrators from different groups, departments, or organizations. Depending on the desired level of control, these sub-administrators can choose to opt in or out of certain rules. They can also run their own mail traffic reports and search their own quarantine.

Using delegated administration, sub-administrators can do the following:

- Opt in or out of spam, virus, and suspect attachment checking.
- Manage group lists (allowed/blocked relays, allowed/blocked senders, offensive words).
- Manage group message disclaimers (inbound and outbound).
- Run group reports (mail trends, relays, top senders/recipients).
- Search and manage the quarantine.
- Search logs to quickly access message forensics.
- Activity logging.

Sub-administrators do NOT have access to the following:

- Policy tree for rule creation/deletion/modification.
- Command line.
- Server administration.
- Global allow lists and block lists.

## Sub-administrator autonomy

The master administrator can grant varying levels of autonomy on policy rules, reporting, and quarantine searching to email administrators in different groups, departments, or even organizations.

Sub-administrators use a different GUI than the master administrator. This new GUI provides easy, visually appealing access to the features outlined above.

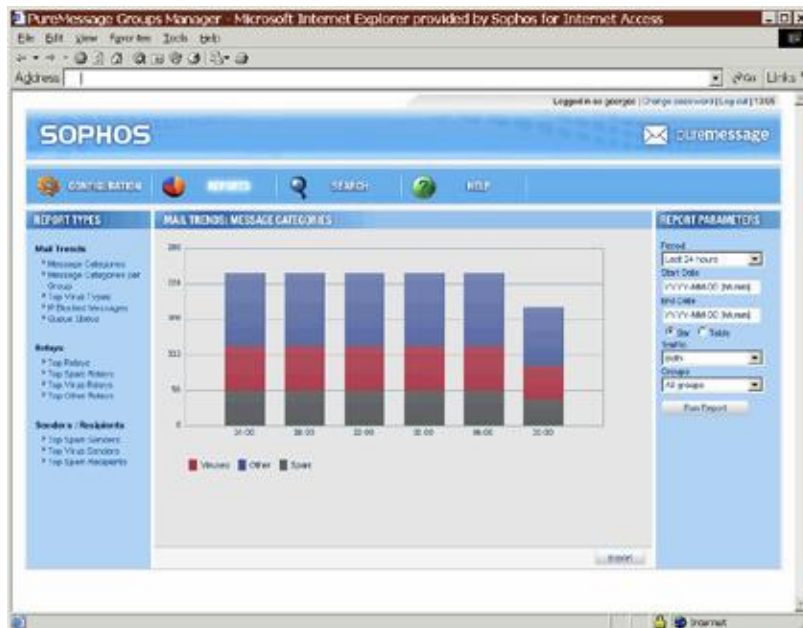


Figure 21: Delegated administration view of message categories report

Delegated administration is particularly useful for internal Help Desk and HR departments, as it allows granular access control of given features such as the quarantine. For example, the HR team can be granted quarantine visibility only for selected reasons (e.g. offensive content), without the authorization to configure rules or release messages from the quarantine. Similarly, one designated group can be given the option to opt out of spam checking while all other groups are not given the option. This ability to tailor administrative privileges to assigned groups greatly reduces the workload of the master PureMessage administrator.

The following figures are sample views of the delegated administration GUI as seen by the master administrator.

The delegated administration GUI contains a powerful yet easy-to-use quarantine search page. From this page, the sub-administrator can view quarantined messages, check on their status, and process them (Approve, Forward, Save, Delete).

### *Reduced workload*

The workload of the master administrator is substantially reduced with tools that allow granular control of groups' access to certain PureMessage features.

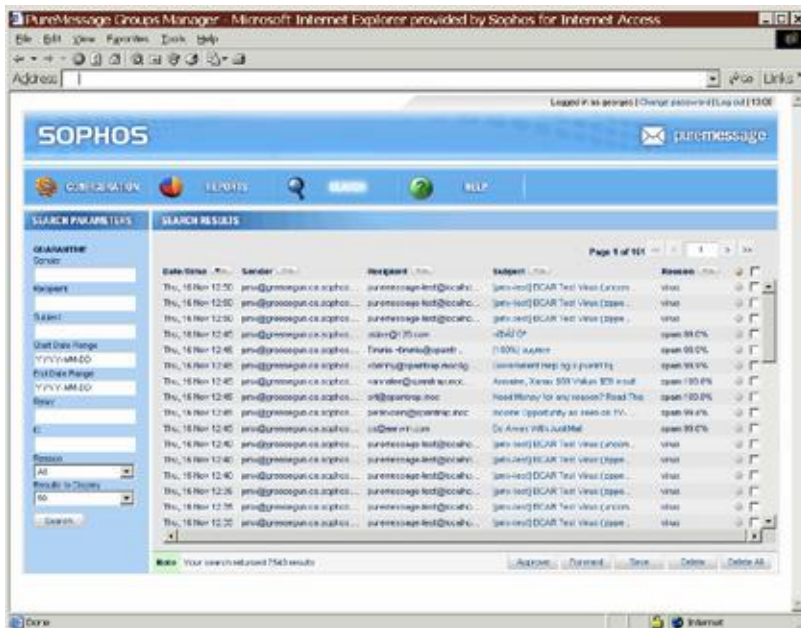


Figure 22: Delegated administration view of quarantine search results

Clicking on the subject line of a message in the search results will reveal more detailed information about the message, its delivery path, why it was quarantined, and its status in the quarantine.



Figure 23: Delegated administration view of quarantine message details

In addition to quarantine searching, the delegated administration GUI can be used for message forensics. Similar search parameters can be used to perform powerful log searches across multiple servers, allowing administrators to quickly determine how a message was processed by PureMessage.

**Important note:** The delegated administration GUI cannot be used by the master administrator to manage the PureMessage servers or policy tree. These tasks can only be done through the standard GUI.

# APPENDIX I: PUREMESSAGE SYSTEM REQUIREMENTS

## Platforms supported\*

- 64-bit Red Hat Enterprise Linux on x86-64 (4 and 5)
- 32-bit RedHat Enterprise Linux on x86/x86-64 (3 to 5)
- 32-bit SUSE Linux on x86/x86-64 (Enterprise Server 8 to 10, Professional 8 to 9.2)
- 32-bit Debian on x86/x86-64 (3.0, 3.1, 4)
- 32-bit FreeBSD on x86/x86-64 (5.4, 6.1, 6.2, 6.3)
- Sun Solaris on SPARC (8 to 10)
- Sun Solaris 10 on x86/x86-64

## Gateway/email platforms

- Includes Sendmail 8.13.6; supports versions 8.11.6 or higher
- Includes Postfix 2.5.4; supports version 2.0.x and 2.1 or higher
- Supports Sun Java™ System Messaging Server 5.2 and 6 on Solaris SPARC
- Other email platforms: supported via relay configuration

## Memory

- Minimum: 1 GB
- Recommended: 2 GB

## Disk space

- 500 MB plus quarantine space

---

\* Run as a native operating system, or as a virtual operating system using VMWare ESX (for Linux) or Sun Solaris 10 containers (for Solaris).

## APPENDIX II: PUREMESSAGE DEFAULT CONFIGURATION

PureMessage ships with the following default policy configuration options:

### Anti-virus options

- Inbound messages with viruses will be cleaned; a copy of the message will be quarantined.
- Inbound message attachments are checked using true filetype identification. Any suspicious attachments will be quarantined. (PureMessage ships with a customizable list of suspicious attachment types.)
- Outbound messages with viruses will be rejected; unscannable messages will be passed through.

### Anti-spam policy options

- Messages with sending relays in the IP blocklist will be quarantined (Sender Genotype).
- End-user allow list and block list enabled.
- Global allow list and block list enabled.
- Recipient opt-out list enabled.

### Anti-spam message handling

- Message from an allow listed sender – deliver.
- Message intended for spam opt-out user – deliver.
- Message from block listed sender – quarantine.
- Message with a spam probability greater than 50%:
  - Tag the message subject as spam
  - Add a hidden header and include filtering results
  - Place a copy of the message in the quarantine
  - Deliver the original message.
- Message with a spam probability less than 50%:
  - Add a hidden header and include filtering results
  - Deliver the original message.

### Policy filter options

Sender Genotype (proactive botnet detection and reputation filtering) at the MTA level is off by default, but is on by default at the policy level. The default configuration does not include any specific policy options, but can be configured to support most email management policies. Sophos can help advise you on appropriate policy filter configurations if you are interested in enforcing specific email policies.

## APPENDIX III: PUREMESSAGE MODULES – TESTS AND ACTIONS

Sophos PureMessage is available with options for anti-virus, anti-spam, and extended policy filtering. The options licensed determine which policy tests and actions are available within the overall PureMessage policy framework.

The tests and actions available with each module are listed below:

All modules	Tests	Actions
	Header address (To, From) <sup>1</sup> Envelope information Header information (including subject) Message size Header size Body size Relay (internal/external) Deliver mail for (i.e. opt out) Header contains (word/phrase) <sup>1</sup> Enables global and user-specific allow lists and block lists	Keep Discard Reject Redirect Tempfail Add recipient Forward Quarantine Map recipients Add/Replace/Delete header Notify sender or recipient Add log entry
Module-specific	Additional tests	Additional actions
PureMessage AV (Anti-Virus)	Virus presence Specific virus presence Suspicious attachment	Clean virus Block message with suspicious attachments
PureMessage AS (Anti-Spam)	Known bad sender/Sender Genotype <sup>2</sup> Spam probability Spam rule hit Offensive word/phrase check <sup>2</sup> Can be applied at MTA level or within PureMessage policy	
PureMessage EP (Extended Policy)	Keyword/phrase check (message and attachment) Credit card check Attachment name Attachment type Number of attachments Attachment size 8-bit percentage	Replace/change body Drop attachment Rename attachment Add banner Route or copy message (to encryption or archiving solutions) Archive

# SOPHOS

Boston, USA | Oxford, UK

© Copyright 2008. Sophos Plc. All rights reserved. All trademarks are the property of their respective owners.  
rg/081023

