

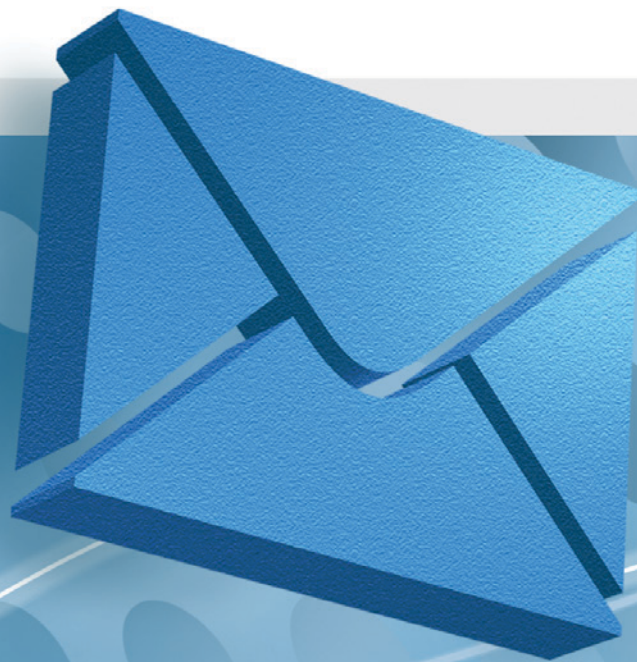
SOPHOS



FOR MICROSOFT EXCHANGE

Reviewer's Guide

 email **security and control**



WELCOME

Welcome to the reviewer's guide for Sophos PureMessage™ for Microsoft® Exchange, part of Sophos Email Security and Data Protection. The guide will introduce you to the solution's key features, provide an overview of its single centralised management console and explain its corporate policy enforcement functionalities.

Like all our solutions, PureMessage for Microsoft Exchange is the product of more than 20 years' experience protecting business, education, and government organisations. It delivers integrated email gateway and Exchange Information Store protection against all email-borne threats including spam, phishing, viruses and spyware. It allows you to control the information your organisation sends and receives, provides protection against the loss of confidential data and guards against the inappropriate use of your email system.

Sophos is acclaimed for delivering pre-emptive detection and protection from increasingly complex and fast-spreading security threats and for our high-levels of customer satisfaction. All our licences include comprehensive 24-hour support from our worldwide network of support engineers every day of the year, which is available at no additional cost. PureMessage for Microsoft Exchange is also backed up by SophosLabs™ – our global network of threat analysis centres – which provides a rapid response to emerging and evolving threats.

For information on pricing and how to buy PureMessage for Microsoft Exchange, please contact your local Sophos representative.

To find out who to contact in your area, please visit:

www.sophos.com/companyinfo/contacting

If you would like to request an evaluation, please go to:

www.sophos.com/puremessage-download

CONTENTS

1	A BRIEF OVERVIEW	4
2	CENTRAL MANAGEMENT FROM A SINGLE CONSOLE	6
	Dashboard	6
	Activity monitor	7
	Active Directory integration and synchronisation	8
	Users and groups	8
3	CORPORATE POLICY ENFORCEMENT	9
	Simplified policy setting and enforcement	9
	Powerful anti-malware scanning	10
	Industry leading spam protection	10
	Content filtering	12
	Disclaimers	13
	Quarantine management	14
4	COMPREHENSIVE REPORTING	15
	Reporting tool	15
	Graphs	16
	APPENDICES	
I	Sophos products for the enterprise	17
II	Other Sophos products and services	18
III	System requirements	19

1: A BRIEF OVERVIEW

PureMessage for Microsoft Exchange stops spam and malware from entering your email infrastructure. A mix of control and automation supports all of your email management needs and delivers complete and proactive protection.

Our award-winning technology scans email as it enters your network, once it is within it and when it leaves. As shown in Figure 1, it also scans the Exchange Information Store. This multi-layered approach not only detects viruses, Trojans, worms and spyware, but helps keep your organisation's inboxes free of unsolicited bulk email, thereby maintaining both network performance and employee productivity.

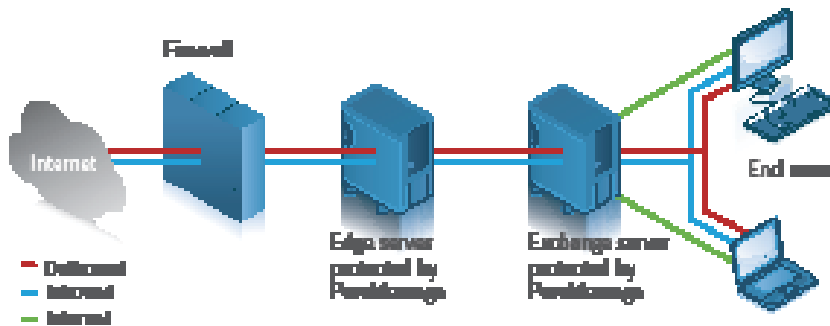


Figure 1: Inbound, outbound and internal mail is scanned for multiple threats

PureMessage for Microsoft Exchange can also protect you against threats before they happen thanks to Sophos's Genotype® technology, which can recognise and block entire spam and virus families. The Genotype technology that is used in our anti-virus and anti-spam engines is constantly updated and block up to 90% of malware without the need for specific threat data.

Further protection is delivered through Dynamic Code Analysis, pattern matching, emulation and heuristics and automatic malicious code checks. We also confirm the reputation of a sender through SXL, which stands for Sophos eXtensible List. SXL is a real-time database that contains instantly available anti-spam data that is easily updated as threats evolve.

PureMessage for Microsoft Exchange is also updated automatically by SophosLabs every five minutes with new spam rule updates. We ensure that the size of each update is very small (typically around 40k per update) so as not to interfere with your network speed.

The solution allows you to run Sophos's default anti-virus and anti-spam policies or set your own, while content and attachments can be filtered in many different ways.

Comprehensive security

PureMessage for Microsoft Exchange offers multi-layered protection against known and unknown threats, and detects over 98% of spam.

After reading the guide you will have a deeper understanding of how PureMessage for Microsoft Exchange delivers cost-effective and reliable protection against known and unknown threats to computer security, and how it provides complete control over all email content within your organisation.

PureMessage for Microsoft Exchange benefits

Unrivalled detection of malware	Detects up to 98% 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.
Proactive protection	Uses Genotype technology to catch evolving threats and dangerous applications.
High accuracy	Automatically balances a range of spam detection techniques to deliver consistent accuracy, minimising false positives.
Intellectual property protection	Provides powerful content scanning controls to protect against confidential data leakage.
Regulatory compliance	Incorporates a rich policy environment to support complex security or regulatory compliance requirements.
Global protection	Protects global organizations from spam and viruses in multiple language message streams, including those that use double-byte characters.
Automatic updating	Updates automatically with the latest protection from SophosLabs – a global network of threat analysis centres.
Delegated administration	Group, department or customer-based management of policy, quarantine, reports, and more.
End-user controls	Provides end-user quarantine review, allow lists, and block lists.

2: CENTRAL MANAGEMENT FROM A SINGLE CONSOLE

The console allows you to manage PureMessage for Microsoft Exchange from a single computer. From it you will see a real-time view of your entire email infrastructure and can manage various functionalities, such as email throughput and volumes, reports and the quarantine area. You will also use the console to set-up and configure policy rules, troubleshoot potential problems and – if required – launch an integrated response to any emerging threat.

Dashboard

The dashboard's simple design allows you to see events as they occur, giving you the opportunity to anticipate potential hotspots more easily and manage your system more efficiently. As shown in Figure 2, there are a number of visible live graphs that provide information on message, spam and virus volumes. Each one comes with a throughput base line which allows for the quick identification of abnormal email traffic patterns.

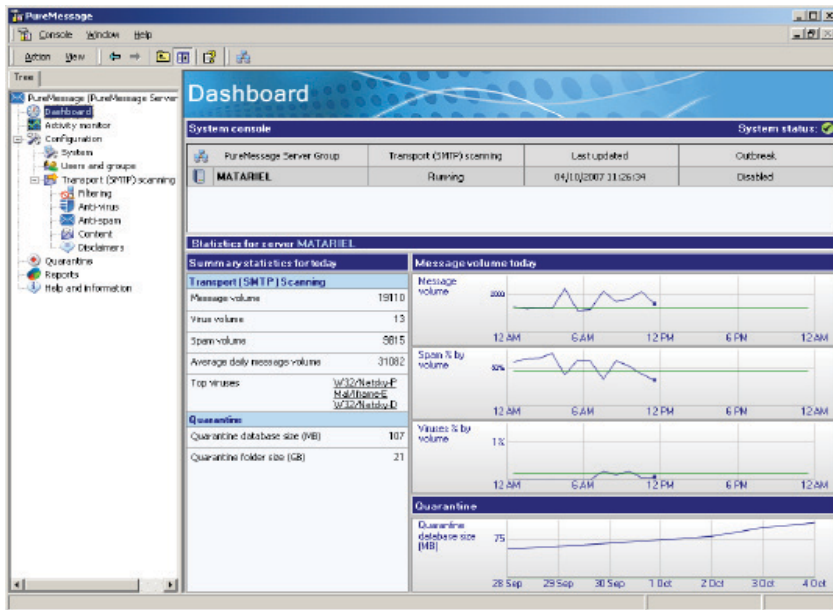


Figure 2: The dashboard provides real-time views

You can also select the name of any individual server through the dashboard and display the key daily statistics for it in either table or graphical form. If you have several PureMessage servers configured within a single group, then each server (including those that are clustered) will be listed on the dashboard. Each one can then be selected in order to obtain its key daily statistics in either tabular or graphical form and any configuration changes will be automatically applied to all servers in the group.

A single indicator light on the dashboard highlights the status of each server. A green signal indicates that everything is running as it should, while a red light acts as a warning. One primary reason for a red warning signal is that PureMessage has detected a virus outbreak and is undertaking corrective measures. In some cases, a red light could mean that Exchange Information Store scanning or AutoUpdate is unavailable, which may just indicate that there is an interruption in your internet connection.

Activity monitor

The console also provides access to the Activity monitor, which supplies a real-time count of the number of messages that PureMessage is processing. As can be seen in Figure 3, this figure is then divided into the categories the solution automatically looks for (as explained more fully in chapter 3), such as emails containing offensive language, encrypted attachments or inappropriate phrases. This counter can be stopped at any point to analyse whether your settings are effective or need adjustment.

Complete control

The PureMessage for Microsoft Exchange console delivers simple policy-based management and easy-to-execute functionality from just one central point.

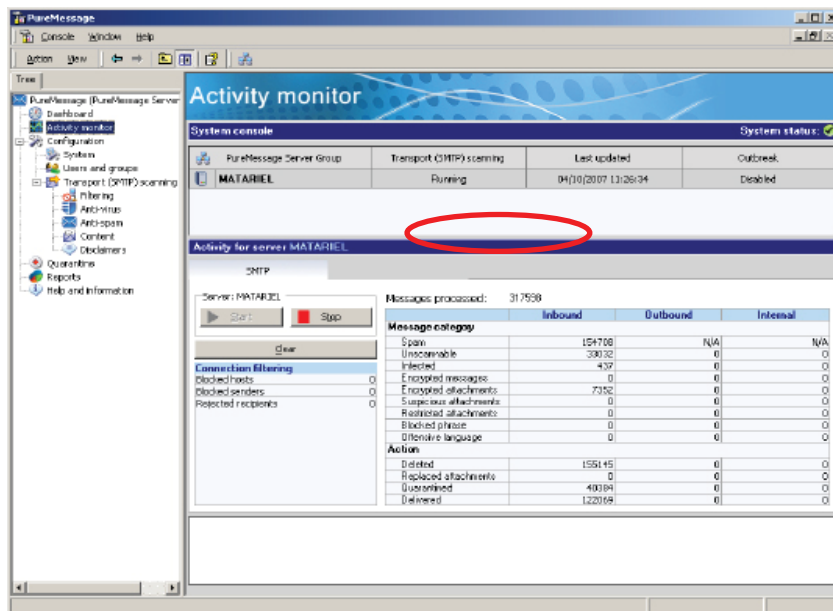


Figure 3: Activity monitor supplies instant message volumes and other data

In addition to providing a detailed breakdown of the number of emails your organisation is receiving, Activity monitor can assist help desk staff identify when a network – or a particular group within that network – is, for example, being targeted by a spam campaign.

Active Directory integration and synchronisation

Organizations using PureMessage for Microsoft Exchange can still make full use of their existing Active Directory user and group structures, which will help you reduce your administration overheads. PureMessage integrates seamlessly with Active Directory so that any changes made in the directory are automatically synchronised with the Sophos solution.

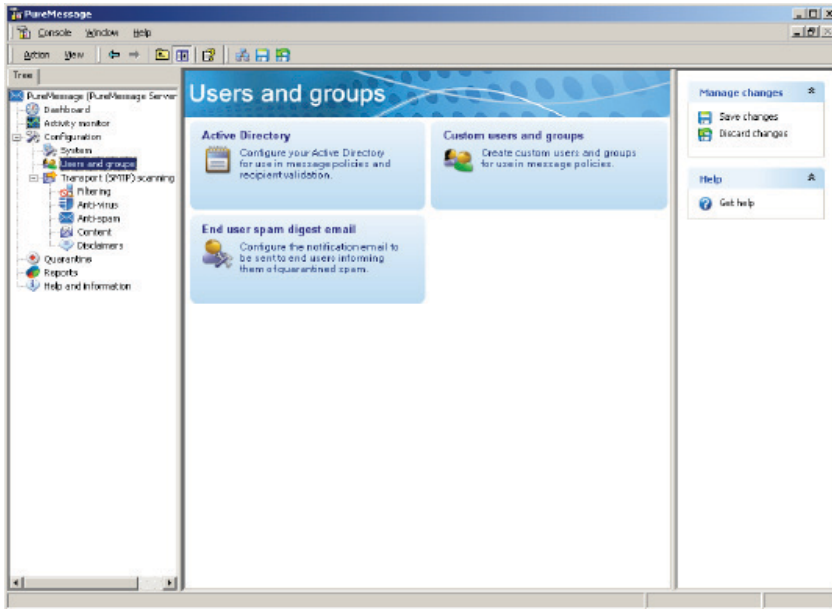


Figure 4: You can make exceptions in email policy for specific users or groups

Users and groups

While policy enforcement (which is covered in more detail in the next chapter) is set by default to activate across your entire network, you can use the console to make exceptions for specific users, groups or a combination of both, as shown in Figure 4.

3: CORPORATE POLICY ENFORCEMENT

Simplified policy setting and enforcement

PureMessage for Microsoft Exchange allows you to centrally configure and consistently enforce your corporate email policies. This helps you to control your organisation's flow of information and prevent the accidental or malicious loss of data, or the distribution of inappropriate material.

An email policy that is correctly configured can greatly reduce email attacks against your network, which is why the solution comes equipped with a number of pre-installed default policies that are based on Sophos's in-depth knowledge of anti-virus and anti-spam enforcement. As shown in Figure 5, emails travel through a number of procedures and at certain points are scanned for viruses, spam and inappropriate content. If an email is identified as being suspicious it will either be blocked, rejected, quarantined or delivered if eventually passed as clean. You can re-write these policies to suit your individual requirements and set exemptions for individuals or groups.

Policy flexibility

Administrators can customise policies so that incoming mail is treated differently from outbound mail, or so exceptions are made for specific users or groups.

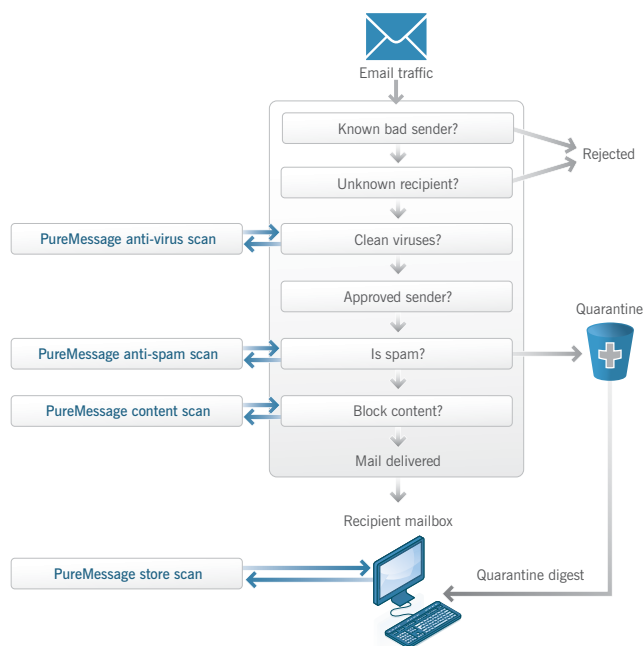


Figure 5: Policies can be customised to manage email in different ways

PureMessage for Microsoft Exchange also allows you to configure your policies to cover email direction, making it possible to set a policy for inbound email, another for internal email and a third to cover outbound email. Even if malware were to enter a network, the separate policies ensure that email distribution and bandwidth efficiency would remain unaffected.

Policies can be written to block certain words or phrases within the main content of an email or its subject line and can cover attachments, such as JPEGs and all common office programs. In addition, policies can also deal with known spammer assets by ensuring that you catch the hyperlinks within an email that are designed to encourage users to click through to a malicious website. All of these techniques are discussed further on page 11.

Powerful anti-malware scanning

PureMessage for Microsoft Exchange incorporates Sophos's malware detection engine which scans all emails entering and leaving the Exchange Information Store. It provides protection against all kinds of threats including those that combine virus, spam and DoS (denial of service) attacks. PureMessage can be configured to scan the Store in a number of different ways: background scanning will sweep all emails at specific times or it can be set-up to provide continuous 24-hour scanning.

PureMessage for Microsoft Exchange also scans for PUAs (potentially unwanted applications) and can block users from downloading them. PUAs are not generally considered malicious, but can be viewed as unsuitable for business needs. Examples include applications such as adware and remote administration tools.

Industry-leading spam protection

Spam can account for up to 60% of all daily incoming email that attempts to penetrate your gateway. To combat this, PureMessage for Microsoft Exchange filters suspicious email in hundreds of different ways, one example being a test that looks for the billions of different spellings of the word Viagra.

From the initial scan the solution determines whether an email is spam or suspected spam by using a scoring system. In the example shown in Figure 6, if an email has a rating of 90 to 100 it is categorised as spam, while anything rated between 50 to 90 is treated as suspected spam.

Intelligent filtering

Threats are usually stopped at the gateway by a combination of aggressive scanning and multi-layered filtering that identifies the good from the bad.

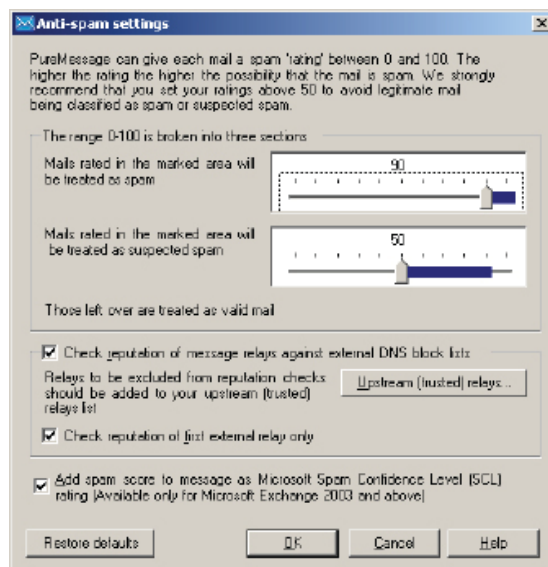


Figure 6: A score system determines if an email is treated as spam

You can, of course, tailor these thresholds to suit the specific operational environments of your organisation.

Spam scoring can be compared against the overall email flow and the quantity captured at a specific score reproduced as a standard report, as shown in Figure 7 below. In this example, the report identifies how email is scored and how much is blocked versus the category settings, enabling you to fine tune your scoring system. If you are running Microsoft Exchange 2003 or later, PureMessage can calculate the spam score as a Microsoft Spam Confidence Level (SCL) rating. If you choose to configure the system in this way, any message delivered to end-users with a SCL

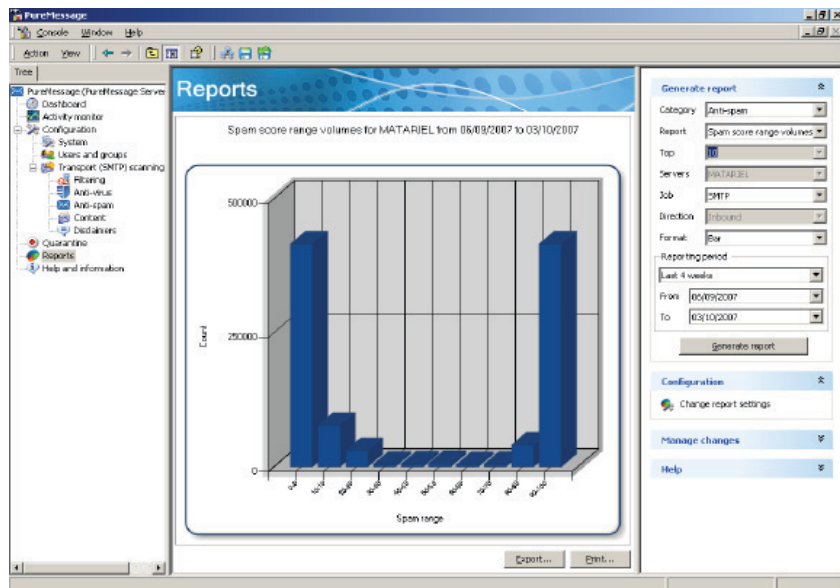


Figure 7: Instant reports show how much spam is being blocked

rating higher than the PureMessage value is automatically diverted into a user's Junk Mail folder in Microsoft Outlook.

Spammers often snare unwary users through placing a malicious hyperlink in an email and encouraging them to click on it. As mentioned earlier, PureMessage for Microsoft Exchange deals with this through spammer asset tracking, and does so by:

- Evaluating URLs contained in an email and blocking those messages that contain links to a known spammer's web assets
- Filtering URIs and blocking any messages that link to hijacked, freeweb and other suspect websites
- Checking against the Sophos IP Block List for known spam servers, open proxies and hijacked systems.

Configuring trusted upstream relays will also help you improve your email scanning speeds and spam detection. By default, PureMessage for Microsoft Exchange runs a reputation check on every email's server IP address. However, this is skipped if the address is on the trusted upstream

relay list, which shortens the time it takes an email to reach its recipient.

Content filtering

The optimum method for deploying PureMessage for Microsoft Exchange and building end-user confidence in its content filtering is to gradually adjust the content policy actions over time, increasing their aggressiveness as users become more familiar with the filters.

There are two broad types of content policies available:

Attachment type

This policy identifies and blocks email attachments that are commonly known to carry malicious code, such as screensavers. A list of recognised file types is constantly updated by SophosLabs and can identify a file's format even if the file name extension has been changed.

Phrase/regular expression

This policy looks for full and partial phrases and regular expressions that you deem unacceptable. PureMessage for Microsoft Exchange also comes with a list of terms and words that are commonly considered offensive, which you can apply by default.

PureMessage for Microsoft Exchange also uses Windows Filters to analyse content within common document types, such as Word and Excel.

Once the content policy has been defined an action, and any exceptions, can be applied when an email is captured.

Common actions are:

- Delete
- Log only
- Replace with text
- Quarantine
- Quarantine and deliver.

The last option allows you to quarantine a blind copy of an email, which is particularly useful for monitoring sensitive data contained within outbound emails.

Disclaimers

The disclaimers option allows you to add unique text to all outbound messages and can be configured for specific groups or individual users. As the example in Figure 8 on the page opposite shows, promotional text can be added to emails sent from the sales team or you could provide helpdesk information from those coming from the IT department. You can also set exceptions so that, for instance, messages coming from a sales or IT director may contain information more applicable for their audiences.

Disclaimers can also be directed at known spammers and anyone else on the block list, informing them why their message has been blocked and of the remedial action your organisation has undertaken.

Time saver

Blocking spam at the Exchange server improves productivity for both the organisation and employee as it reduces the time taken to deal with unsolicited emails.

Spammers often send emails to non-existent users, hoping that the message may find its way to someone within an organisation who has a similar name. Recipient validation verifies incoming messages against Active Directory, and any that are identified as false can again be tagged

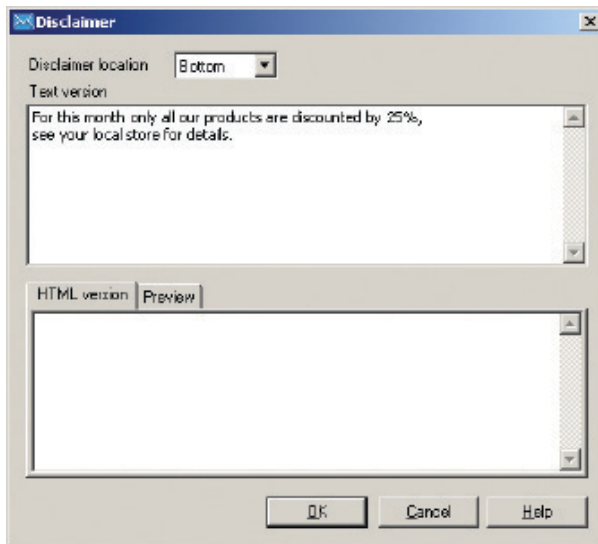


Figure 8: Disclaimer text can be added to outbound messages

with a disclaimer informing the sender that their message was identified as spam and of the consequences. Because this happens at the gateway, spam volumes are automatically reduced, with processing speeds and bandwidth unaffected.

Quarantine management

You can configure the policy so that any message identified as possible spam is placed into PureMessage for Microsoft Exchange's central quarantine, giving the administrator and – optionally – the end user a secure area of the network in which to view the details and decide what to do with it.

You can grant end users access to the quarantine through a web interface and ask them to respond to any immediate concerns about a specific email. They can either confirm that a particular message is spam, or request that it be marked as safe and passed on. From here they can also review and amend their approved sender list and check for any messages that they suspect may have been inadvertently identified as spam.

Access can be provided as a one-off event, or you can establish a regular routine by emailing end users a personalised spam digest that contains a link to the quarantine. Allowing staff to manage their own spam not only ensures that all incoming email is correctly identified, but it will help you keep your IT resources focused on core responsibilities.

Keep it safe

The quarantine is a secure area of your network where you can store and manage all suspect emails.

As can be seen in Figure 9, the quarantine contains a sophisticated search engine which identifies who has sent the email, the intended recipient, the subject line, the reason it is being quarantined and the policy criteria it matched.

From here you can either:

- Release the email to its intended recipient(s)
- Forward the email onto a different email account

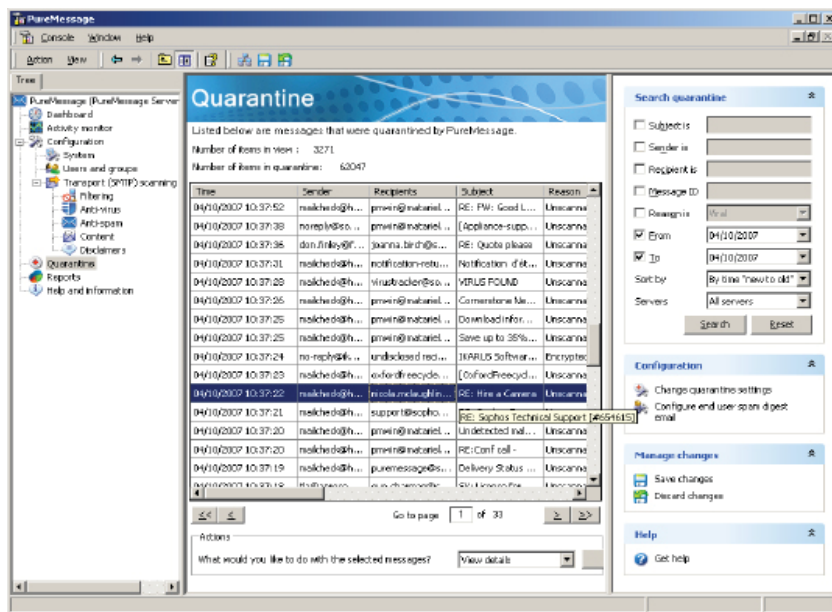


Figure 9: Messages in the quarantine can be sorted quickly and effectively

4: COMPREHENSIVE REPORTING

- Delete the email from the quarantine
- Disinfect the email
- Delete any viral attachment
- Submit the email to Sophos.

Reporting tool

PureMessage for Microsoft Exchange provides you with extensive reporting and logging options that record exactly the information you need to analyse your message traffic and filter options. You can create customised reports that detail all aspects of your email network, such as showing trends in email throughput, policy rule hit rates, disk usage and any issues that require remedial action. This data can then be exported for further analysis or be included in other office programs such as word processing documents and spreadsheets.

Reports can be defined and customised using the advanced filters provided, as shown in Figure 10. These options include:

- General report formats

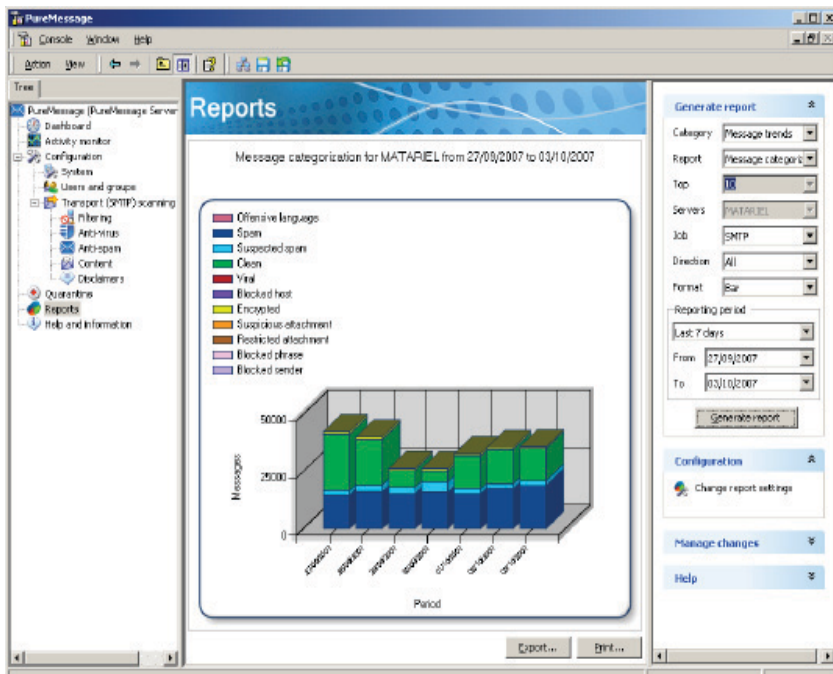


Figure 10: Reports can be customised with the advanced filter

- Output format
- Report period
- Server status
- Email direction.

Graphs

PureMessage for Microsoft Exchange also provides 25 standard report graphs that include:

- **Top 10 Viruses.** Details the names of each virus found in inbound and outbound messages over a specific period
- **Message Trends by Category.** Compares scanned messages against your policies and, for example, could show how many contained offensive language, blocked phrases, encrypted attachments or were clean
- **Top 10 Quarantine Release Report.** Identifies the recipient who

Standard reporting

Extensive reporting options can analyse and present data quickly and efficiently.

APPENDIX I: SOPHOS PRODUCTS FOR THE ENTERPRISE

Sophos Security and Data Protection

Sophos Security and Data Protection™ provides integrated threat management across the entire organisation. In addition to Email Security and Data Protection it includes:

Sophos Endpoint Security and Data Protection

Sophos Endpoint Security and Data Protection™ protects networks from malware and controls unauthorised applications, with centralised management through Sophos Enterprise Console™. A single client detects viruses, spyware, adware, suspicious files, suspicious behavior and controlled applications such as VoIP and games and, in combination with a client firewall, stops zero-day threats and prevents intrusion by hackers.

Sophos Web Security and Control

Sophos Web Security and Control™ is a fully-integrated Web Appliance that protects against the full range of web threats, providing a complete infrastructure for secure browsing and eliminating the complexity of administering effective web security.

Sophos NAC Advanced

Sophos NAC Advanced™ controls access to the network for guest, unmanaged and unauthorised computers, identifying and isolating non-compliant computers based on a centrally defined, policy-driven assessment.

APPENDIX II: OTHER SOPHOS PRODUCTS AND SERVICES

SAV Interface

SAV Interface™ enables software vendors, OEMs, ISPs, and ASPs to integrate Sophos malware detection into their own firewalls, gateways, and similar solutions, and is included in Sophos Email Security and Data Protection and Sophos Web Security and Control licences.

Sophos Small Business Solutions

Sophos small business solutions provide award-winning virus, spyware, and spam protection to enterprises with little or no IT expertise.

Sophos Professional Services

Sophos Professional Services provide businesses with the right skills to implement and maintain complete endpoint and gateway security. We have worked with some of the most recognised organisations in the world, meeting their specific requirements and assuring rapid, optimal deployment of Sophos products. Our expertise is delivered through standard or customised packages, provided on-site or remotely, to ensure the maximum return on your investment.

Sophos Alert Services

Sophos ZombieAlert™ Service provides you with immediate warning if spammers have hijacked any of your organisation's computers to send spam or launch denial-of-service attacks.

Sophos PhishAlert™ Service provides fast, near real-time alerts of phishing campaigns, so that you can take steps to shut down the imitation website and protect your organisation's customers.

For more information on Sophos Alert Services, visit:

www.sophos.com/products/enterprise/alert-services/phishalert.html
www.sophos.com/products/enterprise/alert-services/zombiealert.html

Industry-leading, 24/7 support

Our round-the-clock technical customer support operation is included as standard in your licence and you'll receive unlimited access to our highly-acclaimed customer support team. You can contact our engineers for one-to-one support by email or telephone, or use our web-based support knowledgebase. Working from support centers around the world, our experts draw on a wealth of experience and technology to replicate, analyse, and resolve your problems fast.

Our technical support operates from centres in Australia, Canada, France, Germany, Japan, Italy, Singapore, UK and USA. Whichever centre handles your problem, you can be assured of the highest level of expertise, professionalism and customer service.

For more details, visit www.sophos.com/support

APPENDIX III: SYSTEM REQUIREMENT

The latest release of PureMessage for Microsoft Exchange adds support for Microsoft Exchange 2007 and Windows Server 2003 (64-bit edition), although the product can still be used as a standalone Windows SMTP gateway solution to protect non-Exchange email servers.

It can be installed on all Exchange 2000, 2003 and 2007 servers and can also be used in an edge server role on a vanilla Windows IIS SMTP server. When used in this configuration, it does not require an installation of Exchange to scan email.

Operating Systems	
Version	Level supported
Windows 2000 and earlier (all editions)	Unsupported.
Windows Server 2003 and Windows Server 2003 R2 (including Small Business Edition)	Supported from SP2. R2 required for CCR.
Windows XP	Supported from SP3
Windows Server 2008 (including Essential Business Server and Small Business Server)	Officially supported from SP2. SP1 support added in CC01.
Windows Vista	Officially supported from SP2.
Windows Server 2008 R2 (including Essential Business Server and Small Business Server if available)	Supported from RTM.
Windows 7	Supported from RTM

Microsoft Exchange Server	
Version	Level supported
Exchange 2000 and earlier	Unsupported
Exchange 2003	Supported from SP2.
Exchange 2007	Officially supported from SP2. SP1 support added in CC01.
Exchange 2010	Supported from RTM.

Microsoft SQL Server	
Version	Level supported
SQL 2000/MSDE	Not officially supported
SQL 2005/Express	Unofficial support prior to SP3. SP3 officially supported
SQL 2008/Express	Unofficial support prior to SP1. SP1 officially supported

SOPHOS

SOPHOS INC North America Toll free 1 866 866 2802 Email nasales@sophos.com www.sophos.com
Boston, USA | Oxford, UK

© Copyright 2010. Sophos All rights reserved. All trademarks are the property of their respective owners.

rg/100512

