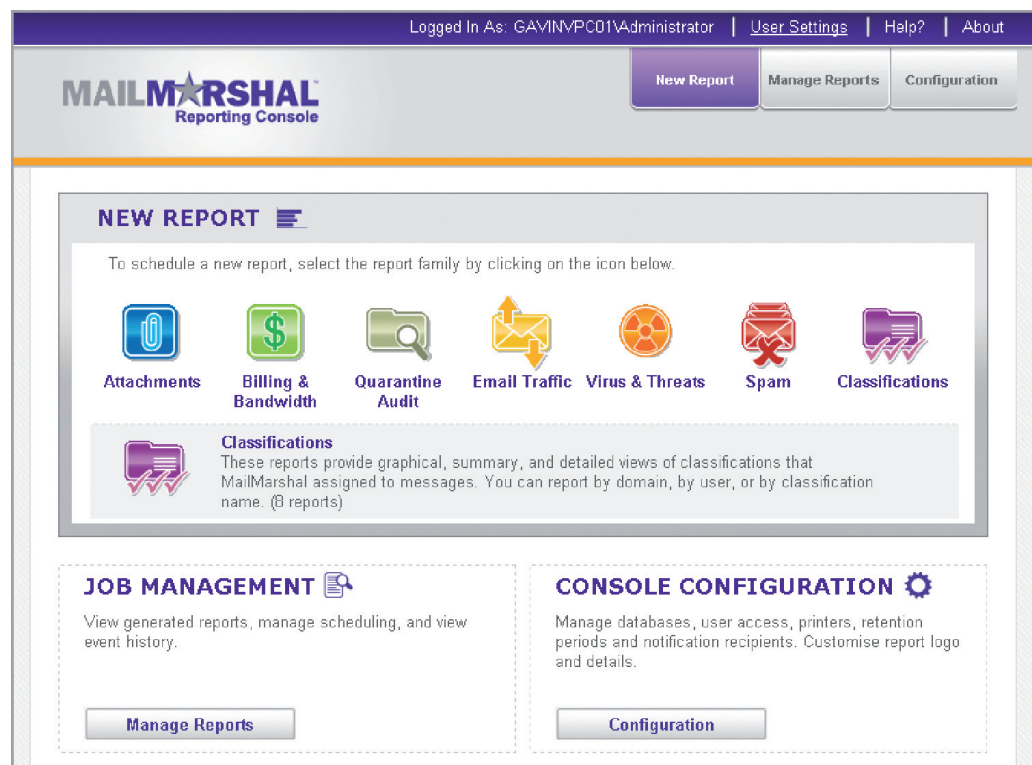


MailMarshal Reporting Console

Comprehensive email security and activity reporting for MailMarshal SMTP

The MailMarshal Reporting Console (MRC) is a web-based reporting suite for MailMarshal SMTP. It offers a comprehensive set of reports covering email gateway activity, content filtering and monitoring of email policy enforcement. MRC provides rich, enterprise reporting facilities such as scheduling, automated email delivery and a range of export formats including Adobe Picture Document Format (PDF) and Microsoft Office Excel.



THE MAILMARSHAL REPORTING CONSOLE (MRC) PROVIDES EASY ACCESS TO 32 REPORTS COVERING A RANGE OF EMAIL TRAFFIC AND SECURITY SUBJECTS, AS WELL AS REPORT SCHEDULES AND CONFIGURATION SETTINGS.

OVERVIEW

An email gateway security solution, MailMarshal SMTP provides protection against threats such as spam and viruses. It enforces email Acceptable Use Policies, ensuring that employee email activity is safe, secure and appropriate. A key aspect of the value MailMarshal SMTP provides is the ability to measure its effectiveness and benefits through reports.

The MailMarshal Reporting Console (MRC) provides detailed information on how MailMarshal SMTP is performing, the behavior of email users and overall email activity across your email gateway. It allows IT administrators to provide evidence of policy breaches and demonstrate MailMarshal's return on investment to managers and executive officers.

MRC enables an administrator to automatically send regular reports to interested stakeholders. It allows you to establish scheduled reports, saved as you want them, generated and delivered automatically at defined times. Completed reports can be emailed to any email address or saved to a local file directory in a range of easily accessible formats.

KEY FEATURES

- Features a clear, easy-to-use Web console interface with remote authenticated access for multiple users
- Presents summary and detail reports covering email traffic, attachments, quarantined messages, viruses and threats, spam, content classification results, bandwidth usage and cost apportioning for billing purposes
- Provides advanced scheduling and automated report generation
- Offers a wide choice of automated report delivery methods to multiple destinations:
 - On screen through the MRC interface
 - Email
 - Network printer
 - FTP
 - UNC
 - Local disk directory

MailMarshal Reporting Console

Comprehensive email security and activity reporting for MailMarshal SMTP

- Supports multiple report formats:
 - On screen – SSRS report viewer (SQL Server Reporting Services)
 - PDF – Adobe Picture Document Format
 - XLS – Microsoft Office Excel
 - MHTML – web archive

KEY BENEFITS

Provides visibility into your email environment

MailMarshal SMTP is designed to provide transparent security and policy enforcement. MRC gives you an insight into how MailMarshal is performing and the activity of email users.

Demonstrates Return on Investment (ROI)

A key component of implementing any security solution is justifying its cost and subsequent payback to executives and managers. MRC provides clear, easy to understand reports for IT administrators and executives, enabling them to appreciate the benefits they have paid for. The amount of spam blocked, viruses quarantined, bandwidth saved and other results that can show a direct cost saving for your organization are presented.

Easy-to-use, convenient, accessible reporting

Visibility into email activity and demonstrating ROI are made easier with a range of delivery options and a web console which can be accessed with a standard web browser. PDF reports delivered directly to any email account or XLS format saved to a network directory for easy access are amongst the many available report delivery options. MRC is a flexible tool that enables you to provide tailored reports to those who need them, when they need them.

Promotes email security and awareness

MailMarshal SMTP provides in-depth protection against external email threats and can be tailored to block other security concerns that arise. MRC provides a means to investigate and address these security concerns. It can generate specific reports for managers as tools to assist them in their roles and decision making. For example, virus incident reports can be emailed to IT managers, Acceptable Use Policy (AUP) violation reports can be sent to HR Managers or department supervisors and cost apportioning reports can be sent to financial controllers.

Saves time and empowers stakeholders

MRC's advanced report schedules, automated generation and delivery options form the basis of many time-saving measures. MRC enables email administrators to provide direct report access to multiple stakeholders, enabling them to access and generate reports at any time. This creates greater transparency and affords greater control to stakeholders. MRC also eliminates annoying, repetitive administrative tasks for generating common reports. These can be scheduled and issued to multiple recipients with multiple delivery methods. Automation of reports provides set-and-forget convenience, saving time and freeing up administrators to get on with other jobs.

Measure and improve Acceptable Use Policies

An Acceptable Use Policy (AUP) is a standard means of informing employees of their IT usage and security obligations. Many organizations understand that these policies are organic and require continual reinforcement and modification to keep pace with evolving trends. MRC is a tool for Human Resource (HR) managers to measure policy effectiveness, identify and deal with rule breaches and amend policies to meet changing workplace conditions.

Enables email administrators to be more efficient and effective

MRC addresses overall email usage in addition to email threats and content security. In this way, it can help IT administrators better understand how their email system is used. It shows an administrator when peak bandwidth usage occurs and which users generate the most email traffic. With this information, MRC provides the basis for administrators to realize email efficiency gains and fine-tune policy to be more effective.

Educates employees and helps enforce Acceptable Use Policies

MRC reports can be provided to employees to help raise security awareness, such as the volume of spam blocked for the organization or incidents of outbound virus-infected messages blocked. Reports can be used to educate employees about their email usage such as emailing large attachments or to show prolific users how much bandwidth they consume.

SAMPLE REPORTS

One of the most important aspects of MRC is that it enables you to answer essentially any question about your email environment. MRC allows you to investigate and solve email related queries that arise or track a desired parameter over time. More than this, MRC often provides you with answers to questions you had never considered before, empowering administrators with greater knowledge and awareness. Provided here are some samples of the reports available in MRC.

MailMarshal Reporting Console

Comprehensive email security and activity reporting for MailMarshal SMTP

REPORT: Email Traffic Summary

Email Traffic Summary by Local User

Database: acmesample
Internal traffic included
Sent messages counted Once
Sorted by Total Bytes
For 01-Jan-2007 to 01-Sep-2008



(GMT+12:00) Auckland, Wellington
Printed: 15-Aug-2008 at 11:55

Local Domain User Name	Sent		Received		Total	
	Msgs	MB	Msgs	MB	Msgs	MB
acmeblueprints.zz	27,828	5,266.54	318,252	8,976.32	346,080	14,242.87
othman	1,391	283.49	27,888	787.03	29,279	1,070.52
alma	2,143	605.16	17,460	329.50	19,603	934.66
sinead	2,705	429.55	5,169	394.44	7,874	823.99
steve	458	583.72	436	46.17	894	629.88
danielle	854	160.33	15,334	374.07	16,188	534.41
anthony	323	27.29	17,540	487.24	17,863	514.53
emma	796	241.82	5,378	267.33	6,174	509.15
coach	990	311.64	1,688	183.80	2,678	495.44
karl	1,078	85.57	13,191	407.85	14,269	493.42
stuart	558	209.96	2,459	222.13	3,017	432.09

The Email Traffic Summary report shows which users are sending and receiving the most messages and utilizing the most bandwidth. In this sample report, the top 10 users by total bytes used are shown. The biggest user is "Othman" with 1,070 megabytes made up from 29,279 messages. For this domain, 92% of email is incoming, indicating a possible high level of spam. Also of interest in this report is the top ten users (out of 150) account for 45% of the organization's email bandwidth.

An unusual result in this report is that the users "Alma" and "Sinead" are sending more than double the number of messages that most other users send, which raises further questions about the nature of the emails they are sending. It is also interesting to note the amount of sent email from the user "Steve". This user has sent a 458 emails, a comparatively low volume, but consumed a relatively high 584 megabytes giving an average sent message size of 1.3 megabytes. This suggests that "Steve" is sending a lot of large attachments and, therefore, may warrant further investigation.

REPORT: Spam Overview

Spam Overview

Database: acmesample



Messages Counted Once
(GMT+12:00) Auckland, Wellington
Printed: 16-Aug-2008 at 13:35

For 01-Jan-2007 to 01-Sep-2008

Anti Spam Summary	Messages	MB	%
Inbound Emails	354,741	9,806.09	
Spam Detected	295,900	3,721.23	83.41%

Spam as a Percentage of Inbound Email

Percentage of Spam Released by Users



18.50% Mail
81.50% Spam



0.70% Released
99.30% Discarded

Return on Investment	Cost per Spam Email	Total Spam Detected	Savings
Estimated Spam Savings	\$0.04	295,900	\$11,836.00

The Spam Overview report shows the total volume of incoming messages compared to the total number of messages classified as spam to give a percentage of incoming spam. In this case it is a very typical 83.41%.

MRC provides the ability to place a cost on each spam message blocked to give a return on investment (ROI) estimate. In this sample, the value is \$0.04 for each spam message. This value is based on Marshal's own research into the costs of spam and factors such as lost employee productivity reading and deleting spam, wasted helpdesk support time, and hardware storage costs. In this case the saving is \$11,836 for 295,900 messages blocked, illustrating a substantial saving.

Questions:

- "How much spam do we block?"
- "What proportion of our incoming email is spam?"
- "How much money have we saved by blocking spam?"

MailMarshal Reporting Console

Comprehensive email security and activity reporting for MailMarshal SMTP

REPORT: Virus Overview

Virus Overview

Database: acmesample			
Messages Counted Once (GMT+12:00) Auckland, Wellington			
For 01-Jan-2007 to 01-Sep-2008			
Printed: 18-Aug-2008 at 15:30			
Anti-Virus Summary			
	Messages	Viruses	%
Total Emails	381,686	3,671	0.96%
Inbound	354,741	3,649	1.03%
Outbound	26,945	22	0.08%
Return on Investment			
Cost per Virus Email			
Estimated Virus Savings	\$50.00	3,671	\$183,550.00

Top 10 Virus Incidents by Virus Name



In the Virus Overview report, a detailed breakdown shows how many virus infected emails were detected and blocked and what percentage were caught coming into or going out of your organization. In the sample shown, 3,671 virus infected emails were blocked out of a total of 381,686 messages scanned. This equates to a virus infection rate of 0.96%. The report also shows 22 outbound virus infected messages were blocked, saving the company from embarrassment and potential liability. In this sample a conservative cost estimate per virus infection of \$50 has been applied. This has provided a cost saving estimate of \$183,550.

Questions:

- “How many virus infected emails do we receive?”
- “How many outgoing virus infected emails have we blocked?”
- “What cost savings are there for blocking viruses?”

REPORT: Attachment Summary

Attachment Summary by Local Domain

Database: acmesample						
Internal traffic excluded						
Sorted by Total Bytes						
For 01-Jan-2007 to 01-Oct-2008						
Messages Counted Once						
Printed: 05-Sep-2008 at 10:01						
Local Domain	Sent		Received		Total	
Attachment Type	Msgs	MB	Msgs	MB	Msgs	MB
User Name						
acmeblueprints.zz	25,433	4,948.53	129,502	41,634.48	154,935	46,583.01
PDF	1,970	1,563.81	4,459	7,197.74	6,429	8,761.55
JPG	7,425	957.17	8,145	6,524.78	15,570	7,481.94
ASF	143	266.24	204	3,705.59	347	3,971.83
DOC	1,134	378.29	2,141	3,449.81	3,275	3,828.09
GIF	1,968	54.55	97,580	3,581.61	99,548	3,636.16
TEXT	7,261	203.33	11,219	2,197.00	18,480	2,400.33
ZIP	147	175.21	342	1,813.84	489	1,989.06

Questions:

- “What kinds of attachments do users typically send?”
- “What types of attachments do we commonly receive?”
- “What types of attachments consume the most bandwidth?”

The Attachment Summary Report looks at messages containing attachments and can be sorted in a variety of ways. The sample provided is sorted by Total Bytes. The result shows that PDF files consume the most bandwidth for both sent and received attachments. The most numerous type of attachment is TEXT followed by JPG images.

Of particular interest in this report is the comparatively high level of bandwidth consumed by ASF attachments (Advanced Streaming Format), a multimedia file type. 204 incoming messages with ASF attachments have consumed 3.7 gigabytes of data. This equates to an average file size of over 18 megabytes which some organizations might consider excessive. Assuming ASF file types are not a common business-related file format for this organization, this result raises serious questions about who has been receiving these attachments and why. These questions can also be answered within this report by “drilling-down” into the ASF detail and viewing which users received these messages.

MailMarshal Reporting Console

Comprehensive email security and activity reporting for MailMarshal SMTP

SYSTEM REQUIREMENTS

MailMarshal - MailMarshal SMTP 6.2 or later

Processor - 3GHz or higher

Disk Space - 10GB (NTFS) or higher

Memory - 2GB or higher

Operating System - Windows Server Standard or Enterprise 2003, SP1 or later OR Windows XP Professional SP2 or later

Network Access - TCP/IP protocol, Domain structure, External DNS name resolution – DNS MX record to allow MailMarshal SMTP Server to receive outbound email

Software

SQL Server 2005 OR SQL Server 2005 Express Advanced Edition

Internet Information Services (IIS) 5.1 or later

.NET Framework 2.0

SQL Server Reporting Services (SSRS)

Supported Browsers - Microsoft Internet Explorer 6 or later, Mozilla Firefox 2.0.0.12 or later

Please note: MailMarshal SMTP does not support 64-bit versions of Windows

TRY BEFORE YOU BUY.

Marshal offers a free 'try before you buy' program for MailMarshal SMTP with MailMarshal Reporting Console. Please visit us on the Web at www.marshal.com and click on the Evaluation Center to download a full function complimentary trial.

CONTACT MARSHAL

Europe, Middle East & Africa

Marshal Limited,
Renaissance 2200,
Basing View,
Basingstoke,
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

Email: emea.sales@marshal.com

Americas

Marshal, Inc.
5909 Peachtree-Dunwoody Rd
Suite 770
Atlanta
GA 30328
USA

Phone: +1 404-564-5800
Fax: +1 404-564-5801

Email: americas.sales@marshal.com

Asia-Pacific

Marshal Software (NZ) Ltd
Suite 1, Level 1, Building C
Millennium Centre
600 Great South Road
Greenlane, Auckland
New Zealand

Phone: +64 9 984 5700
Fax: +64 9 984 5720

Email: apac.sales@marshal.com

info@marshal.com | www.marshal.com

Microsoft®
GOLD CERTIFIED
Partner

Networking Infrastructure Solutions

© 2008 Marshal Limited, all rights reserved. U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the U.S. Government is subject to the terms of the Marshal standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations. Marshal, MailMarshal, the Marshal logo, WebMarshal, Security Reporting Center and Firewall Suite are trademarks or registered trademarks of Marshal Limited or its subsidiaries in the United Kingdom and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.

MARSHAL™
Secure. Protect. Comply.