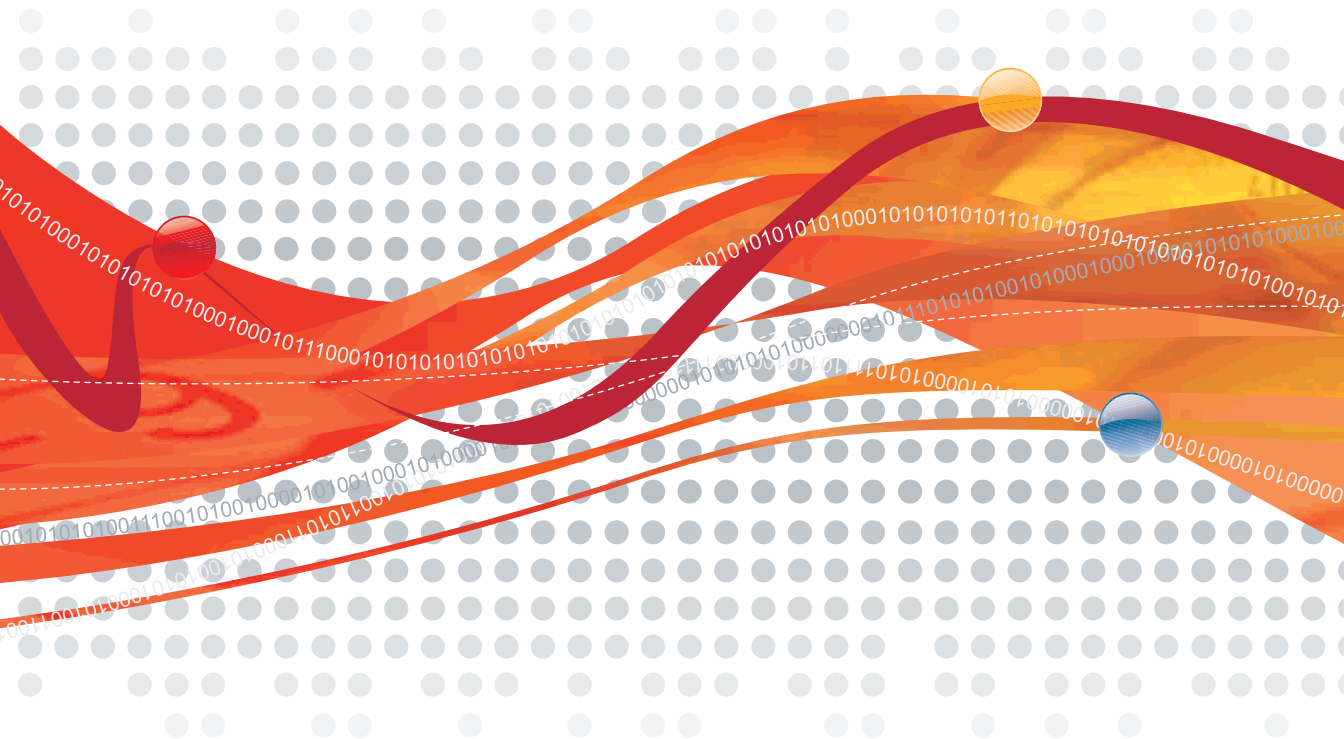




InterScan™ Messaging Hosted Security

Integrated email threat protection in a hosted service

Getting Started Guide



Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before using this service, please review the latest version of the applicable user documentation, which is available from the Help drop-down list at the top of the screen (**Help > Download Manual**).

Trend Micro, the Trend Micro t-ball logo, InterScan, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 1995-2008 Trend Micro Incorporated. All rights reserved.

Document Part No. HSEM03543_80213

Publication Date: September 9, 2008

Protected by U.S. Patent No. 5,623,600; 5,951,698; 5,983,348; 6,272,641

The user documentation for Trend Micro InterScan Messaging Hosted Security is intended to introduce the main features of the service. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Contents

Preface

What's New	vi
InterScan Messaging Hosted Security Documentation	viii
Audience	viii
Document Conventions	ix

Chapter 1: Introducing InterScan Messaging Hosted Security

IMHS Message Flow	1-2
Tiers of Protection	1-3
Email Connection-Level Reputation-Based Filtering	1-3
Email Content-Based Filtering	1-3
Levels of Service	1-4
IMHS Standard	1-4
IMHS Advanced	1-4
Email Encryption Add-On Service	1-4
System Requirements	1-5
Software Required for Accessing Your Account	1-5
Onsite Network	1-6
Default IMHS Settings	1-6

Chapter 2: Using InterScan Messaging Hosted Security

Getting Started	2-2
Registering and Activating InterScan Messaging Hosted Security	2-2
Submitting Account Activation Information	2-2
Obtaining a Registration Key and an Activation Code	2-3
Redirecting Your MX Record	2-3
Configuring Your Mail Transfer Agent	2-4
Activating Email Encryption	2-4

Chapter 2: Using InterScan Messaging Hosted Security—cont.

Logging on to the IMHS Administration Console	2-9
Initial Login	2-9
Special Reseller Login	2-10
Using the IMHS Web Console	2-11
Reports	2-12
Total Traffic	2-14
Accepted Size	2-16
Threats Summary	2-17
Threats Details	2-19
Top Spam Recipients	2-21
Top Virus Recipients	2-22

Chapter 3: Policy, Logs, and Administration

Policy Administration	3-2
Default Policy Settings	3-4
Content Filtering	3-6
Filtering Content with Keywords	3-6
Filtering Content with Regular Expressions	3-8
Rule Actions	3-12
Delete Entire Message	3-13
Deliver the Message Now	3-13
Quarantine the Message	3-14
Clean Cleanable Virus and Delete Those That Cannot Be Cleaned	3-14
Delete Matching Attachments	3-15
Insert a Stamp in the Mail Body	3-15
Tag the Subject Line	3-16
Send a Notification Message	3-16
BCC Another Recipient	3-17
Encrypt Email Message	3-18
Execution Order of Rules	3-23
Intercept Actions	3-23
Modify Actions	3-23
Monitor Actions	3-24
Email Encryption Action (IMHS Advanced Only)	3-24

Chapter 3: Policy, Logs, and Administration—cont.

Adding a New Rule (IMHS Advanced Only)	3-25
Editing an Existing Rule (IMHS Advanced Only)	3-30
Copying an Existing Rule (IMHS Advanced Only)	3-33
Deleting an Existing Rule (IMHS Advanced Only)	3-33
Approved Senders	3-34
Quarantine	3-35
Quarantine Query	3-35
Quarantine Settings	3-36
Approving Messages or Senders From Within the Spam Digest Email (Inline Action)	3-36
Logs	3-45
Mail Tracking Details	3-45
Administration	3-47
Changing Passwords	3-47
Changing the Admin Password	3-48
Resetting an End-User Password	3-48
Managing Directories	3-49
Directory Management Notes	3-50
Verifying Your User Directory	3-52
Co-Branding	3-53
Web Services	3-56
Web End-User Quarantine	3-57
End-User Password Reset	3-57
Disabling InterScan Messaging Hosted Security	3-58
Changing Your MX Record	3-58

Appendix A: Frequently Asked Questions (FAQs)

What is Trend Micro InterScan Messaging Hosted Security?	A1
What are the advantages of a hosted email security service?	A-1
Do I need to buy/upgrade any hardware or software?	A-1
How much does the service cost?	A-1
How confidential is this service? I don't want anyone reading my email.	A-2
Why should I trust Trend Micro with my email?	A-2
What do I need in order to use this service?	A-2

Appendix A: Frequently Asked Questions (FAQs)—cont.

How do I begin using the service? Do I need to install, configure, or maintain anything?	A-2
How do I redirect my email/mail exchange record?	A-2
Can I try the service on a limited number of users?	A-3
Will delivery of my email be delayed as a result of this service?	A-3
Do you store/archive email?	A-3
What happens to my messages if my mail server is unavailable for a period of time? Do you provide any solution towards disaster recovery?	A-3
Where does my outgoing email go?	A-3
Is there an SLA?	A-4

Appendix B: Contact Information and Web-Based Resources

Contacting Technical Support	B-2
Email Support	B-2
Worry Free Business Security with IMHS	B-2
General Contact Information	B-3
Supported Performance Levels	B-3
Service Availability	B-3
Email Delivery	B-3
Knowledge Base	B-4
Sending Suspicious Code to Trend Micro	B-4
TrendLabs	B-6
Security Information Center	B-7

Appendix C: Introducing Web EUQ

Accessing the Web EUQ Service	C-1
Creating an Account	C-2
Logging into IMHS Web EUQ	C-4
Working with Quarantined Spam	C-4
Using the Approved Senders Screen	C-6
Changing Your Password	C-8



Preface

Welcome to the *Trend Micro™ InterScan™ Messaging Hosted Security Getting Started Guide*. This book contains information about product settings and service levels.

This preface discusses the following topics:

- [What's New](#) on page vi
- [InterScan Messaging Hosted Security Documentation](#) on page viii
- [Audience](#) on page viii
- [Document Conventions](#) on page ix

What's New

At time of the publication of this manual, the new features added to Trend Micro InterScan Messaging Hosted Security (IMHS) in 2008 include the following:

- [Inline Action for Spam Digest Email](#)—You can enable users to approve senders and messages from within a spam digest email message, using an HTML form.
- [Email Encryption Service](#)—If you are an IMHS Advanced customer, you can now choose to encrypt outbound email as the single action of a rule. (Email Encryption is purchased separately as an add-on service to IMHS.)
- [New Web Service](#)—You can automate the upload of valid email recipient lists
- [Deliver Now Action](#)—You can create rules by which IMHS will deliver email immediately without further scanning
- [Enhanced Co-branding](#)—You can now place your company logo across the entire top of the IMHS user interface with “Powered By Trend Micro” appearing underneath

Inline Action for Spam Digest Email

From the Quarantine Settings screen, you can enable inline action from spam digest email, that is, the ability for recipients of the spam digest email to approve one or more messages or senders directly from within the spam digest email message itself, using an HTML-based form. By enabling this function, you can relieve users of the necessity of logging on to the End User Quarantine and manually approving quarantined messages or senders.

Email Encryption Service

Trend Micro Email Encryption is a separate add-on service available to IMHS Advanced customers. Email Encryption is seamlessly integrated with the content-filtering capabilities of IMHS. The service does not automatically encrypt email. Once activated, Email Encryption appears as a rule enforcement option within the IMHS administrative console. You will need to configure rules that apply encryption as a rule action. See [Encrypt Email Message](#) on page 3-18 for guidelines on creating rules that apply encryption.

Note: Email Encryption is available only as an add-on service to IMHS, purchased separately. Once activated, Email Encryption appears as a rule action in the IMHS administrative console.

New Web Service

You can now use Web services to automate some repetitive tasks. The first available Web service automates the periodic import of directory files with valid recipient email addresses. This functionality is equivalent to the User Directory Import feature on the IMHS administrative console. (For more on Web services, see [Web Services](#) on page 3-56.)

Two client programs are available, one that is specific for Microsoft Windows Active Directory and one for all other operating systems. You can manage Web services in the Administration section of the Web console. You can download the *IMHS Web Services Guide* and client programs this section.

Deliver Now Action

A “deliver email now” policy action is now available for Advanced customers when creating or editing rules. You can terminate further processing of an email that meets the rule criteria. If a rule is associated with the “deliver now” action and this action is triggered, IMHS immediately delivers the message and executes no additional rules for that message. “Deliver now” is considered a terminal action as defined in [Intercept Actions](#) on page 3-23. The automated rule execution order places a “deliver now” rule after rules with a “delete” action and before rules with a “quarantine” action. (For more information on execution order, see [Execution Order of Rules](#) on page 3-23.)

Enhanced Co-branding

The service now offers enhanced cobranding that provides more prominent placement of the logo of your organization. With this feature you can co-brand the service for your end users. Previously, your logo would be placed on the left side of the interface below the navigation links. The new placement allows for a larger logo to be placed across the top of the interface with a “Powered by Trend Micro” logo below it. You can access this cobranding feature in the Administration section of the Web console. (For more on cobranding, see [Co-Branding](#) on page 3-53.)

InterScan Messaging Hosted Security Documentation

The InterScan Messaging Hosted Security (IMHS) documentation consists of the following:

Online Help—Helps you configure all features through the user interface. You can access the online help by opening the Web console and then clicking the help icon (🔗).

Getting Started Guide—Helps you plan for deployment and configure all product settings.

The Getting Started Guide is available at:

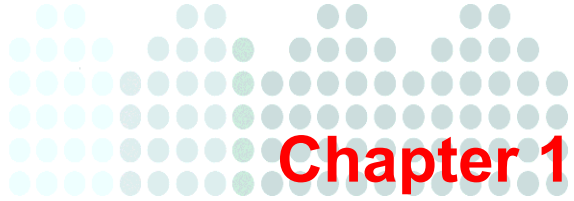
<http://www.trendmicro.com/download>

Audience

The IMHS documentation is written for IT managers and email administrators. The documentation assumes that the reader has in-depth knowledge of email messaging networks, including details related to the following:

- SMTP protocol
- Message Transfer Agents (MTAs)

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.



Introducing InterScan Messaging Hosted Security

Trend Micro™ InterScan Messaging Hosted Security (IMHS) delivers high-performance, cost-effective hosted security services, protecting businesses against spam, viruses, and inappropriate content before they reach your network.

Topics in this chapter:

- [IMHS Message Flow](#) on page 1-2
- [Levels of Service](#) on page 1-4
- [System Requirements](#) on page 1-5
- [Default IMHS Settings](#) on page 1-6

IMHS Message Flow

Figure 1-1 shows the flow of messaging traffic from the Internet, through the IMHS servers, and then to your messaging server.

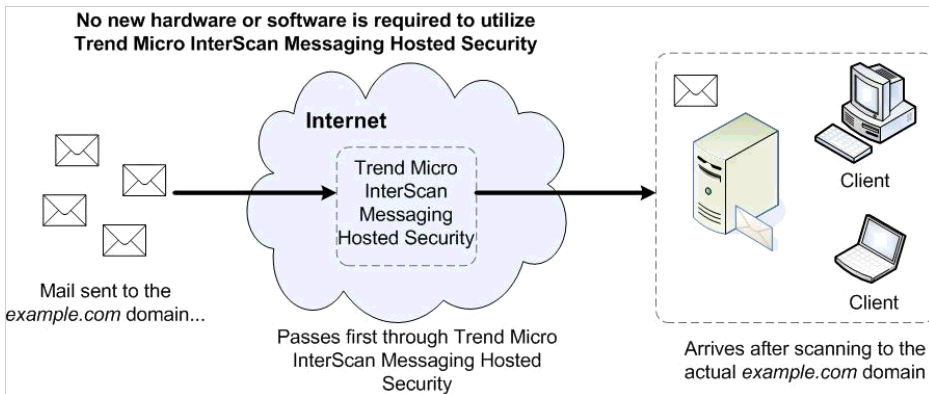


FIGURE 1-1 IMHS workflow diagram

The processes IMHS performs are explained further in the following list:

1. The originating mail server performs a DNS lookup to determine the location of the *example.com* domain. The Mail eXchange (MX) record for *example.com* holds the IP address of IMHS instead of the original IP address for *example.com*, since IMHS must first scan your company's mail before final delivery to your local email server.
2. The originating mail server routes the mail to IMHS.
3. IMHS servers accept the message and perform message filtering and policy matching on your behalf.
4. Assuming a message is slated for delivery according to its security policy or validity status, the IMHS servers route the message to the original *example.com* mail servers.

Tiers of Protection

IMHS offers two tiers of protection. They include:

- Email connection-level reputation-based filtering
- Email content-based filtering

Email Connection-Level Reputation-Based Filtering

When an upstream mail server attempts to connect to IMHS servers, the IMHS server queries the Trend Micro Email Reputation server to determine whether the IP address of the connecting sender is “trustworthy.” IMHS performs this first tier of filtering prior to receiving the actual message, therefore the content of the message is never scanned.

If the sending IP address is a known source of spam, the IP address of the sending server will be marked “untrustworthy.” IMHS will permanently reject the connection attempt from this IP address.

If the sender’s PC is part of a botnet or a zombie PC, the IP address will be in the ERS dynamic database that identifies spam sources as they emerge and for as long as they are active. IMHS will inform the sending server that IMHS is temporarily unavailable. If the sending server is legitimate, it will try later.

Email Content-Based Filtering

After the message passes through the first tier of protection, IMHS applies content filtering through two scanning engines:

- Spam and phishing
- Malware (viruses, spyware, and so on)

Multiple technologies are integrated in these scanning engines, including:

- Pattern files (or spam signatures)
- Heuristic rules
- Machine learning (or statistical filtering)
- URL reputation

IMHS examines the message contents to determine whether the message contains malware such as a virus, or if it is spam, and so on, according to the content-based policies for this message.

Levels of Service

IMHS is available in two basic levels of service, Standard and Advanced, shown in [Table 1-1 on page 1-5](#).

IMHS Standard

The Standard level of service provides several default settings to provide immediate protection upon deployment. For the Standard version, only the spam action can be changed, minimizing the administration needed.

For a comparison of features available at the Standard and Advanced levels, see [Table 1-1](#).

IMHS Advanced

The Advanced version provides robust management options, enabling you to customize your threat protection and set email use policies to meet the needs of your organization. The features unique to the Advanced service include the following:

- Customized threat filtering
- Outbound email filtering
- Content filtering capabilities
- Email Encryption (a separate, add-on service available for purchase)

Email Encryption Add-On Service

Trend Micro Email Encryption for outbound mail is an add-on service to IMHS Advanced that is available for purchase. Email Encryption is seamlessly integrated with the content-filtering capabilities of IMHS. The service does not automatically encrypt email. Once activated, Email Encryption appears as a rule enforcement option within the IMHS administrative console. You will need to configure rules that apply encryption as a rule action. See [Encrypt Email Message](#) on page 3-18 for guidelines on creating rules that apply encryption.

In order to use this service, you must first deploy IMHS Advanced with outbound filtering and then activate the Email Encryption service separately. See [Activating Email Encryption](#) on page 2-4 for more information.

TABLE 1-1 IMHS levels of service

STANDARD	ADVANCED
<ul style="list-style-type: none"> • Provides multitiered anti-spam, antivirus, and anti-phishing protection for inbound email traffic with streamlined management for complete security requiring minimal administration. • The simplified management console has preset protection defaults and is updated and tuned by Trend Micro. • The administrator can quickly create lists of approved senders designated by email address or domain. • Web-based End-User Quarantine is also available for easy management. 	<ul style="list-style-type: none"> • All features available in Standard level. • Provides in-depth content filtering and policy management for more granular access and control. Optionally, can provide outbound message scanning as well. • Email messages and attachments can be filtered based on keywords, lexicons, and attachment characteristics, as well as more customized filtering rules. • Administrators can create rules by company, group, or individual and can set the appropriate enforcement action for each policy.

System Requirements

IMHS does not require additional hardware (other than your mail gateway) located on your premises. All scanning hardware is located off-site at Trend Micro's secure network operating centers. To access your web-based IMHS administration account, a personal computer with access to the Internet is required.

Software Required for Accessing Your Account

Use of the IMHS Web console requires Java Script™ and Sun™ Java™ Runtime Environment (JRE) 1.4. IMHS supports the following browsers for the Web console:

- Microsoft™ Internet Explorer 6.0 and 7.0
- Mozilla™ FireFox™ 2.0

Onsite Network

The following are required before IMHS can be activated:

- An existing Internet gateway or workgroup SMTP connection
- Access to the DNS mail exchange record required to redirect the MX mail host record. (Contact your service provider, if necessary, for more information or configuration help.)

Note: Do not redirect your MX record until you receive confirmation that your account has been established. If you redirect your MX record before your account is set up, your email may be lost. Redirection details will be provided by Trend Micro.

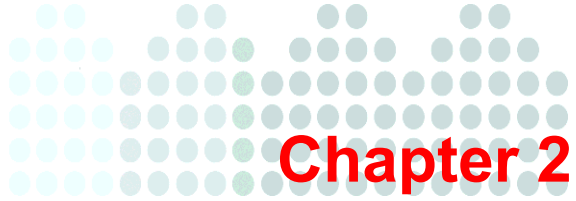
Default IMHS Settings

To ensure high-quality continuous service and to protect your network from common SMTP attacks such as mail floods and Zip of Death, service system limitations by default include the following:

- Message size limits: 50 MB per message (default is 10 MB for new accounts)

Note: Depending on the required service level, the message size limit may be extended up to the system-level protection default.

- Total embedded layers within a compressed file: 20 layers
- Total decompressed message size: 30 MB
- Total files in a compressed archive: 250 files
- Total of quarantine storage per seat: 50 MB
- Total approved senders entries per seat: 50



Using InterScan Messaging Hosted Security

This chapter discusses using InterScan Messaging Hosted Security in the following topics:

- [Getting Started](#) on page 2-2
- [Using the IMHS Web Console](#) on page 2-11
- [Reports](#) on page 2-12

Getting Started

IMHS must be configured to work properly and effectively. This configuration process includes:

- Submitting account activation information
- Redirecting the Mail eXchange (MX) record for your domain
- Configuring your Mail Transfer Agent (MTA) if applicable
- Logging on to the Trend Micro InterScan Messaging Hosted Security console
- Confirming your messaging security policy

Registering and Activating InterScan Messaging Hosted Security

You need an IMHS Activation Code (AC) or Registration Key (RK) for activation. If you do not have the AC or RK, contact your Trend Micro sales representative or download an AC or RK from the Trend Micro web site. Until you input a valid Activation Code, you will be unable to use IMHS.

Trend Micro recommends that you register your product before using the service. You can register online at:

<https://olr.trendmicro.com/registration/us/en-us/login.aspx>

The Email Encryption service is an add-on component to IMHS and so must be purchased and activated separately. For information on activating Email Encryption, see [Activating Email Encryption](#) on page 2-4.

Submitting Account Activation Information

Before using IMHS, you must first activate the account.

To activate the IMHS account:

1. Locate your confirmation of purchase and a registration key in the email message received from Trend Micro.
2. Visit the Product Registration site (URL provided in email message) to complete the registration process.

Trend Micro will set up your account and send you a confirmation email. (Allow one business day.) This email will contain information on where to direct your MX

record, as well as your user name and temporary password to access the IMHS Security console.

Note: Do not redirect your MX record until you receive confirmation that your account has been established. If you redirect your MX record before your account is set up, your email may be lost.

Obtaining a Registration Key and an Activation Code

Registration Key

A product RK is required to complete the product registration process. This uses 22 characters, including hyphens, in the following format:

XX-XXXX-XXXX-XXXX-XXXX

InterScan Messaging Hosted Security (IMHS) must be registered, using your product RK, before you receive an AC that allows you to begin using IMHS.

Activation Code

An AC is required, and the management console will display the status of your license. An AC uses 37 characters, including hyphens, in the following format:

XX-XXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

After you have completed the product registration process, you will receive your Activation Code from Trend Micro.

Redirecting Your MX Record

The Mail eXchange (MX) record determines the message routing for all email sent to your domain. To route messages destined for your domain through the IMHS servers, you must redirect your MX record. Your MX record is part of your DNS record. In the confirmation email that you receive ([Step 2](#) above), you also will be given information on where to redirect your MX record.

The actual redirection of the MX record involves simply changing the IP address for all inbound SMTP traffic. This is typically accomplished manually (for self-managed smaller accounts) or through a support technician.

If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider's (ISP) help desk or your Domain Name Service (DNS) technician for assistance.

Note: The full transition (DNS propagation) may take up to 48 hours. During this time, we recommend that you do NOT discontinue any on-premise security. You may receive some email directly for a limited time until the transition period is completed.

Configuring Your Mail Transfer Agent

For all IMHS customers, the default setting for “spam or phish” messages is to delete all such messages. Advanced service customers may modify this rule. (See [Editing an Existing Rule \(IMHS Advanced Only\)](#) on page 3-30.)

Note: Standard service user can modify the action portion of the spam-related rules. They can determine how the spam will be handled: tag the subject as spam, delete, or quarantine the message. See [figure 3-2](#) on page 3-4 for more information.

You can configure your MTA to handle spam in a way that corresponds to your company security policy. Tagged messages can be forwarded to a spam folder, deleted, passed to the end user, and so on. If you choose to tag such messages, the subject line of spam messages will be tagged with **Spam/Phish>** followed by the original subject line.

Note: It is beyond the scope of this document to provide detailed MTA configuration instructions. Please contact your email administrator if you need assistance.

Activating Email Encryption

Trend Micro Email Encryption is available only as an add-on service for IMHS Advanced with outbound filtering. Outbound filtering is available at no extra cost to IMHS Advanced customers. For more information on enabling outbound filtering, or

to request outbound filtering service, contact imhs_support@trendmicro.com. The activation process for Email Encryption depends on the status of your IMHS license, as shown in [Table 2-1](#) below.

TABLE 2-1 Options for activating the Email Encryption service

IMHS ADVANCED LICENSE STATUS	EMAIL ENCRYPTION LICENSE OPTIONS
PURCHASED	You can try or purchase Email Encryption. <ul style="list-style-type: none"> • See Starting a Free Trial of Email Encryption on page 2-5 • See Purchasing Email Encryption on page 2-7
IN TRIAL PERIOD	You can only conduct a free trial of Email Encryption. See Starting a Free Trial of Email Encryption on page 2-5.

Starting a Free Trial of Email Encryption

If you have purchased or are conducting a trial of IMHS Advanced with outbound filtering, you can start a free trial of Email Encryption from within the IMHS console. You can request a free trial of Email Encryption either on the IMHS product page of the Trend Micro Web site or from within your IMHS Advanced administrative console.

Note: Email Encryption is available only to IMHS Advanced customers who have enabled outbound filtering. When filling out the IMHS trial form on the Trend Micro Web site, be sure to:

1. Select **IMHS Advanced** option in the drop-down list.
2. Select **Yes** when asked if you want to enable outbound scanning.

In order to conduct a trial of Email Encryption or purchase it, you must have IMHS Advanced with outbound filtering enabled.

To verify that you have IMHS Advanced:

1. Log in to IMHS. The Report screen loads.
2. Observe the title of the screen, as shown in [figure 2-1](#) below. If your account is IMHS Advanced, the screen title is “Report - Advanced.” If your account is IMHS Standard, the screen title is “Report - Standard.”

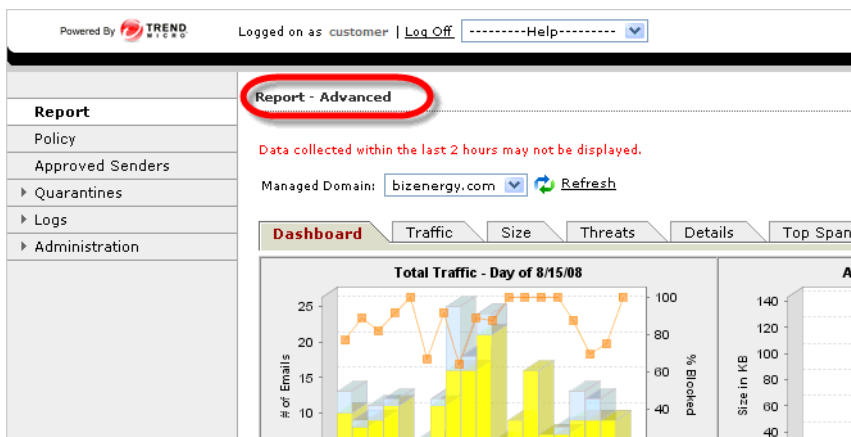


FIGURE 2-1 Initial screen upon login for IMHS Advanced

Note: If you have IMHS Standard and want the Email Encryption service, contact Trend Micro to upgrade to IMHS - Advanced.

Outbound filtering is a feature that requires interaction with Trend Micro staff in order to set up. If outbound filtering has been set up for your account, your organization will have received email confirmation from Trend Micro stating that this feature has been enabled and identifying which server to point to for the relay access.

Tip: When outbound filtering is set up, four new default rules are added to your policy list, all with rule names starting with “Outbound.” If these rules are in your list, then your account has outbound filtering.

To request a free trial of the Email Encryption service from the IMHS console:

1. Verify that you have IMHS Advanced and that outbound filtering is enabled, as explained above.
2. On the IMHS left menu, click **Administration > Licenses**. The Licenses (Activate an Account) screen appears. (See [figure 2-2](#) below.)
3. Select **Trial Activation** and click **Submit**.

Note: It may take 24-48 hours for Trend Micro to verify your Email Encryption trial request and initiate this service for your account. Upon activation, Email Encryption appears as a rule action available when adding or editing a rule from the IMHS Policy screen.

Purchasing Email Encryption

To purchase Email Encryption, you must have purchased IMHS Advanced with outbound filtering. You can conduct a free trial of Email Encryption while in the trial period for IMHS Advanced, but you cannot purchase Email Encryption until you have purchased IMHS Advanced and have enabled outbound filtering.

Note: In some regions, you must obtain a Registration Key (RK) before getting an Activation Code (AC). If you have an RK but do not yet have an AC, register online at the Trend Micro Online Registration site to request your AC:
<https://olr.trendmicro.com/registration>

Licenses (Activate an Account) 

If you have a **Registration Key**, [register online](#) to get an Activation Code.

Activation Type:

Trial Activation
Service Name 
(An Activation Code is not required to activate a trial)

Purchase Activation
Service Name 
Activation Code
(Insert Activation Code provided by email to activate this service)

FIGURE 2-2 The Licenses (Activate an Account) screen

To activate the Email Encryption service:

1. On the IMHS left menu, click **Administration > Licenses**. The Licenses (Activate an Account) screen appears, as shown in [figure 2-2](#) above.
2. Select **Purchase Activation** and type your Email Encryption activation code in the **Activation code** text box.
3. Click **Submit**.

Note: If you have already activated a trial of the Email Encryption service, the Trial Activation option will appear disabled, as shown in [figure 2-2](#).

Logging on to the IMHS Administration Console

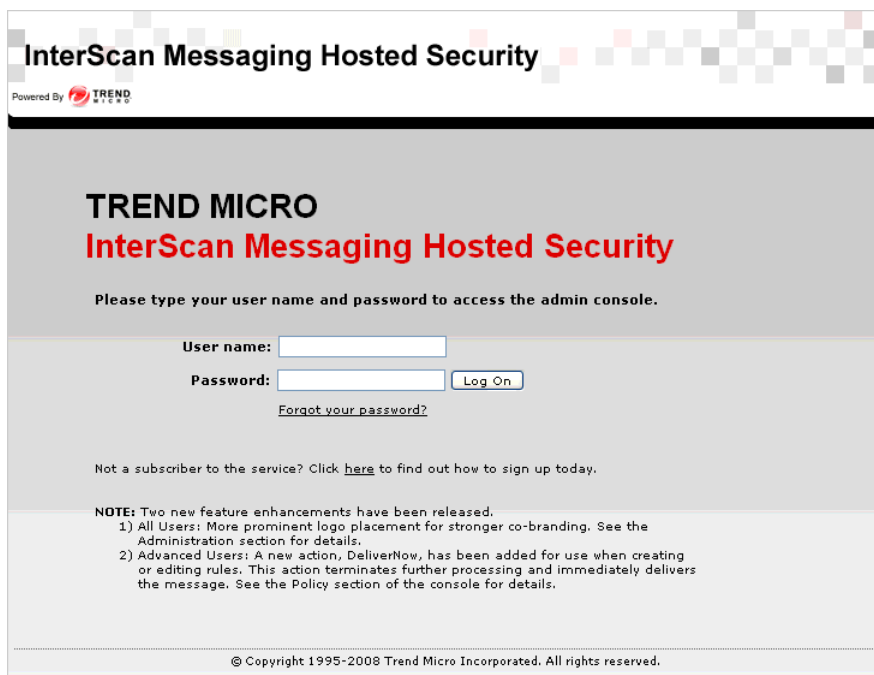
You can view reports and use the mail tracking tool to locate messages by logging on to the IMHS Web console. As an IMHS Advanced user, you can also make changes to your messaging security policy.

Initial Login


The Welcome Packet that you received after signing up for IMHS contains a user name and password for you to use during your initial logon.

To log on to the console:

1. Point your browser to the URL provided in the confirmation email that you received (See [Step 2](#) on page 2-2) to access the logon page.



InterScan Messaging Hosted Security

Powered By 

TREND MICRO
InterScan Messaging Hosted Security

Please type your user name and password to access the admin console.

User name:

Password:

[Forgot your password?](#)

Not a subscriber to the service? Click [here](#) to find out how to sign up today.

NOTE: Two new feature enhancements have been released.

- 1) All Users: More prominent logo placement for stronger co-branding. See the Administration section for details.
- 2) Advanced Users: A new action, DeliverNow, has been added for use when creating or editing rules. This action terminates further processing and immediately delivers the message. See the Policy section of the console for details.

© Copyright 1995-2008 Trend Micro Incorporated. All rights reserved.

FIGURE 2-3 Login screen

2. Type your **User name** and **Password**.
3. Click **Log On**.

Tip: To help ensure the security of your IMHS account, Trend Micro recommends changing your password after you have logged on for the first time. (See [Administration](#) on page 3-47.)

Special Reseller Login

If you are a reseller, you can log in as one of your customers. For resellers, upon login a customized view appears. Your login name appears along with “on behalf of” and a drop-down menu in the top banner area. The drop-down menu contains all of the domains that you as a reseller manage, as shown in [figure 2-4](#).

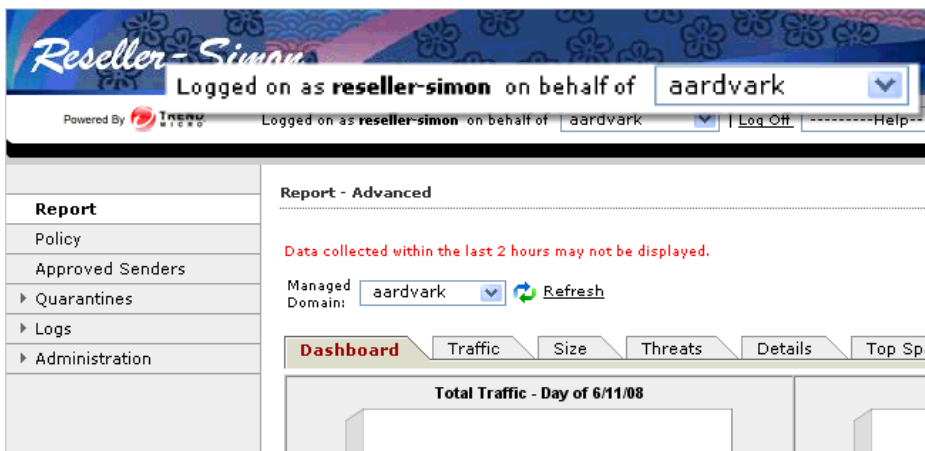


FIGURE 2-4 Reseller login, (enlarged for readability)

Note: The customer domains that you as a reseller manage are listed in alphabetical order in the drop-down menu. The first customer domain at the top of the list is the one shown in the reports screen by default.

Select the domain to manage from the drop-down menu, and the screen reloads showing reports drawn from the data for that domain only. The top banner maintains this special reseller login function on all IMHS screens.

Using the IMHS Web Console

The IMHS Web console allows mail administrators to create reports, view logs, perform administrative tasks, and set or alter policies (Advanced customers only).

A summary of user-level capabilities includes:

- **Standard service:**
 - Antivirus and IP connection spam prevention
 - Heuristic, content-based spam prevention filter
 - Standard anti-virus policies cannot be changed (read-only)
 - Access to reports, mail tracking, and password administration
 - End-user quarantine with configurable quarantine digest notification email
- **Advanced service:**
 - All of the **Standard service**, plus:
 - Outbound message filter
 - Content filtering for corporate compliance
 - Ability for administrator to create custom policies (create and modify rights)

All features are presented in this section for completeness.

See the online help files for detailed information about working with the IMHS Web console. You can access the complete product help by clicking “Contents and Index” from the Help drop-down menu, or you can access help for a particular screen by clicking the blue question mark (?) near the upper right corner of each screen.

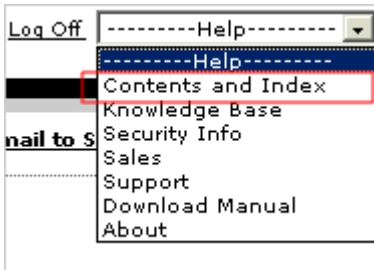


FIGURE 2-5 Drop-down help menu

Reports

The Dashboard page ([figure 2-6](#)) displays when you log on to IMHS. [Table 2-2](#) on page 2-14 describes the Dashboard graphs.

For specifics concerning IMHS actions, click the appropriate tab or double-click the image in the Dashboard page.

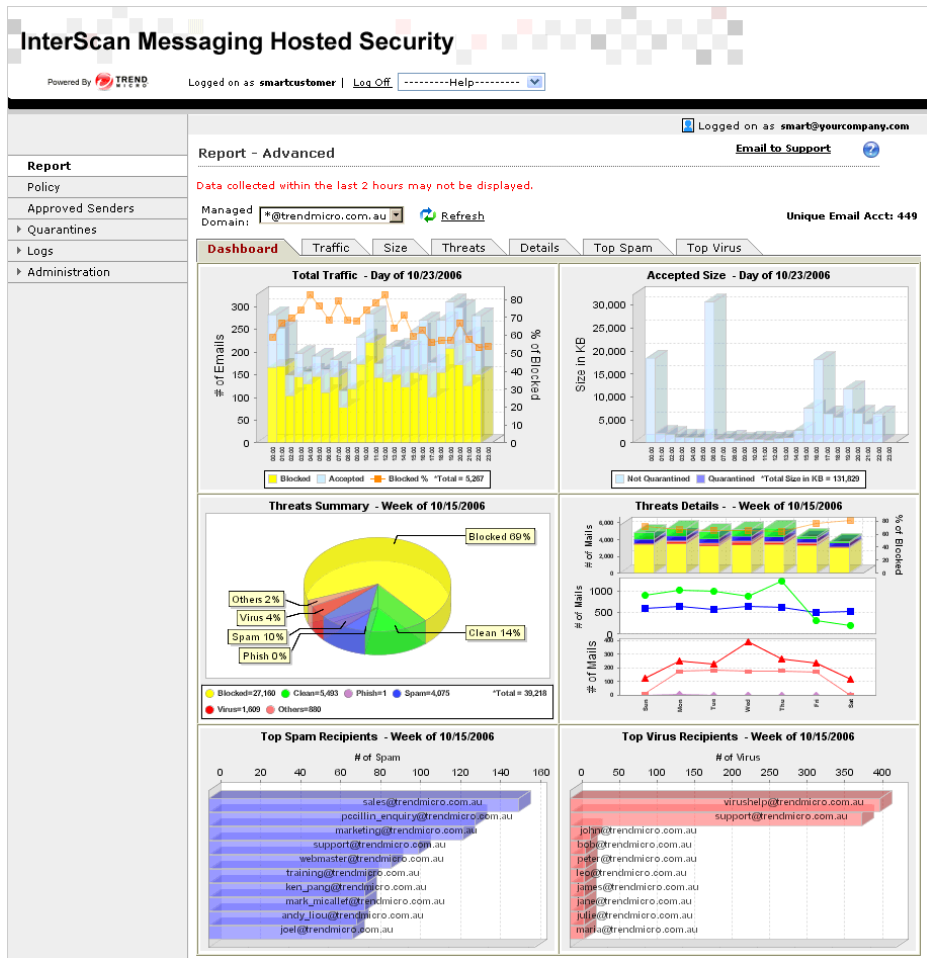


FIGURE 2-6 Summary report page

Table 2-2 on page 2-14 describes the Dashboard tab screen graphics.

TABLE 2-2 Dashboard screen graphics

GRAPHIC	TAB NAME	DESCRIPTION
Total Traffic	Traffic	Shows the total blocked and accepted email traffic for the selected domain
Accepted Size	Size	Shows the total size (in KB) of accepted email traffic for the selected domain
Threats Summary	Threats	Shows what percentage of specific types of messages make up the email traffic for the selected mail domain
Threats Details	Details	Shows detailed email traffic distribution for the selected mail domain
Top Spam Recipients	Top Spam	Shows the top spam messages recipients for the selected mail domain
Top Virus Recipients	Top Virus	Shows the top virus messages recipients for the selected mail domain

Total Traffic

The Total Traffic screen ([Figure 2-7](#)) displays the total blocked and accepted email traffic for the selected domain at each interval and the traffic trend for the selected period. The legend indicates the number of blocked email messages; email messages accepted for further processing, the percentage of blocked traffic, and the total number for all email messages for the selected domain. To enhance visibility, the blocked % has its own scale on the right side of the graph.

- **Blocked** — the number of “bad” message attempts to send to the selected domain. This “bad” message traffic are connections blocked by Trend Micro Email Reputation Services (ERS) filter.
- **Accepted** — the number of messages that were passed by the ERS filter and were accepted for further processing by Trend Micro InterScan Messaging Hosted Security (IMHS).

- **Blocked %** — the percentage of message traffic blocked by ERS for the selected mail domain.
- **Total** —the total number of messages processed by Trend IMHS for the selected mail domain. This is the sum of blocked and accepted traffic.

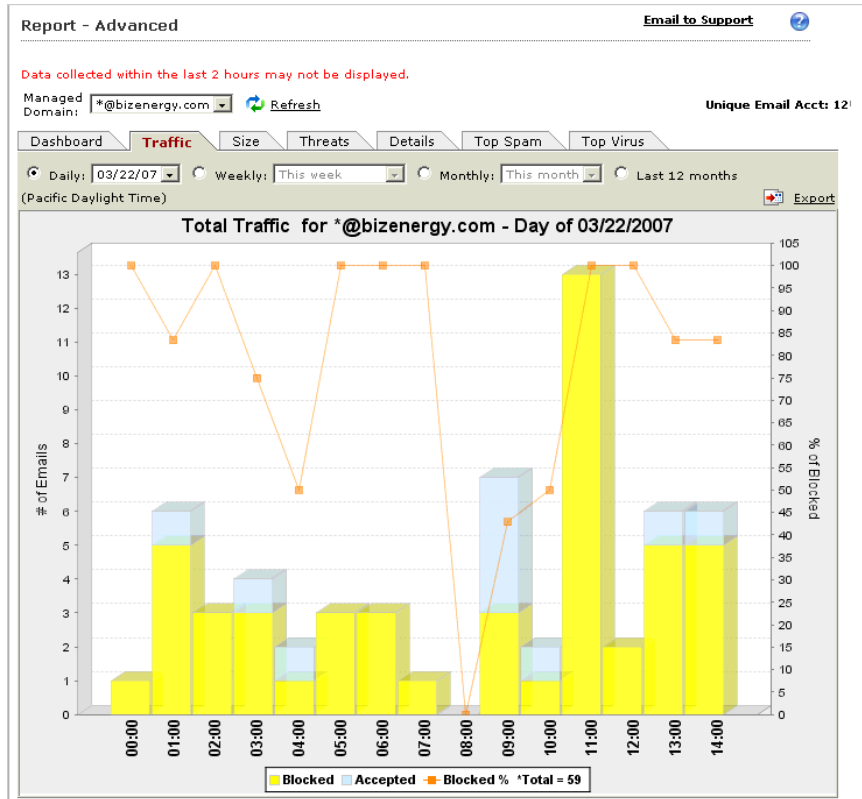


FIGURE 2-7 Total Traffic report page

Accepted Size

This Accepted Size report (Figure 2-8) shows the total size (in KB) of accepted email traffic for the selected domain. The default reporting period is today. The legend indicates the total size of non-quarantined messages, quarantined messages, and total size of accepted messages.

Not Quarantined — the size of accepted messages, which were not quarantined, for the selected mail domain.

Quarantined — the size of “quarantined” messages for the selected mail domain. If quarantine is not configured in policies for this mail domain, there will be no quarantined mail in this graph.

Total Size — the total size of accepted messages for the selected mail domain. This is the sum of non-quarantined and quarantined messages.

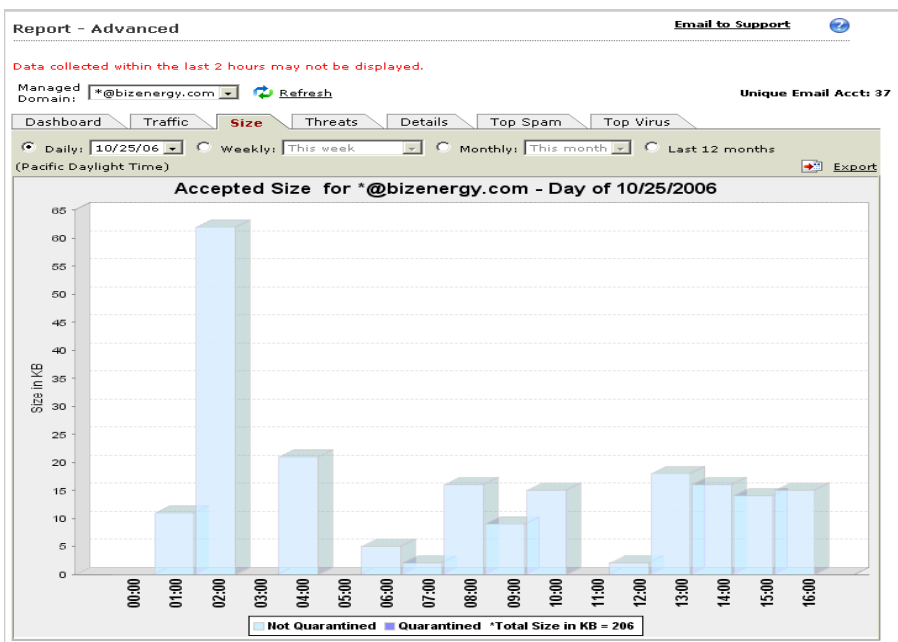


FIGURE 2-8 Accepted Size report page

Threats Summary

This Threats Summary report (Figure 2-9) shows percentage of what kind of messages made up the email traffic for the selected mail domain. The default reporting period is the current week. The pie chart graph shows the percentage make-up of different kinds of messages for the selected domain.

The legend indicates the number of blocked traffic, clean messages, phishing email messages, spam, viruses, as well as the total number of messages for the selected mail domain.

- **Blocked** — the number of email connections for the selected mail domain blocked by Trend Micro ERS service.
- **Clean** — the number of email messages for the selected mail domain that were deemed “clean” by IMHS.
- **Phish** — the number of email messages for the selected mail domain that were identified as phishing messages by IMHS.
- **Spam** — the number of email messages for the selected mail domain that were identified as spam by IMHS heuristic spam prevention engine.
- **Virus** — the number of email messages for the selected mail domain that were identified as carrying a virus by IMHS.
- **Others** — the number of email messages for the selected mail domain that were filtered by other IMHS content filters (such as the attachment size filter).
- **Total** — the total number of email messages for the selected mail domain. This is the sum of all 6 categories.

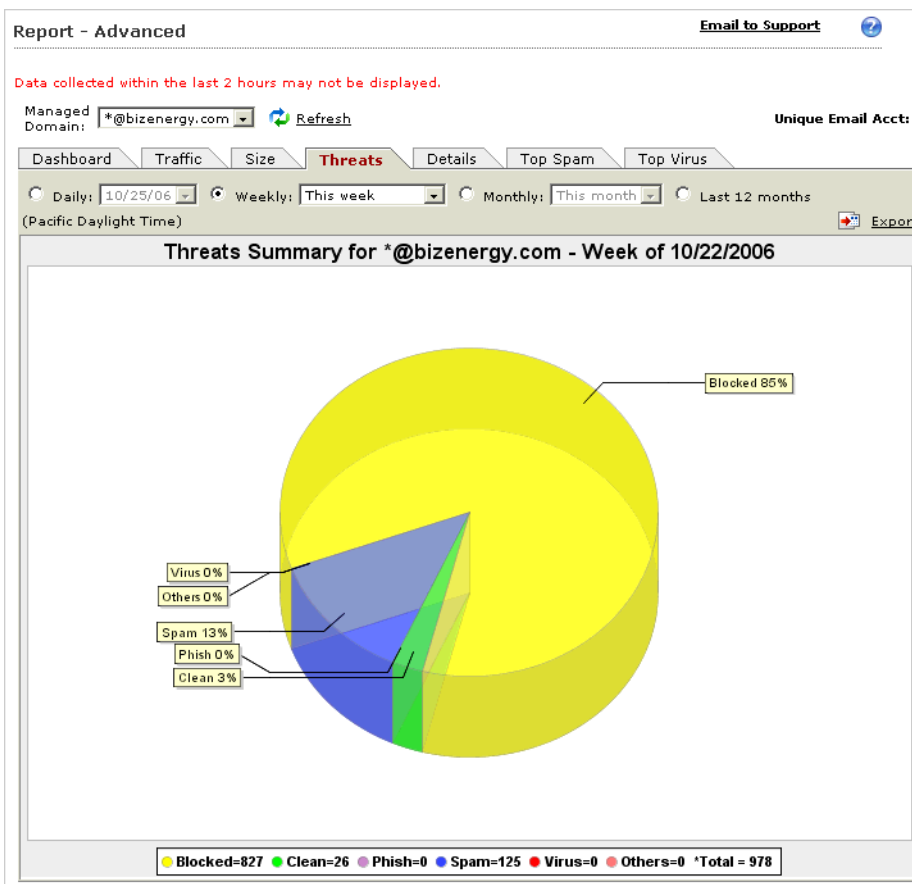


FIGURE 2-9 Threats Summary report page

Threats Details

This Threats Details report (Figure 2-10) shows detailed email traffic distribution for the selected mail domain. The default reporting period is the current week. This report employs the same coloring scheme as the other reports. To avoid cluttering the dashboard display, the legend for this report will be presented in the enlarged report only. There are three detailed graphs and a Totals table:

- **Graph 1** — Number of messages and percentage of blocked traffic.
The graph is similar to the Total Traffic report described above. It further breaks down the accepted messages into various categories such as virus, phish, spam, clean, and others.
 - The vertical axis on the left corresponds to the vertical bars, which indicate the total number of messages for the selected mail domain. Each vertical bar is made up of numbers of blocked, clean, phish, spam, virus, and other messages.
 - The vertical axis on the right corresponds to the line graph, which represents the percentage of all traffic blocked by Trend Micro Email Reputation Service (ERS) at each interval.
- **Graph 2** — Number of each kind of email-Spam and clean
 - Each line represents the number of a kind of email at each interval.
- **Graph 3** — Number of each kind of email threats-Virus, phish, and others
 - Each line represents the number of a kind of email threat at each interval.
- **Totals Table** — Provides a weekly compilation of total for:
 - Percent of blocked messages
 - Number of blocked messages
 - Number of viruses
 - Number of phish
 - Number of spam
 - Number of messages cleaned
 - Others
 - Daily total

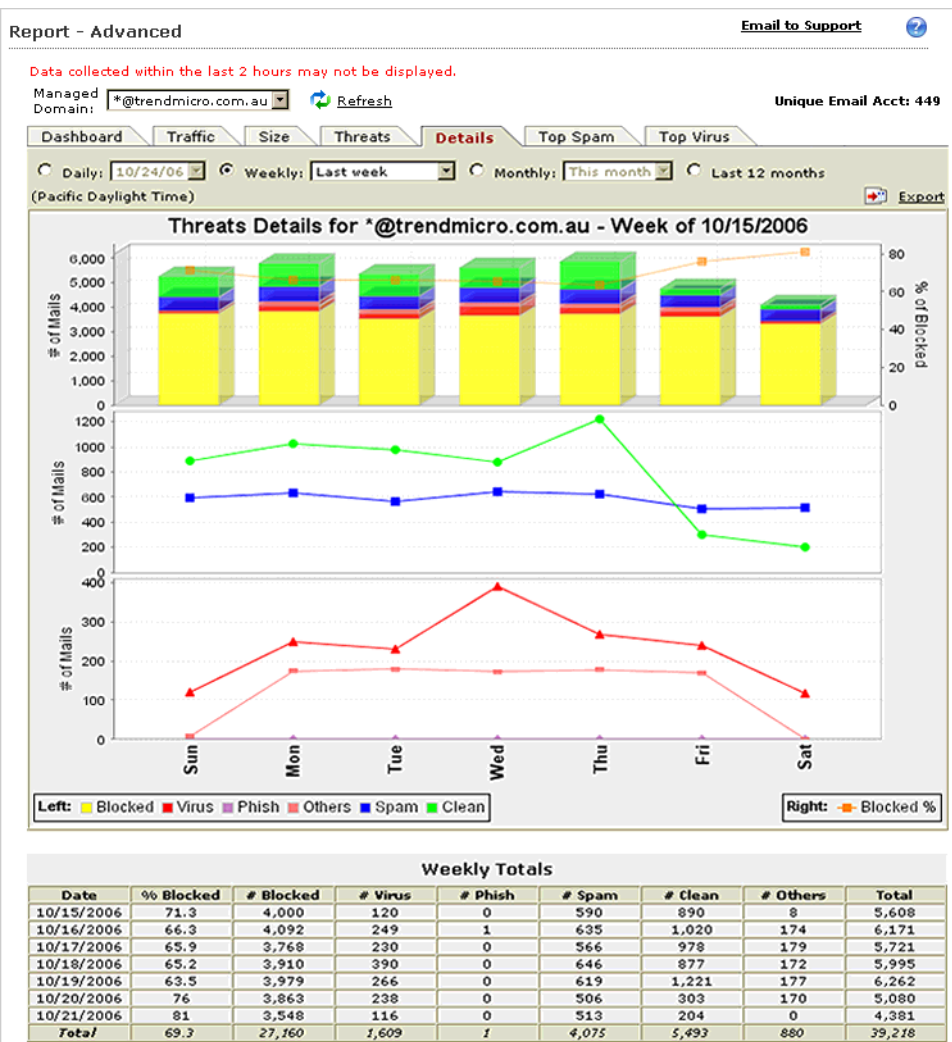


FIGURE 2-10 Threats Details report page

Top Spam Recipients

This Top Spam Recipients (Figure 2-11) report shows the top spam recipients for the selected mail domain. The default reporting period is the *current week*. Top spam recipient reports are displayed in GMT time.

Report - Advanced

[Email to Support](#)



Data collected within the last 2 hours may not be displayed.

Managed Domain: [Refresh](#)

Unique Email Acct: 12

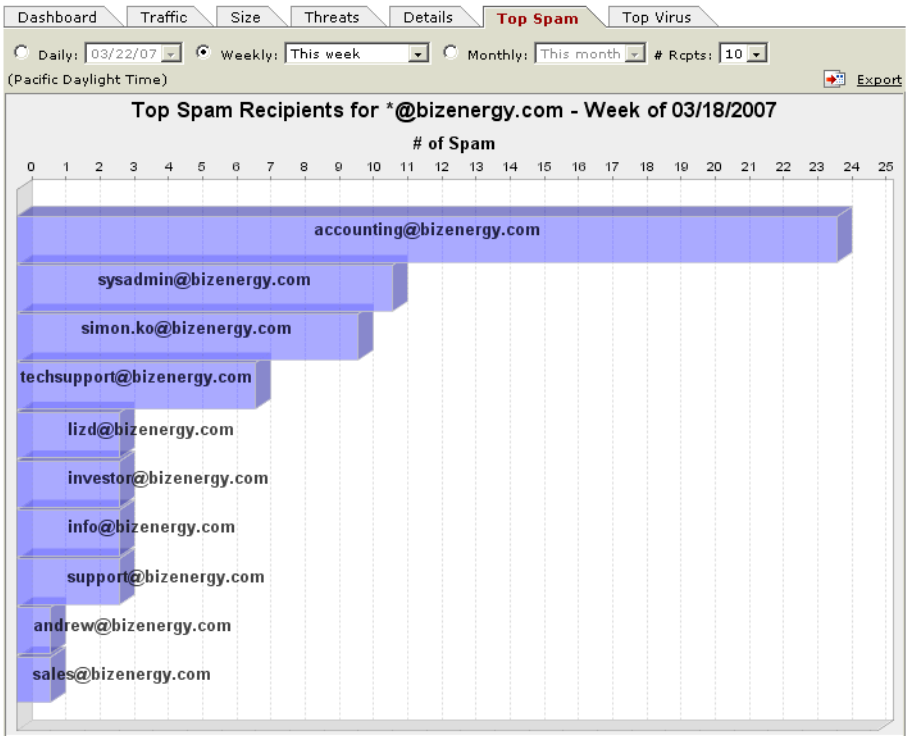


FIGURE 2-11 Top Spam Recipients report page

Top Virus Recipients

This Top Virus Recipients report (Figure 2-12) shows the top virus recipients for the selected mail domain. The default reporting period is the *current week*. Top virus recipient reports are displayed in GMT time.

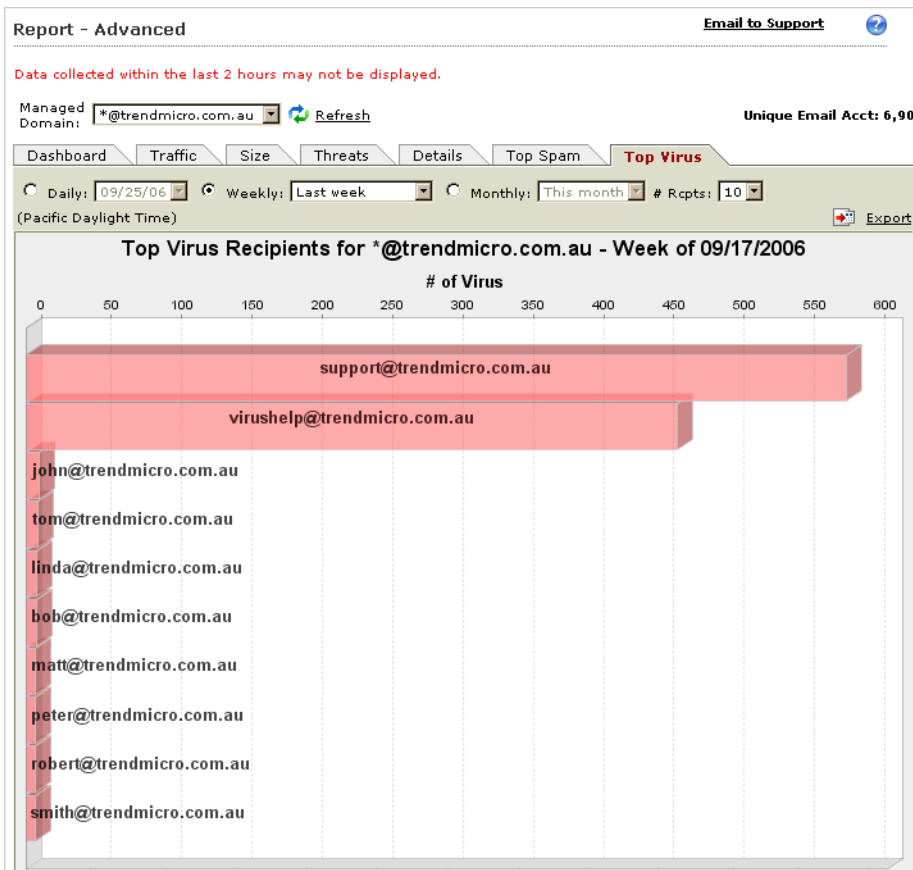
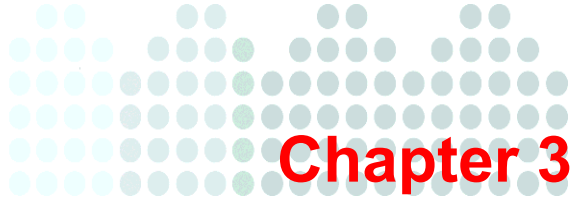


FIGURE 2-12 Top Virus Recipients report page



Policy, Logs, and Administration

This chapter covers the following InterScan Messaging Hosted Security functions:

- [Policy Administration](#) on page 3-2
- [Approved Senders](#) on page 3-34
- [Quarantine](#) on page 3-35
- [Logs](#) on page 3-45
- [Administration](#) on page 3-47
- [Disabling InterScan Messaging Hosted Security](#) on page 3-58

Policy Administration

An IMHS policy is defined as a set of rules for a specific mail domain. Multiple rules can exist for each domain (policy), but only a single policy can exist for any one domain.

At any time, administrators can see the rules that apply to their organization.

Depending on your level of service, you can view, modify, and create rules for a specific domain policy.

Standard customers have read-only rights, except for spam rules.

Advanced customers have creation and modification rights.

The screenshot shows the 'Policy Administration' interface. At the top, there are two tabs: 'Current rules' and 'Topic Help'. The 'Current rules' tab is active. Below the tabs, there is a 'Policy for:' section with a dropdown menu set to 'All my groups' and an 'OK' button. To the right of this section is a '15 per page' dropdown menu. Below the policy information is a table of rules. The table has columns for 'Rules', 'Action', 'Order', 'Modified', and 'Status'. The rules listed are:

Rules	Action	Order	Modified	Status
<input type="checkbox"/> bizenergy: Virus-mass-mailing	Delete	1	3/17/07	✓
<input type="checkbox"/> bizenergy: Exceeding msg size or # of recipients	Delete	2	3/17/07	✓
<input type="checkbox"/> bizenergy: Spam or Phish	Delete	3	3/17/07	✓
<input type="checkbox"/> bizenergy: Virus-uncleanable	Del. Attach ...	4	3/17/07	✓
<input type="checkbox"/> bizenergy: High-risk attachment	Del. Attach ...	5	3/17/07	✓
<input type="checkbox"/> bizenergy: Virus-cleanable	VirusClean	6	3/17/07	✓
<input type="checkbox"/> bizenergy: Newsletter or spam-like	Tag Subject	7	3/17/07	✓

At the top right of the Rules list, the text '1-7 of 7' is displayed. A red circle highlights the 'Topic Help' icon in the top right corner of the screen.



FIGURE 3-1 Policy screen, Advanced level

The Policy screen shows a list of the currently defined rules and the status of each. If you have a service level that allows it, from this screen you can add a new rule and edit, copy, or delete existing rules. For an description of the default rules, see [Default Policy Settings](#) on page 3-4.

At the top right of the Rules list, the number of rules shown on this page and the total number of rules are displayed. You can filter the list by using the drop-down lists near the top of the screen.

The rules are displayed in a table, and sorted by the order in which the rules are applied during scanning by IMHS. The contents of each table can be resorted by clicking a column heading. For example, click the Action column heading to resort the table alphabetically by action.

TABLE 3-1 Enabled and disabled icons

ICON	DESCRIPTION
	The rule is enabled.
	The rule is disabled.

Click the icon to the right of each rule to enable or disable that rule.

Note: Disabling any rule may have adverse effects on your email security. For example, disabling a virus rule will expose you to virus attacks.

Though Standard service users have read-only privileges for creating new rules, they can configure the spam rule settings such as tagging the subject, deleting and quarantine as shown in [Figure 3-2](#).

Policy

Policy for:

1-7 of 7

Rules	Action	Order	Modified	Status
bizmomentum: Virus-mass-mailing	Delete	1	4/12/07	✓
bizmomentum: Exceeding msg size or # of recipients	Delete	2	4/12/07	✓
bizmomentum: Spam or Phish	<input type="text" value="Delete"/> <input type="button" value="OK"/> <input type="button" value="cancel"/>	3	4/24/07	✓
bizmomentum: Virus-uncleanable	<input type="text" value="Delete"/>	4	4/12/07	✓
bizmomentum: High-risk attachment	<input type="text" value="Tag Subject"/> <input type="text" value="Quarantine"/>	5	4/12/07	✗
bizmomentum: Virus-cleanable	VirusClean	6	4/12/07	✓
bizmomentum: Newsletter or spam-like	<input type="text" value="Tag Subject"/>	7	4/24/07	✓

1-7 of 7

FIGURE 3-2 Standard-level users spam rule options

Default Policy Settings

The following rules makes up the default policy for all IMHS customers.

IMHS Advanced customers can edit the default rules as well as create new rules.

IMHS Standard customers have read-only access and can view the default policy but cannot edit the rules.

Rule 1: Virus

If any of the following are found, then the entire message is deleted.

- a. **Mass Mailing:** Designed to protect the user from viruses that are often spread by mass mailing type campaigns. A message is identified as containing a virus that cannot be cleaned and the message shows mass-mailing behavior.
- b. **Virus-uncleanable:** A message is identified as containing a virus that cannot be cleaned.
- c. **Virus-cleanable:** A message is identified as containing a virus that can be cleaned.

Rule 2: Exceeding Message Size or Allowed Number of Recipients

This rule is designed to protect the system from Denial of Service (DOS) and Zip of Death attacks. If the size of the incoming message exceeds the default limit of 10MB or it has been sent to more than 50 recipients in the organization, then the message is deleted. IMHS Advanced customers may modify this rule up to the system limits of 50MB and 100 recipients.

Rule 3: Spam or Phish

This rule is designed to catch spam or phishing email messages. The default action is to delete all messages identified as spam or phishing email messages. All IMHS customers have the ability to change the default action. We highly recommend that only the Delete or Quarantine actions are used for this rule. All quarantined messages are saved for seven days in the IMHS web-accessible quarantine.

IMHS Advanced customers can modify the criteria used for the spam catch rate from Lowest (least aggressive) to Highest (most aggressive). The default setting is Moderately Low.

Note: There are two default rules relating to spam. For newsletters or spam-like email messages, please refer to [Rule 5: Newsletter or Spam-Like](#).

Rule 4: High-Risk Attachment

This rule is only available to IMHS Advanced service customers. Delete high-risk attachments from email messages are defined in the criteria of the rule. Examples of a high-risk attachment could be an executable file with .exe extension or a media file (.mp3) that has been renamed to harmless_file.txt. If a message is identified as containing a high-risk attachment, then the high-risk attachment is deleted from the email message before it is delivered.

Rule 5: Newsletter or Spam-Like

This rule is designed to catch “gray-mail” such as newsletters. The default action for these spam-like email messages is to Tag Subject (with “Spam>”). We highly recommend that only the Tag Subject or Quarantine actions are used for this rule. All quarantined messages are saved for seven days in the IMHS web accessible quarantine.

IMHS Advanced customers can modify the criteria used for the spam catch rate from Lowest (least aggressive) to Highest (most aggressive). The default setting is Moderately High.

Note: There are two default rules relating to spam. For highly likely spam or phishing messages, please refer to [Rule 3: Spam or Phish](#).

Rule 6: Password-Protected Zipped File Attachments

This rule is designed to allow advanced users to configure the action taken to handle email messages with password-protected zip file attachments. By default, messages with a password-protected zip file attachment are passed through to the recipient and a notification is placed in the body of the mail stating that the attached file was not scanned.

Default Outbound Filtering Policies

If, as an IMHS Advanced user, you opt to enable outbound filtering, an additional four default rules are added. These rules are designed just as their namesakes described above, except that they apply to outbound email only. The default outbound-filtering rules are:

- Outbound – Virus
- Outbound – High-risk attachment
- Outbound – Exceeding msg size or # of recipients
- Outbound – Spam or Phish

Content Filtering

IMHS Advanced users can apply content filtering rules to email messages. InterScan Messaging Hosted Security provides flexible and easy content-filtering options by which you can flag virtually any type of content.

Filtering Content with Keywords

You can configure IMHS rules to match content as part of their operating logic. IMHS can match content by using keywords, regular expressions, or both. Configure content filtering in step 2 when adding a new rule or editing a rule, as follows.

To configure content filtering using keywords:

1. When adding or editing a rule, in Step 2: Select Scanning Criteria, select **Advanced**. A number of options appear under Advanced, such as those shown in [figure 3-3](#) below.

Add Rule

Step1 >>> **Step 2: Select Scanning Criteria** >>> Step3 >>> Step4

Advanced	All Match <input checked="" type="radio"/> Any Match <input type="radio"/>
<input type="checkbox"/> Attachment is	password protected
<input type="checkbox"/> Attachment is	name or extension
<input type="checkbox"/> Attachment is	MIME content-type
<input type="checkbox"/> Attachment is	true file type
<input type="checkbox"/> Message size is	> <input type="text" value="10"/> <input type="text" value="MB"/>
<input type="checkbox"/> Subject matches	keyword expressions
<input type="checkbox"/> Subject is	blank
<input type="checkbox"/> Body matches	keyword expressions
<input type="checkbox"/> Attachment is	keyword expressions

FIGURE 3-3 Content filtering options

2. Select the portion of the email to scan for content. Relevant options are:
 - Subject
 - Body
 - Specified header
 - Attachment
3. Click the **keyword expressions** link to the right of your selection. The Keyword Expressions screen opens, as shown in [figure 3-4](#) below.

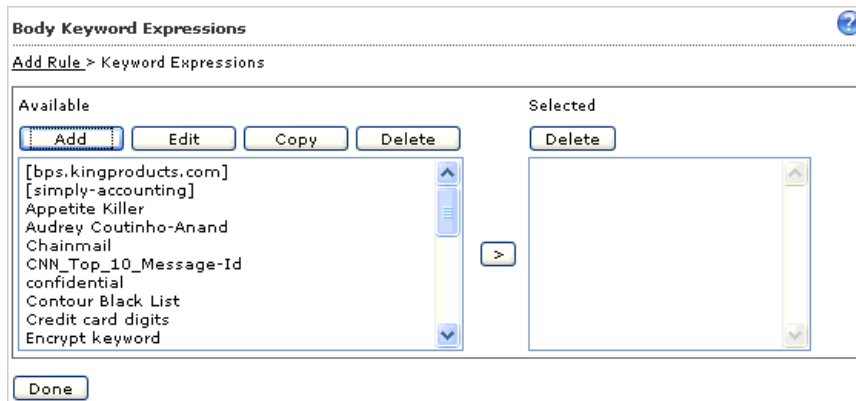


FIGURE 3-4 Keyword Expressions screen

4. Select one or more existing expressions and click the right arrow button (>). The selected expressions appear in the Selected box on the right.
5. Optionally, click **Add** to create a new expression, **Edit** to edit an existing one, **Copy** to create a copy (for modifying), or **Delete**.
6. Click **Done**. IMHS records your selections and redisplay the main Step 2: Select Scanning Criteria screen.
7. Repeat the above steps for each portion of the email to filter for content.
8. Once you have completed adding advanced filtering criteria, select **All Match** (the default) or **Any Match** in the column to the right of “Advanced” to configure whether an email must match all of your selected criteria or any of them in order to trigger the rule.
9. Click **Next** and complete the rule as explained in [Adding a New Rule \(IMHS Advanced Only\)](#) on page 3-25.

Filtering Content with Regular Expressions

To configure content filtering using regular expressions:

1. Follow [Step 1](#) through [Step 3](#) above to display the Keyword Expressions screen.
2. Click **Add** to create a new expression or select an existing expression and click **Edit**. The Keyword Expressions screen redisplay with a different layout, as shown in [figure 3-5](#) below.

FIGURE 3-5 Keyword expressions screen for regular expressions

3. In the **List name** field, type a name for the expression if creating a new one. (If editing an expression, the existing name prepopulates this field.)
4. In the **Match** drop-down list, select one of the following:
 - **Any specified**—Matches any of the keywords or regular expressions that you list
 - **All specified**—Must match all of the keywords and/or regular expressions that you list in order to be considered a match
 - **Not the specified**—Equivalent to a .NOT. operator, results in a match if the content does not match any of the keywords or regular expressions that you list
 - **Only when combined score exceeds threshold**—Upon selection, this option displays another field below it, “Total message score to trigger action.” With this option, IMHS filters the content for the expression(s) that you list only if the total email message spam score is higher than the threshold that you enter (default is 2).
5. Click **Add**. The Add Keyword Expressions screen appears.
6. In the text box type any combination of keywords and regular expressions to define a keyword expression (without line breaks). The available regular expression operators are shown below:

\ | () ^ \$ * + ?

Tip: To use a regular expression operator as a literal character, you must escape out of it by using a backslash character (\) immediately before it. Trend Micro recommends using regular expressions only if you are experienced in using them. IMHS cannot accept expressions inputted in incorrect regex syntax.

- Click **Save**. The Keyword Expressions screen displays a table that lists the expressions that you have created, as shown in [figure 3-6](#) below.

Keyword Expressions

Add Rule > Keyword Expressions

List name:

Match:

<input type="checkbox"/>	Keywords/regular expressions	Case sensitive
<input type="checkbox"/>	frog\$	<input type="checkbox"/>
<input type="checkbox"/>	toast burnt bread	<input type="checkbox"/>
<input type="checkbox"/>	^Cranky	<input checked="" type="checkbox"/>

FIGURE 3-6 Keyword expressions have just been added

- Select the **Case sensitive** check box as applicable. If you selected **Only when combined score exceeds threshold** for the Match field and you have added multiple expressions, select the weighting score for each expression, as explained in [Weighting Keyword Expression Lists](#) on page 3-11.
- Click **Save**. The expression list that you just created appears in the “Available” list in the box on the left, as shown in [figure 3-7](#) below.

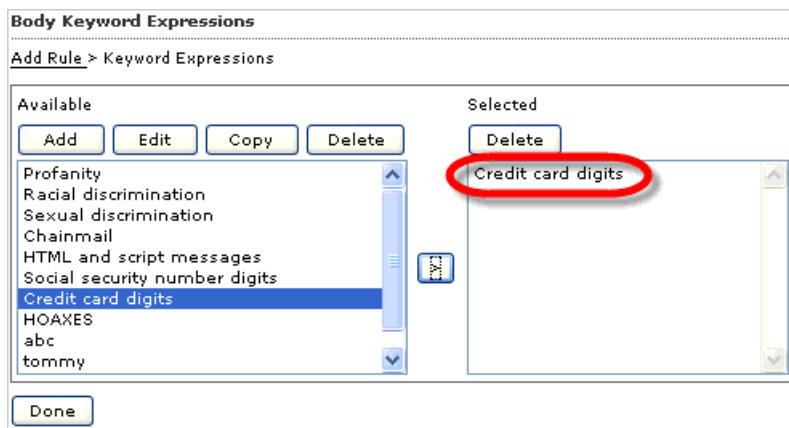



FIGURE 3-7 Adding a keyword expression to a rule

10. To add the new criteria to the rule, select the name of the list in the left box, click the right arrow button () , and then click **Done**. IMHS adds your criteria to the rule that you are creating.
11. Click **Next** and complete the rule as explained in [Adding a New Rule \(IMHS Advanced Only\)](#) on page 3-25.

Weighting Keyword Expression Lists

When creating a list of keyword expressions, you can assign a weighting factor to each expression in the list.

and the Match drop down option is set to “Only when combined score exceeds threshold” an overall score must be set for the keyword expression as well as an individual score for each component.

To use weighting on keyword expression lists:

1. Ensure that you have selected **Only when combined score exceeds threshold** in the Match drop-down list.
2. Type a total weight in the **Total message score to trigger action** field.
3. Select a weight for each expression in the list from the drop-down lists in the **Score** column, as shown in [figure 3-8](#) below.

Add Rule > Keyword Expressions

List name:

Match:

Total message score to trigger action:

<input type="checkbox"/>	Keywords/regular expressions	Case sensitive	Score
<input type="checkbox"/>	"IN GOD WE TRUST"\s+(\S+\s+)*electioneering posters	<input type="checkbox"/>	6
<input type="checkbox"/>	anti-persipant\s+(\S+\s+)*breast cancer	<input type="checkbox"/>	5
<input type="checkbox"/>	ASPARTAME\s+(\S+\s+)*multiple sclerosis	<input type="checkbox"/>	1
<input type="checkbox"/>	autograph.t.pif\s+(\S+\s+)*Virus	<input type="checkbox"/>	4
<input type="checkbox"/>	AWARD NOTIFICATION FINAL NOTICE	<input type="checkbox"/>	10

FIGURE 3-8 Weighting keyword expressions

4. Optionally, select the **Case sensitive** check box for any applicable keyword lists
5. Click **Save**.

For each keyword expression item listed that matches content in an email, IMHS increases the keyword score of the message by the number in the Score column for that list. For example, if two words in a message match words in a keyword list named “Profanity,” with a score of 2, then the score for that message will be 4.

If the total score exceeds the number in the “Total message score to trigger action” field, then the rule will be triggered. For example, if two keyword list matches are triggered for a message score of 4, and the Total message score to trigger field value is 3, then the rule will be triggered.

Rule Actions

IMHS provides a number of actions that you can use when building or modifying a rule. Actions available to IMHS Advanced users are:

- [Delete Entire Message](#) on page 3-13
- [Deliver the Message Now](#) on page 3-13
- [Quarantine the Message](#) on page 3-14
- [Clean Cleanable Virus and Delete Those That Cannot Be Cleaned](#) on page 3-14

- [Delete Matching Attachments](#) on page 3-15
- [Insert a Stamp in the Mail Body](#) on page 3-15
- [Tag the Subject Line](#) on page 3-16
- [Send a Notification Message](#) on page 3-16
- [BCC Another Recipient](#) on page 3-17
- [Encrypt Email Message](#) on page 3-18 (purchased separately)

These actions are executed in a pre-set order based on processing logic built into IMHS. For more information on execution order, see [Execution Order of Rules](#) on page 3-23.

Delete Entire Message

This action deletes the message and all attachments. The message is recorded as deleted in the IMHS logs, but once deleted, the message cannot be recovered. It falls into the Intercept category of actions (see [Intercept Actions](#) on page 3-23).

To configure a rule action to delete a message:

1. Select the **Delete entire message** action from the Intercept section.
2. Click **Next** if you are creating a new rule, or **Save** if you are editing an existing rule.

Deliver the Message Now

Use the Deliver Now action to deliver email immediately. When this action takes effect, IMHS delivers the email without executing any more rules for the affected email.

All rules are auto-ordered for security and execution efficiency. Administrators are relieved of determining the order of rule execution. The Deliver Now action bypasses the automatic order of execution so that IMHS can deliver the email immediately.

WARNING! The “Deliver now” action is not recommended for use as the only action. If you choose “Deliver now” as the only action for Spam mail, for example, all of that mail will simply be delivered to your recipients, as if there were no Spam filter in place.

If you use “Deliver now” with a virus rule, ensure that you also have a “Delete” action for the virus rule. Only the “Delete” action takes higher priority than “Deliver now” and so would be processed before it (and then terminate the processing of that rule).

To configure a rule action to deliver a message immediately:

1. Select the **Deliver Now** action from the Intercept section.
2. Click **Next** if you are creating a new rule, or **Save** if you are editing an existing rule.
3. Click **OK** on the Deliver Now warning message that appears. The message closes.
4. If creating a new rule, type a name for the rule in the **Rule Name** field.
5. Click **Save**.

WARNING! If you chose “Deliver now” as the only action for a virus rule, mail containing viruses would leak through unblocked.

Quarantine the Message

If your service level includes Quarantine Action, this action places the message and all attachments in the quarantine area configured in the rule. It falls in the category of Intercept actions (see [Intercept Actions](#) on page 3-23).

To configure a rule action to quarantine a message:

1. In the Intercept section of the Rule Action screen, select the **Quarantine** action.
2. Select a quarantine area from the drop-down list, or click **Edit** to create a new quarantine area.

Note: Quarantined items are now stored in a directory structure created by InterScan Messaging Hosted Service. This allows for increased performance when the product is saving items into quarantines or when users view them through the Web console. Quarantined messages are indexed in the InterScan Messaging Hosted Service database to provide you with queries and improved search tools.

3. Click **Next** if you are creating a new rule, or **Save** if you are editing an existing rule.

Clean Cleanable Virus and Delete Those That Cannot Be Cleaned

This action will clean cleanable viruses (or other configured threats) contained in message attachments. If the threat cannot be cleaned, the message attachment that contains it will be deleted. Clean cleanable Viruses falls into the category of Modify actions (see [Modify Actions](#) on page 3-23).

Note: The “clean cleanable viruses” action is only available when the virus criteria are selected in the rule definition. For example:

If this action is used in the rule and a message contains an uncleanable virus, the message will be deleted.

If both the “delete matching attachment” and “clean cleanable viruses” actions are used in the same rule, a violating attachment will be deleted directly and the “clean cleanable viruses” action will not be taken.

To configure a rule action to clean virus-infected attachments:

1. From the Modify section of the Action page, select the **Clean virus-infected files** action.
2. Click **Next** if you are creating a new rule, or **Save** if you are editing an existing rule.

Delete Matching Attachments

This action deletes any attachments that match the rule criteria. It falls into the Modify category of actions (see [Modify Actions](#) on page 3-23).

Note: The Delete Matching Attachments action is invoked only when Size, Attachment, Content and/or Virus criteria are used in rule. For instance, a spam rule with an action of Delete Matching Attachment does not have an effect on the message.

To configure a rule action to delete attachments that match a criteria:

1. Select **Delete Matching Attachments** from the Modify section.
2. Click **Next** if you are creating a new rule, or **Save** if you are editing an existing rule.

Insert a Stamp in the Mail Body

The Insert Stamp action inserts a block of text into the message body. The stamps are maintained as named objects in the database and are selected from a list. The stamp definitions contain the text of the stamp (which can contain IMHS variables), whether they are to be inserted at the beginning or the end of the message body, and whether or not to avoid stamping TNEF and digitally signed messages to prevent breakage.

To configure a rule action to insert a stamp in the message body:

1. Select the **Insert stamp in body** check box.
2. Click **Edit**. The Stamps screen appears, showing a drop-down list of available stamps.
3. Select a stamp from the list or click **Add**, **Edit**, or **Copy** to create a new stamp or edit an existing one.
4. Click **Done**.

Tag the Subject Line

The Tag Subject action inserts configurable text into the message subject line. It falls into the Modify category of actions (see [Modify Actions](#) on page 3-23).

To configure a rule action to tag the message subject:

1. Select the **Tag Subject** check box.
2. Click the tag link to open the Tag editing screen.
3. Type a tag in the Tag field.
4. Select or clear the **Do not tag digitally signed messages** check box.
5. Click **Save**.

Send a Notification Message

Notifications are messages that are sent when the rule is triggered. This action falls into the Monitor category of actions (see [Monitor Actions](#) on page 3-24).

To configure a notification message:

1. In the Monitor section of the Action screen, select the **Send notification** check box and click the **message to people** link.
2. Select an existing notification and click **Edit** or click **Add** to create a new notification message. The Add Rule > Notifications screen appears.
3. Name the notification.
4. Type an address in the **From** field. This address will appear in the sender field when the notification message is viewed by recipients and can be used to mask IMHS from internal users or external message recipients.
5. Type an address in the **To** field. This address will be used when the notification message is sent to the Administrator.

6. Select notification recipients:
 - Select **Sender** to send the notification message to the sender.
 - Select **Recipient** to send the notification message to the recipient. (Only applicable if your IMHS service level provides it.)
 - Select **SNMP Trap** to send the notification by SNMP. If you select SNMP, also either select the first of the two radio buttons and choose the appropriate category code. (Only applicable if your IMHS service level provides it.)
7. Type a message subject. Use variables if needed.
8. Select **Attach** to attach a copy of the original message to the notification message, and select **Modified message** or **Unmodified message** from the drop-down list.

WARNING! Selecting “Unmodified message” could result in infected messages or attachments entering your messaging environment. Trend Micro strongly recommends against choosing this setting unless you have a strong need to analyze messages in their unmodified form.

9. Type the notification message body in the **Text** field. Click the **Variable list** link to see the variables available for use in notification messages.
10. Click **Save**.

BCC Another Recipient

The BCC action sends a BCC (blind carbon copy) to a recipient or recipients configured in the rule. This action falls into the Monitor category of actions (see [Monitor Actions](#) on page 3-24).

You can only configure a notification to be sent to an address in your own domain.

To configure a rule action to send a copy of the message to a BCC recipient:

1. From the Monitor section of the Action page, select the BCC check box.
2. Type the email address of the recipient in the field. If you have more than one email address, enter them in the field separated by commas.
3. If creating a new rule, click **Next**. If editing an existing rule, click **Save**.

Encrypt Email Message

The purpose of this rule action is to protect sensitive data in email sent by users in your organization. The Email Encryption service uses the existing architecture of IMHS. When an email message triggers a content-filtering rule that has encryption as its action, IMHS sends the email to the IMHS encryption server, which encrypts the message and forwards it to the outbound MTA.

This action is unique in that it is a non-terminal action that cannot co-exist with other actions (terminal or non-terminal) in the same rule. This action can apply to outbound rules only.

In most cases, a rule to encrypt email will be based on one of the following:

- Specific senders or recipients of the message (for example, a rule that encrypts all email sent from Human Resources or the Legal department)
- Specific content in the message body

For detailed guidelines on setting up keyword expressions for use with content filtering, see [Content Filtering](#) starting on page 3-6.

To configure a new rule to encrypt an email message:

1. On the left menu, click **Policy**. The Policy screen appears.
2. Click **Add**. The Add Rule / Step 1: Select Recipients and Senders screen appears.
3. Select **Outgoing message** from the “This rule will apply to” drop-down list.
4. Click the **Senders** link and select one or more addresses or domains.
5. Click **Save** to close that screen and then click **Next** to proceed to the Step 2: Select Scanning Criteria screen.
6. Accept the default of “No Criteria” or click **Advanced**. A number of options appear under the Advanced option.
7. From that list select an option that scans the message for particular content, for example, **Subject matches**, **Body matches**, **Specified header matches**, or **Attachment content matches**.
8. Click the keyword expression link next to the selected option and add one or more keyword expressions as explained in [Content Filtering](#) starting on page 3-6.
9. Click **Next**. The Add Rule / Step 3: Select Actions screen appears.
10. Accept the default choice of “Do not intercept messages” and scroll down to the “Modify” section.

11. Select the **Encrypt email** check box and click **Next**. The Add Rule / Step 4: Name and Notes screen appears.
12. Type a name for the new rule and click **Save**. IMHS returns you to the Policy page with the new rule highlighted in yellow.

Reading an Encrypted Email

When an “Encrypt email” rule is triggered, there are two ways for a recipient to decrypt an encrypted message. The first is by purchasing Trend Micro Email Encryption Client. For more information on this product, please see the following page on the Trend Micro Web site: <http://us.trendmicro.com/us/products/enterprise/email-encryption/>

If not using this client, the recipient receives a notification similar to that shown in [figure 3-9](#) on page 3-20.

Note: It is not possible to decrypt the encrypted message with Microsoft Outlook Web Access 2007.

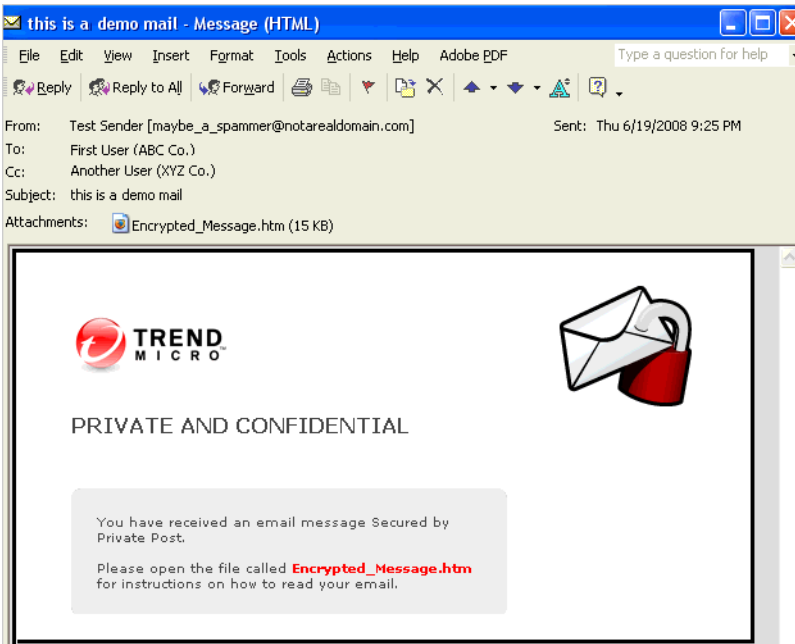


FIGURE 3-9 Encrypted message notification

To retrieve an encrypted email, the recipient must do the following:

1. Double-click the attached “Encrypted_Message.htm” file, which opens in the default browser of the user, as shown in [figure 3-10](#).

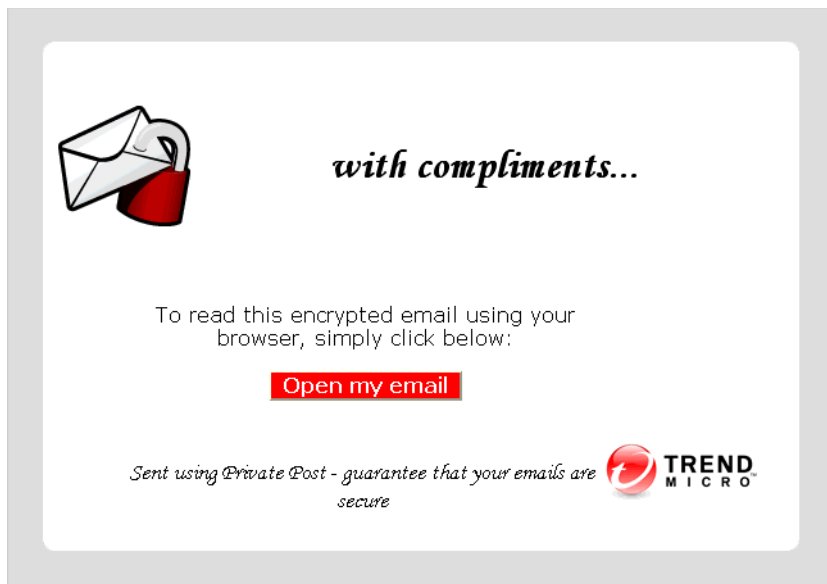


FIGURE 3-10 Encrypted_Message.htm as viewed in browser

2. Click **Open my email**, and if not yet registered, fill in the registration information on the subsequent pages. If you have already registered for this service, the encryption site displays your decrypted email at this point.

Note: The “Open my email” function may not work reliably with some Web-based email systems. If the button does not work, the customer can save the attachment to a local computer and then open it again.

3. For enhanced security, match a CAPTCHA image, type and confirm a pass phrase, and select and answer three security questions. Upon successful registration, the email encryption site sends an activation message to the recipient’s email account.

4. Upon receipt of the activation message, click **Please click here to validate your identity**. The Trend Micro email encryption site loads in your browser and displays your decrypted message, as shown in [figure 3-11](#) on page 3-22.

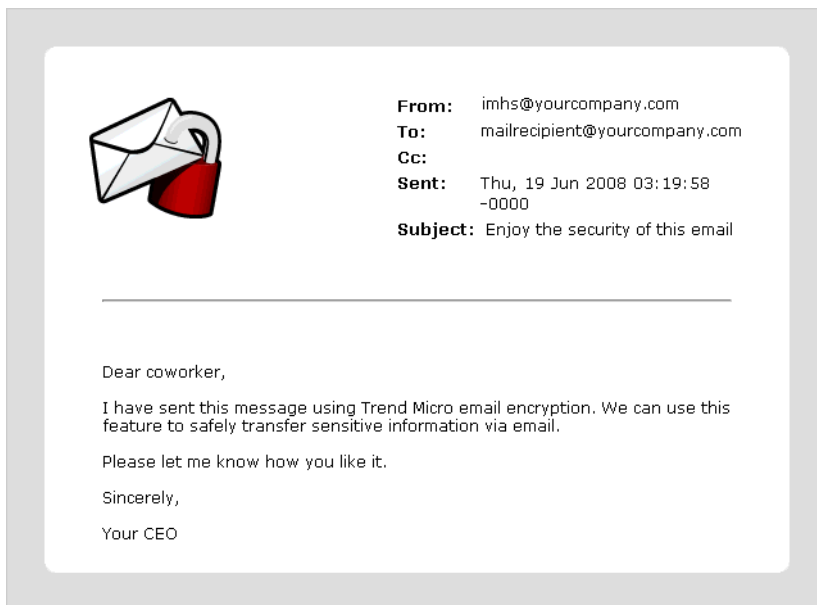


FIGURE 3-11 Decrypted email message

Note: Recipients only need to register once. After registering with the Email Encryption service, the recipient will be able to view decrypted email in a browser window, merely by clicking **Open my email**.

Execution Order of Rules

All rules are auto-ordered for security and execution efficiency. Administrators are relieved of determining the order of rule execution. There are four types of actions in a rule:

- [Intercept Actions](#)
- [Modify Actions](#)
- [Monitor Actions](#)
- [Email Encryption Action \(IMHS Advanced Only\)](#)

Intercept Actions

Once an intercept, or “terminal,” action executes, processing of that rule stops and no further action takes place for that rule.

Intercept actions execute following a strict priority order:

1. Delete the entire message
2. Deliver the message now (See note on [page 3-27](#).)
3. Quarantine the message
4. Re-address to another email recipient

Important Note About the Deliver Now Action

The “Deliver now” action is not recommended for use as the only action. If you choose “Deliver now” as the only action for Spam mail, for example, all of that mail will simply be delivered to your recipients, as if there were no Spam filter in place.

If you use “Deliver now” with a virus rule, ensure that you also have a “Delete” action for the virus rule. Only the “Delete” action takes higher priority than “Deliver now” and so would be processed before it (and then terminate the processing of that rule).

WARNING! If you choose “Deliver now” as the only action for a virus rule, mail containing viruses would leak through unblocked.

Modify Actions

The following “modify” (non-terminal) actions execute but do not terminate processing (email will be delivered to the original intended recipients):

- Clean cleanable virus
- Delete attachment
- Insert a stamp in the mail body
- Tag the subject line

Tip: Intercept (“terminal”) actions have higher execution priority over non-terminal actions. When a terminal action is triggered, there is no need to perform any other actions. However, non-terminal actions can be combined, such as “Delete an attachment” and also “Stamp the mail body.”

Monitor Actions

These actions can be combined with either terminal or non-terminal actions listed above:

- Send a notification message
- BCC another recipient

Tip: The notification email message sent to monitor actions can be customized using the variables shown in the online help.

Email Encryption Action (IMHS Advanced Only)

The Trend Micro Email Encryption action option is enabled if you have purchased this separate service. The Email Encryption service is available only to IMHS Advanced customers who have enabled outbound filtering. This action is unique in that it is a non-terminal action that cannot co-exist with other actions (terminal or non-terminal) in the same rule. If more than one rule applies to a message, IMHS processes the rule that uses the encrypt email action after processing all other rules.

Note: Please note that “do not intercept” is not considered an action.

Adding a New Rule (IMHS Advanced Only)

Rules are the means by which messaging policies are applied to message traffic in IMHS. Each rule consists of three main parts:

- The user(s) or domain(s) to which the rule applies.
- The criteria that are evaluated to determine if the rule should be triggered.
- The action that IMHS will take if the rule is triggered.

After these three parts of the rule have been configured, the rule is given a unique name by which it can be identified in summaries, mail tracking, and elsewhere. Each rule can be disabled without losing its definition and re-enabled at a later time.

To create a new rule:

1. Click **Add** in the Policy screen. The **Add Rule** screen appears.

InterScan Messaging Hosted Security

Powered By **TREND** | Logged on as **smartcustomer** | Log Off | Help

Report

Policy

Approved Senders

Quarantines

Logs

Administration

Logged on as **smart@yourcompany.com**

Step 1: Select Recipients and Senders >>> Step2 >>> Step3 >>> Step4

This rule will apply to Incoming message

To	Recipients	Exceptions
From	Senders	Exceptions

Back Next Cancel

FIGURE 3-12 Add Rule screen

2. Select the user(s) or domain(s) to which the rule applies.

Incoming messageTo

Add Rule > Incoming messageTo

Select addresses

Enter address or domain

Examples: user@trendmicro.com,
*@trendmicro.com

Add >

Selected

*@testing.com

Save Cancel

FIGURE 3-13 Adding domain and users on this screen.

3. Select and configure the criteria.

Add Rule

Step1 >>> **Step 2: Select Scanning Criteria** >>> Step3 >>> Step4

<input type="radio"/>	No Criteria	
<input type="radio"/>	Message contains	<u>viruses or malicious code</u>
<input checked="" type="radio"/>	Message is	<input type="checkbox"/> Spam ⓘ Lowest (most conservative) ▾ <input checked="" type="checkbox"/> Phish and other suspicious content
<input type="radio"/>	Advanced	<input checked="" type="radio"/> All Match <input type="radio"/> Any Match

If message is

incoming
to "@testing.com"
AND
from Anyone

Back Next Cancel

FIGURE 3-14 Select criteria for the rule on this screen.

- Select and configure the intercept action.

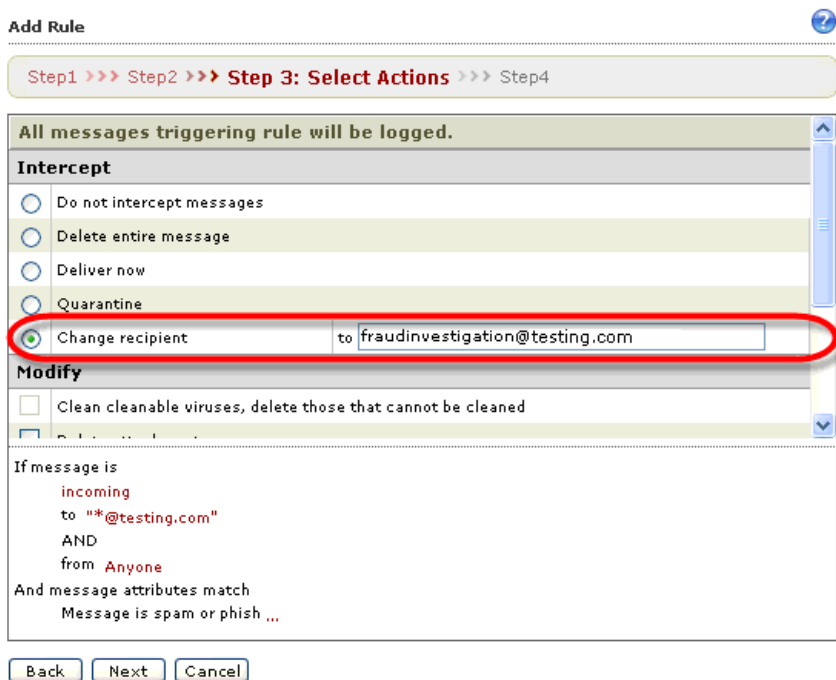


FIGURE 3-15 Select action on this screen

WARNING! The “Deliver now” action is not recommended for use as the only action. When selected, the “Deliver now” action bypasses all other rules. Therefore, if you have criteria to search for, they will not be processed.

If you choose “Deliver now” as the only action for Spam mail, for example, all of that mail will simply be delivered to your recipients, as if there were no Spam filter in place.

If you chose “Deliver now” as the only action for a virus rule, mail containing viruses would leak through unblocked.

If you attempt to set “Deliver now” as the action, the warning message shown in appears.

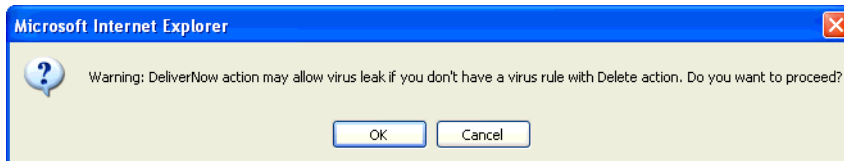


FIGURE 3-16 Deliver Now warning message

5. Optionally, select any Modify or Monitor actions, as shown in [figure 3-17](#) below.

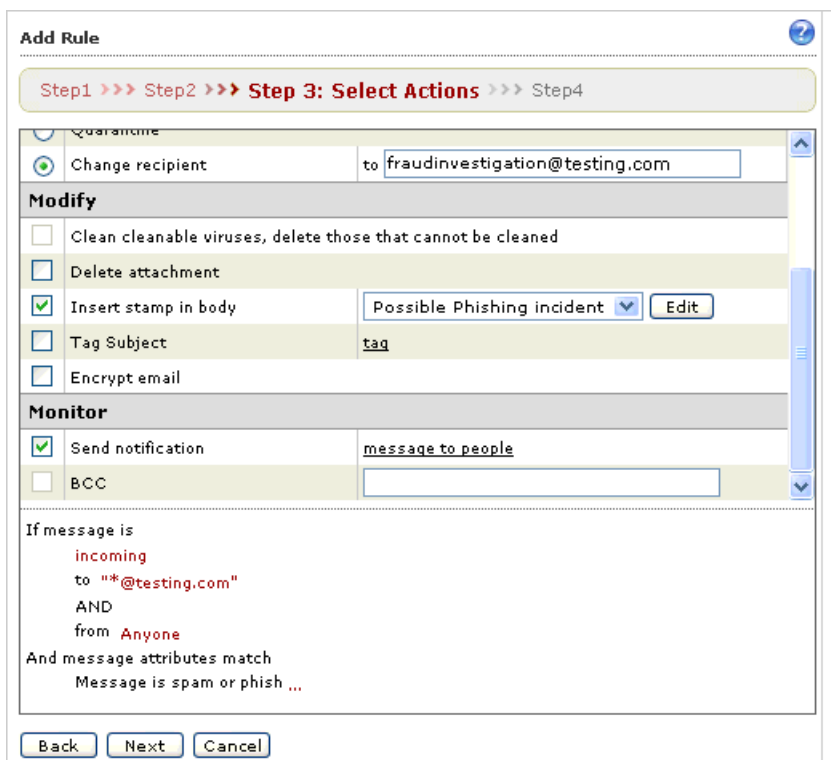


FIGURE 3-17 Step 3: Selecting Modify and Monitor actions

6. Name and enable the rule.

Add Rule ?

Step1 >>> Step2 >>> Step3 >>> **Step 4: Name and Notes**

Rule | Notes

Rule Name: Phish email redirect, stamp, and notify

Enable

to "*"@testing.com"
AND
from Anyone
And message attributes match
Message is spam or phish ...

Then action is
Change recipient to fraudinvestigation@testing.com
AND
Insert stamp in body from Possible Phishing incident
AND
Send notification

Back Save Cancel

FIGURE 3-18 Name and save the rule on this screen

7. Click **Save**.

The **Policy** screen appears with your new rule in the appropriate order and highlighted in the list, as shown in [figure 3-19](#) below.

Policy

Policy for:

<input type="checkbox"/>	Rules	Action	Order	Modified	Status
<input type="checkbox"/>	Everything coming from irad@iradrocks.com DELETE !	Delete	1	1/30/08	
<input type="checkbox"/>	testing: Exceeding msg size or # of recipients	Delete	2	1/30/08	
<input type="checkbox"/>	testing: Spam or Phish	Delete	3	1/30/08	
<input type="checkbox"/>	testing: Virus	Quarantine	4	1/30/08	
<input type="checkbox"/>	testing: Password protected	Quarantine ...	5	1/30/08	
<input type="checkbox"/>	Spam or Phish: Delete All	Quarantine	6	1/30/08	
<input type="checkbox"/>	Phish email redirect, stamp, and notify	Readdress ...	7	3/21/08	
<input type="checkbox"/>	testing: High-risk attachment	VirusClean ...	8	1/30/08	
<input type="checkbox"/>	testing: Newsletter or spam-like	Stamp	9	1/30/08	

1-9/9

1-9/9

FIGURE 3-19 Policy screen showing newly created policy

Editing an Existing Rule (IMHS Advanced Only)

To edit an existing rule:

1. In the rule list, click the name of the rule you want to edit.
2. Edit the rule.

The example below shows adding an approved sender to this rule.

- a. Click on the **If message is...** link to edit the sender exception list.
- b. Click on **Exception** on the Sender line.
- c. Type the sender's address in the text box to add an approved sender to the exception list.

In this example, `imhs_support@trendmicro.com` was excluded from this rule.

3. Click **Save** to save the approved senders for this rule. This saves the approved senders but not the rule.

Incoming messageExcept From ?

[bizenergy: Virus-mass-mailing >](#) Incoming messageExcept From

Select addresses

Enter address or domain

Examples: user@trendmicro.com,
*@trendmicro.com

Selected

imhs_support@trendmicro.com	
-----------------------------	--

FIGURE 3-20 Edit sender exceptions on this screen.

4. Click **Save** to continue.

bizenergy: Virus-mass-mailing 

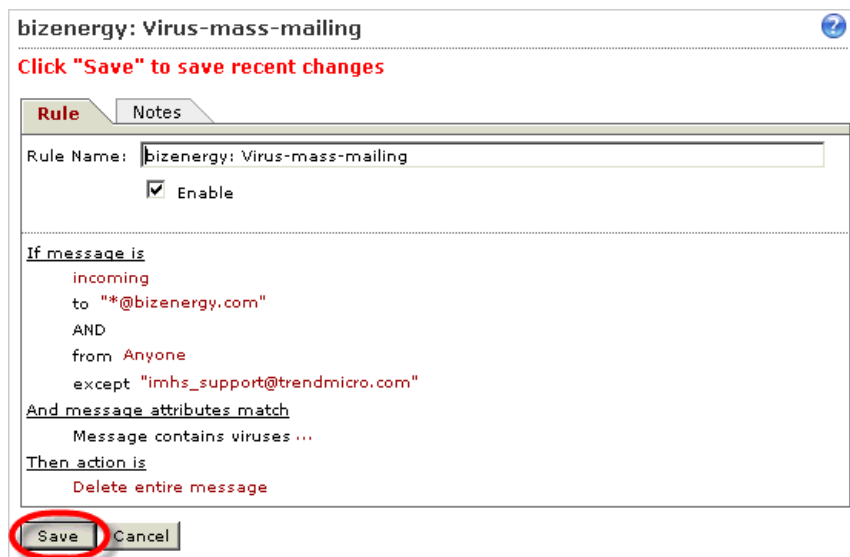
Click "Save" to continue

This rule will apply to

To	<u>Recipients</u>	<u>Exceptions</u>
From	<u>Senders</u>	<u>Exceptions</u>
If message is		
incoming		
to ".*@bizenergy.com"		
AND		
from Anyone		
except "imhs_support@trendmicro.com"		
And message attributes match		
Message contains viruses ...		
Then action is		
Delete entire message		

FIGURE 3-21 Edit Policy screen

5. Click **Save** again to save the rule.



bizenergy: Virus-mass-mailing ?

Click "Save" to save recent changes

Rule | Notes

Rule Name:

Enable

If message is

- incoming
- to "*"@bizenergy.com"
- AND
- from Anyone
- except "imhs_support@trendmicro.com"

And message attributes match

- Message contains viruses ...

Then action is

- Delete entire message

FIGURE 3-22 Save Policy changes on this screen

Copying an Existing Rule (IMHS Advanced Only)

Often a new rule will be very similar to one you already have. In such cases, it is usually easier to copy the rule and then edit the copy, rather than create a new rule from scratch.

To copy an existing rule:

1. In the rule list, select the check box in front of the rule to copy.
2. Click **Copy**. A rule named "Copy of [original rule name]" appears in the list of rules.
3. Edit the rule.

Deleting an Existing Rule (IMHS Advanced Only)

To delete existing rules:

1. In the rule list, select the check box in front of the rule or rules to delete.
2. Click **Delete**.

Approved Senders

The Approved Senders screen allows mail administrators to approve specific email addresses or domains to send email messages to the managed domains.

For approved senders:

- IMHS will not block any email messages from the senders (or domains) specified
- Content-based heuristic spam rules will not apply to email messages received from the specified senders or domains
- All virus, content-based, and attachment rules will still apply

The screenshot shows the 'Approved Senders' screen in the InterScan Messaging Hosted Security interface. The page title is 'InterScan Messaging Hosted Security'. The user is logged in as 'smartcustomer' and 'smart@yourcompany.com'. The 'Managed Domain' is set to 'bizenergy.com'. The table below lists the approved senders for this domain.

Sender	Recipient Domain	Date Approved
accounting@bizmomentum.com	bizenergy.com	10/26/06 06:45:31
finance@bizmomentum.com	bizenergy.com	10/26/06 06:45:38
support@bizmomentum.com	bizenergy.com	10/26/06 06:45:48
hr@fairywisteria.com	bizenergy.com	10/26/06 06:46:19
it@fairywisteria.com	bizenergy.com	10/26/06 05:44:40
finance@yum.com	bizenergy.com	10/26/06 05:41:43
support@yum.com	bizenergy.com	10/26/06 05:40:48

FIGURE 3-23 Approved Senders screen

To add Approved Senders:

1. Select the specific domain (or All Domains) to which the approved senders will be added from the Managed Domain drop-down list.
2. Click **Refresh**.
3. Enter a single address or domain in the **Add** field

Example:

- For a single address, enter: name@example.com
- For a domain, enter: *@example.com

4. Click **Approve Sender**.

To edit a listed entry:

1. Click on the entry.
2. Make your changes.
3. Click OK.

To delete an entry:

1. Select the check box for that entry.
2. Click Delete.

Quarantine

Note: This section is only applicable if your service level provides for the quarantine feature.

Quarantine Query

This screen provides you with a list of all quarantined messages that satisfy your query criteria. It also provides tools for handling these messages.

To delete one or more messages from Quarantine:

1. Select the check box in front of the message or messages to delete.
2. Click **Delete** to permanently remove the selected messages.

To resend one or more messages from Quarantine:

1. Select the check box in front of the message or messages to resend.
2. Click **Deliver (Not Spam)** to release the selected messages from quarantine.

Note: If you click **Deliver (Not Spam)**, the selected messages will be released from quarantine, and they are processed by InterScan Messaging Hosted Service (except that this time the anti-spam criteria are not applied). These messages may not arrive in your email in-box, however, if they violate other corporate messaging security policies.

To delete or resend all messages in the list:

1. Select the check box next to the **Date** column heading to select all messages. IMHS selects all messages on the screen.
2. Click **Delete** or **Deliver (Not Spam)**. IMHS deletes all the messages in the list.

Quarantine Settings

On the Quarantine settings screen you can configure a summary digest email message that lists up to 100 of the end user's quarantined email messages. This email digest provides a link for the account holder to access messages of interest. You can also enable the account holder to approve quarantined messages from within the email digest, as explained further below.

Approving Messages or Senders From Within the Spam Digest Email (Inline Action)

From the Quarantine Settings screen, you can enable inline action from spam digest email, that is, the ability for recipients of the spam digest email to approve one or more messages or senders directly from within the spam digest email message itself, using an HTML-based form.

Configuring Spam Digest Inline Action

By enabling spam digest inline action, you can relieve users of the necessity of logging on to the End User Quarantine and manually approving quarantined messages or senders.

Quarantine Settings ?

Managed Domain: Disabled

Digest Mail Schedule for imhs.com

Daily
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Sunday

Time:

Digest Mail Template for imhs.com

Sender's Email:

Subject: (Maximum number of characters is 256.)

HTML content: Inline Action: Disabled:

```

<html><head><style>.data2b {BACKGROUND-COLOR:
#ececdb;}</style></head><body><br/><b>Total number of
quarantined spam message(s):
%DIGEST_TOTAL_COUNT%</b><br/>Release quarantined spam
messages: <a href
="https://us.imhs-euq.trendmicro.com"
>https://us.imhs-euq.trendmicro.
(username: %DIGEST_RCPT% )<br/>Number of days to keep
quarantined spam messages: 7 <br/><br/>The following summary
displays a maximum of 100 of the most recent quarantined spam
messages:<br/><form id="01AE5E" method="post"
  
```

Plain text content:

```

Total number of quarantined spam message(s):
%DIGEST_TOTAL_COUNT%
Release quarantined spam messages:
https://us.imhs-euq.trendmicro.com (username: %DIGEST_RCPT% )
Number of days to keep quarantined spam messages: 7

The following summary displays a maximum of 100 of the most recent
quarantined spam messages:
-----
Date:           From:           Subject:
  
```

FIGURE 3-24 Quarantine Settings for digest email message configuration

To configure the digest email message:

1. From the left menu, click **Quarantines > Settings**. The Quarantine Settings screen appears.
2. At the top right of the screen, click the **Disabled** icon to enable the spam digest feature. (It is disabled by default.)
3. Select the managed domain for which the digest email message will be created.
4. Select the frequency with which to send the quarantined messages digest:
 - Daily
 - On specified days. For example, select the check boxes for Monday, Wednesday and Friday on those days only.

Note: Quarantined email messages are retained for seven days.

5. Select a time and time zone for when to send the digest email message.
6. Set up the following for the digest email message:
 - **Sender's Email** — The email address that will appear in the “From” line in the digest email message
 - **Subject** — Text that will appear in the digest email message subject line
 - **HTML content** — Content that will appear if the email client of the end user allows HTML email messages (See [figure 3-26](#).)
 - **Plain text content** — Content that will appear if the email client of the end user allows only plain text email messages (See [figure 3-25](#).)
7. Optionally, right-click each field to display a popup menu from which to select available tokens. See the description of available tokens in [table 3-2](#).



Note: The domain used in the sender's email address must be the same as the domain to which the email will be delivered.

TABLE 3-2. Variables for digest email message template

FIELD	AVAILABLE TOKENS	WHEN THIS TOKEN IS USED. . .
Sender's Email	%DIGEST_RCPT%	Digest recipient's email address appears in the From: field of the received digest email message.
Subject	%DIGEST_RCPT%	Digest recipient's email address appears in the subject line
	%DIGEST_DATE%	Digest date appears in the subject line.
HTML Content	%DIGEST_RCPT%	Digest recipient's email address appears in HTML body of message
	%DIGEST_DATE%	Digest date appears in HTML body of message.
	%DIGEST_BODY_HTML%	Digest summary in HTML table format appears in HTML body of message
	%DIGEST_TOTAL_COUNT%	Total number of all currently quarantined messages appears in HTML body of digest email message.
	%DIGEST_PAGE_COUNT%	Total number of quarantined messages in listed digest summary (up to 100 maximum) appears in HTML body of digest email message.

TABLE 3-2. Variables for digest email message template (Continued)

FIELD	AVAILABLE TOKENS	WHEN THIS TOKEN IS USED. . .
Plain Text Content	%DIGEST_RCPT%	Digest recipient's email address appears in text body of message
	%DIGEST_DATE%	Digest date appears in text body of message.
	%DIGEST_BODY_TEXT%	Digest summary in plain text format appears in text body of message
	%DIGEST_TOTAL_COUNT%	Total number of all currently quarantined messages appears in plain text in the body of digest email message.
	%DIGEST_PAGE_COUNT%	Total number of quarantined messages listed in the digest summary (up to 100 maximum) appears in plain text body of digest email message.

8. Optionally, click the “Disabled” icon (**Disabled** ) next to “Inline Action” above the HTML content text box to enable inline action, as described in [Approving Messages or Senders From Within the Spam Digest Email \(Inline Action\)](#) on page 3-36. The icon changes to the “Enabled” icon (**Enabled** ) and the spam digest sent will contain radio buttons and Submit buttons by which the user can approve messages or senders directly from within the spam digest message.
9. Click **Save** to save your changes.

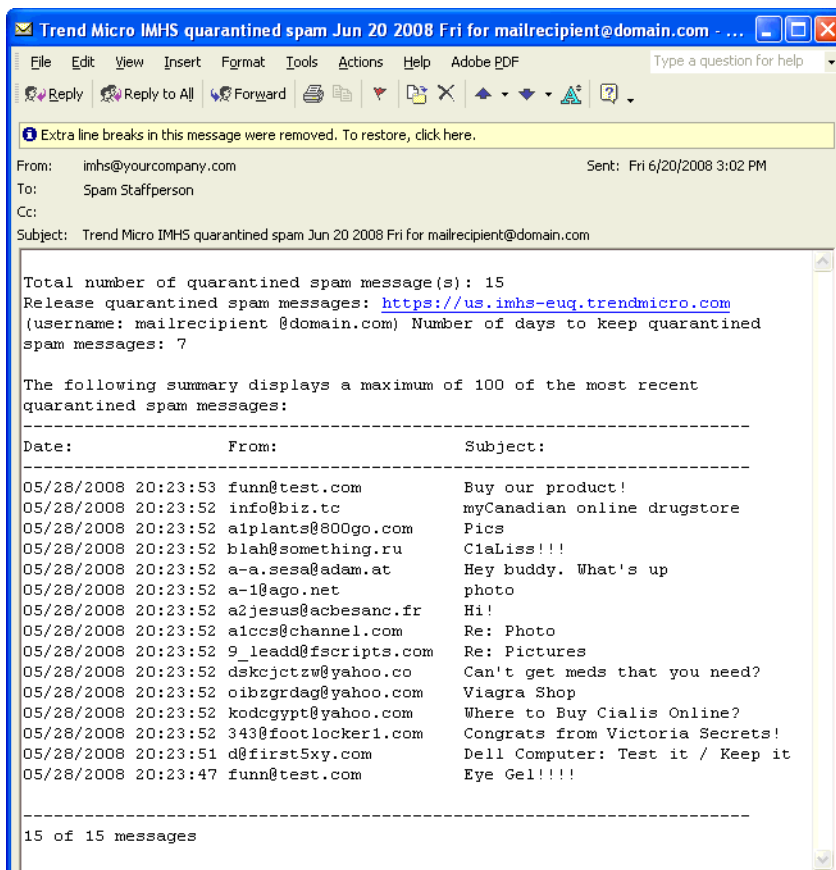


FIGURE 3-25 Sample of plain text spam digest email message

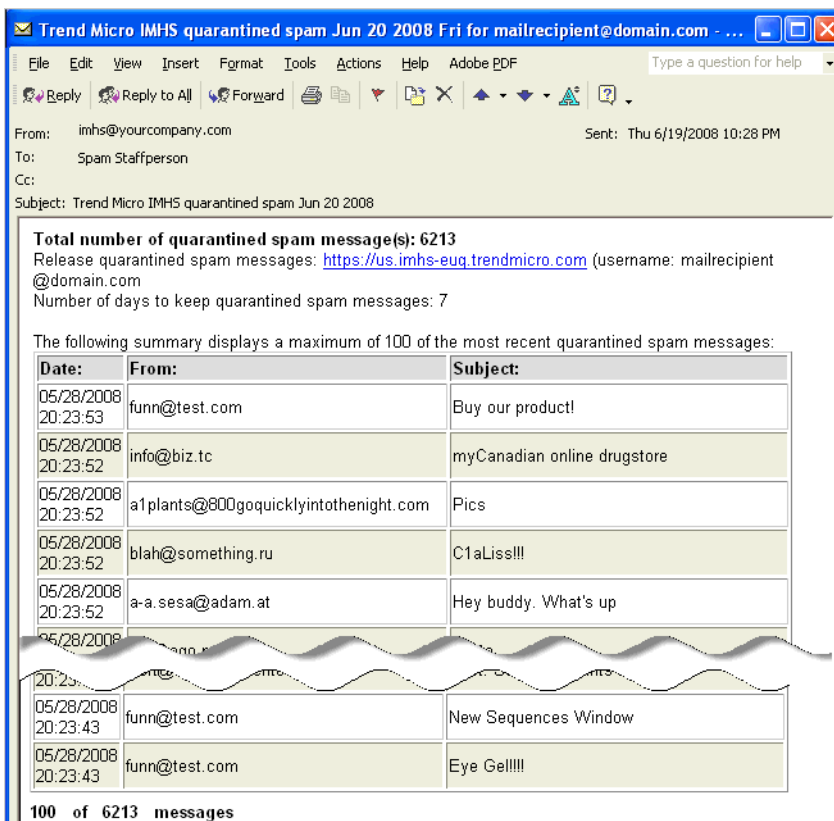


FIGURE 3-26 Sample HTML digest email message with inline action disabled (truncated for readability)

Using the Spam Digest Inline Action

Because it relieves you of the necessity of logging on to the End User Quarantine site, the spam digest inline action feature can save you time. There are a few points to keep in mind when using a mail client with this feature:

1. The spam digest inline action feature supports only client computers meeting the following system requirements:
 - Microsoft Office XP, service pack 3
 - Microsoft Outlook 2003 (SP3) or Outlook Express 6.0
2. Clicking the hyperlinked subject line of a message opens a browser window to the EUQ site login page.
3. Submitting a message with the “Not Spam” option simply releases that message from the quarantine. If the message violates more than one scanning policy, it is possible that, upon reprocessing, the message will trigger a policy other than the one that originally quarantined it and so will end up in the quarantine again.
4. Submitting a message with the “Approve Sender (Not Spam)” option both releases the individual message from quarantine and also adds the sender of the message to the approved senders list.
5. Once you have submitted a message for removal from the quarantine with “Not Spam,” if you later submit that same message but with the “Approved Sender (Not Spam)” option selected, IMHS will not add the sender to the approved sender list, because the message itself is no longer in the quarantine, and so IMHS has no way of identifying the sender. You will still see the response page message as before, however:

IMHS has received your request to revise the spam status of one or more messages or senders.
6. Finally, and most importantly:

WARNING! Anyone receiving this spam digest email message will be able to add any of these senders to your approved senders list. Therefore, Trend Micro advises against forwarding the spam digest email message.

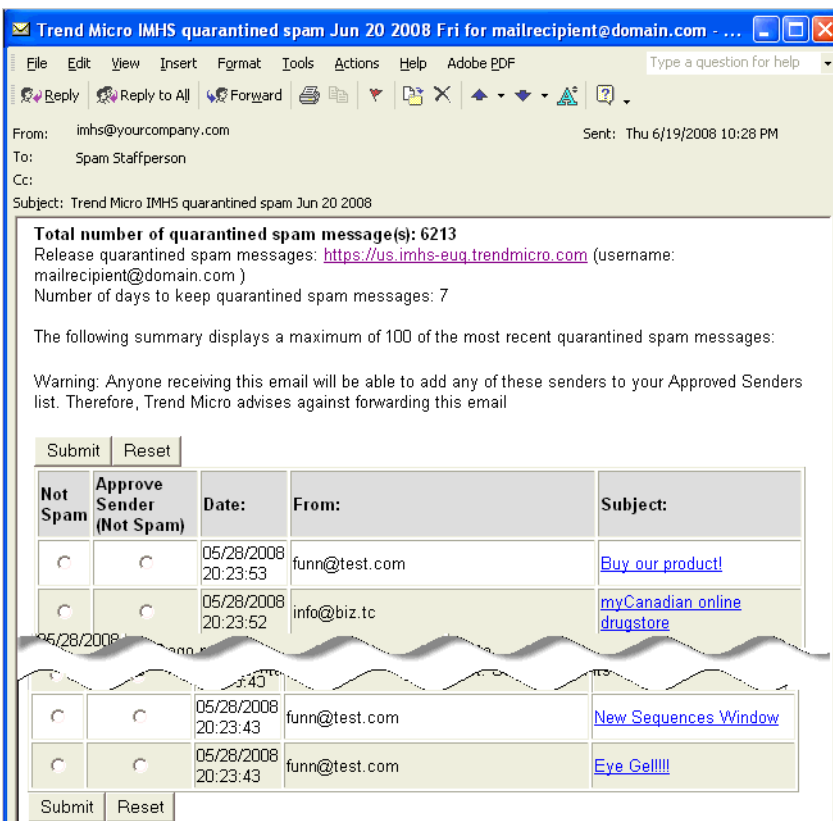


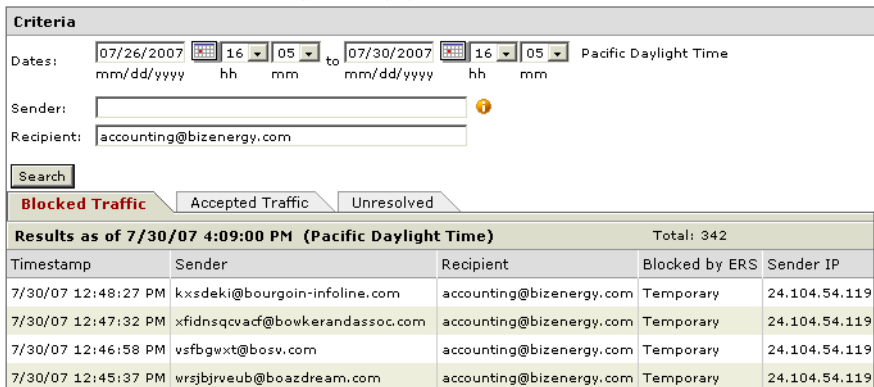
FIGURE 3-27 Sample HTML spam digest email message with inline action enabled (truncated for readability)

Logs

The Logs section allows you to search for and view mail tracking logs based on a specific date or date range, sender, and/or recipient. Mail tracking information is only available for the previous five days.

Mail Tracking - Inbound Traffic

Data collected within the last 2 hours may not be displayed.



Criteria

Dates: 07/26/2007 16 05 to 07/30/2007 16 05 Pacific Daylight Time
 mm/dd/yyyy hh mm mm/dd/yyyy hh mm

Sender:

Recipient:

Blocked Traffic Accepted Traffic Unresolved

Results as of 7/30/07 4:09:00 PM (Pacific Daylight Time) Total: 342

Timestamp	Sender	Recipient	Blocked by ERS	Sender IP
7/30/07 12:48:27 PM	kxsdeki@bourgoin-infoline.com	accounting@bizenergy.com	Temporary	24.104.54.119
7/30/07 12:47:32 PM	xfidnsqvacf@bowkerandassoc.com	accounting@bizenergy.com	Temporary	24.104.54.119
7/30/07 12:46:58 PM	yfbgwxt@bosv.com	accounting@bizenergy.com	Temporary	24.104.54.119
7/30/07 12:45:37 PM	wrsbjrveub@boazdream.com	accounting@bizenergy.com	Temporary	24.104.54.119

FIGURE 3-28 Mail Tracking log screen

Mail Tracking Details

The Mail Tracking feature allows the administrator to locate any message within the system using sender and recipient information. It shows the status and the action taken on the message such as:

- Blocked or delayed at the system edge by reputation service
- Accepted for processing and deleted with a virus
- Accepted, processed, and delivered
- Unresolved

InterScan Messaging Hosted Security

Powered By TREND MICRO

Logged on as **smartcustomer** | [Log Off](#) | [-----Help-----](#)

Logged on as **smart@yourcompany.com**

Mail Tracking Details

Timestamp: 7/28/07 11:35:24 PM

Sender: gekaudioacousticsdow@audioacoustics.com

Recipients: accounting@bizenergy.com
simon.ko@bizenergy.com
sysadmin@bizenergy.com

Subject: Customers alert, new pharma site is realised!

Message size: 2.31 KB

Sender IP: 79.8.126.148

Sender msg ID: <162864527.06730085931690@thhebat.net>

Actions:

- Receiving: Accepted from 79.8.126.148 - 7/28/07 11:35:24 PM
- Policy: Queued for policy evaluation
Quarantined (bizenergy: Spam or Phish)
- Delivery:

[Back to List](#)

FIGURE 3-29 Mail Tracking Details screen

The IMHS Mail Tracking Details screen (Figure 3-29) allows you to:

- View message details to confirm location
- Follow actions taken, policies applied, and message resolution
- Answer quickly the question, “What happened to my email?”

Administration

In the Administration section, you can do the following:

- [Changing the Admin Password](#) on page 3-48
- [Resetting an End-User Password](#) on page 3-48
- [Managing Directories](#) on page 3-49
- [Co-Branding](#) on page 3-53
- [Web Services](#) on page 3-56

Changing Passwords

Administrators can change the admin password, and they can also reset a forgotten password for an end user who needs to access the IMHS Web End-user Quarantine (EUQ) service.

All IMHS passwords require between eight and 32 characters. Trend Micro strongly recommends using passwords that contain multiple character types (a mix of letters, numbers, and other characters) that are not part of a recognizable format (for instance, do not use your birthday, license number, etc.)

The screenshot shows the 'Change Admin Password' interface. At the top, it says 'InterScan Messaging Hosted Security' with the Trend Micro logo. Below that, it indicates 'Powered By TREND MICRO' and 'Logged on as smartcustomer'. A 'Log Off' link and a help dropdown are also visible. The user is logged in as 'smart@yourcompany.com'. The left sidebar lists navigation options: Report, Policy, Approved Senders, Quarantines, Logs, and Administration (expanded). Under Administration, 'Admin Password' is selected. The main form contains three input fields for 'Old password:', 'New password:', and 'Confirm password:'. A note states: 'Note - Passwords must be between 8-32 alphanumeric characters.' At the bottom of the form are 'Save' and 'Cancel' buttons.

FIGURE 3-30 Change Admin Password Screen

Changing the Admin Password

To change the admin password:

1. Go to **Administration > Admin Password**.
2. Type your current/old password.
3. Type your new password.
4. Confirm your new password.
5. Click **Save**.

Resetting an End-User Password

System administrators can reset an end user's forgotten password.

To reset an end-user password:

1. Click **Administration > End-user Password**.

The screenshot shows a web form titled "Change End User Password". At the top right of the form is a blue question mark icon. Below the title bar, there are two input fields: "Registered end-user email address" and "Domain name". The "Domain name" dropdown menu is currently set to "bizenergy.com". Below these fields are two more input fields: "New password" and "Confirm password". A note below the password fields states: "Note - Passwords must be between 8-32 alphanumeric characters." At the bottom of the form are two buttons: "Save" and "Cancel".

FIGURE 3-31 Change end-user password

2. Type the end user's email address.
3. Type and confirm a new password.

Note: The end user will need to know the new password to log in.

4. The end user will receive an email with an activation URL.
The end user will need to click on the activation URL and then enter the appropriate email address and new password in the IMHS Web EUQ login screen.

Managing Directories

IMHS uses user directories to help prevent backscatter (or “outscatter”) spam and Directory Harvest Attacks (DHA). You can import user directories to let IMHS know legitimate email addresses and domains in your organization. IMHS only recognizes ANSI-encoded LDAP Data Interchange Format (LDIF: .ldf) and ANSI or UTF-8-encoded comma-separated values (CSV: .csv) files.

The Directory Management (Administration > Directory Management) screen shows the following sections:

- **Import User Directory section**—Fields for importing a new user directory file.

- **Imported User Directories**—The current user directory file(s) that IMHS is using. IMHS replaces one mail domain user at a time. Users may be a combination of multiple user directories.

Directory Management Notes

Before you import an LDIF or CSV directory file, note the following:

- You can only see the directories that are associated with your administrator account. If you are sharing your IMHS service with another administrator, that administrator will not see the directories for that account upon login.
- Every time you add more users to your network, you must import your updated user directories; otherwise, IMHS will reject email from newly added users.
- Do not include blank lines or other irrelevant data in the file that you import. Use caution when creating a file.
- Every time you import a directory file, it overwrites the old directory file.

However, if you import an updated user directory file that does not have any information for one of your domains, the entries for those domains remain the same for IMHS; they are not overwritten.

WARNING! Use caution when importing a directory file. If you import an updated directory file that has information for one of your domains, all entries for those domains are overwritten.

Exporting a User Directory File

First, export your directories from your system. Trend Micro recommends using the LDIFDE tool to create an LDIF file. For instructions on using the LDIFDE tool and creating the file, go to the following link at the Microsoft Web site:

<http://support.microsoft.com/kb/237677>

Importing a User Directory File

WARNING! Trend Micro strongly suggests that you do not import more than 24 directories in a day. Doing so could overwhelm system resources.

To import a user directory file:

1. Click **Administration > Directory Management**. The Directory Management screen displays.

The screenshot shows the 'Directory Management' window. The 'Import User Directory' section has the following fields:

- Format*:** A dropdown menu with 'LDIF' selected.
- Name*:** An empty text input field.
- File location*:** An empty text input field with a 'Browse...' button to its right.

Below these fields are two buttons: 'Verify File' and 'Reset'.

The 'Imported User Directories' section is currently disabled, as indicated by a 'Disabled' label and a red 'X' icon. It shows a dropdown menu with '*@testing.com' selected and an 'Export to CSV' button.



Name	Filename	Type	Date Imported

FIGURE 3-32 Directory management




2. From the **Format** drop-down list, select the format type:
 - **LDIF**
 - **CSV**
3. In the **Name** field, type a descriptive name for the file.
4. In the **File location** field, type the file directory path and file name or click **Browse** and select the .ldf or .csv file on your computer.
5. Click **Verify File**. After the progress bar completes, a summary screen appears showing the following:
 - **Summary**—A summary of the information above.
 - **Domains and Number of Current Users to Replace Current Users**—The domains that you specified when you subscribed to the IMHS service.
 - **Invalid domains**—Domains that are included in your directory file, but are not officially used on your IMHS service. IMHS cannot provide service for these domains and their corresponding email addresses.
6. Click **Import**.

Verifying Your User Directory

If you are uncertain which domains in the user directories are going to be active for your service, you can temporarily disable the directories, import the new file, export the directories to a CSV file, and view them without the directories' being "live." When you are confident that the user directories are correct, you can re-enable them.

Note: The directories in the file are enabled by default. When enabled, a green check mark icon appears in the **Imported User Directory** table: . When disabled, a red X icon appears: . IMHS takes up to five (5) minutes to enable or disable the directories.

To verify user directories:



1. Disable the directories by clicking the "enabled" icon (). The check box turns into a "disabled" red X icon () and the word **Disabled** appears.
2. Import the directory file (see [To import a user directory file](#): on page 3-51).
3. Select the domain to verify.
4. Click **Export** and save the directory file locally (in CSV format).
5. Open the directory file in an application that reads CSV files.
6. Verify that the directory information is correct.
7. Re-enable the directories by clicking the "disabled" icon (.

Co-Branding

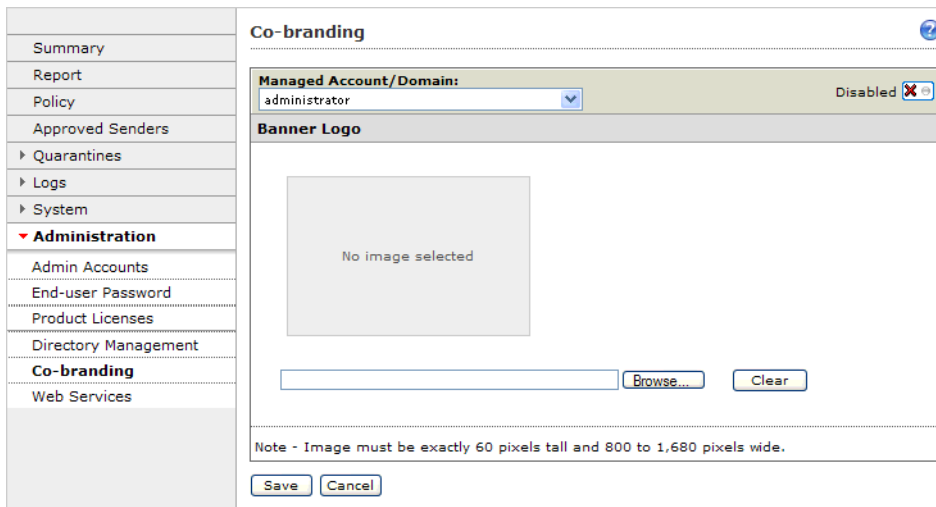
IMHS allows you to display your company logo on the banner bar of the login page. The logo that you choose to display in the IMHS top banner for your domain will also display in the banner of the IMHS Web EUQ.

Users at the reseller level may set different domains with the same logo, different logos, or allow the domain administrators to set the logo to be displayed for their domain. Resellers can also leave the feature disabled.


To display your logo:

1. Verify that your logo image meets the following requirements:
 - **Image height:** Exactly 60 pixels (no taller or shorter)
 - **Image width:** 800 – 1680 pixels
 - **Image file format:** .gif, .jpg, .or .png
2. Go to **Administration > Co-branding** as shown in [figure 3-33](#).
3. Click the icon (**Disabled** ) in the upper right corner to enable the feature. The icon changes to its enabled form (**Enabled** ).

It is disabled by default.



Co-branding

Managed Account/Domain: administrator Disabled 

Banner Logo

No image selected

Note - Image must be exactly 60 pixels tall and 800 to 1,680 pixels wide.

FIGURE 3-33 Co-branding screen

4. From the Managed Account/Domain drop-down list, select the account or domain that will display the logo.
5. Click **Browse**, and browse to the location of the your logo file. Click **Open** and a preview of the logo displays as shown in [figure 3-34](#).



The screenshot shows a web-based configuration window titled "Co-branding". At the top, there is a "Managed Account/Domain:" dropdown menu with "administrator" selected and a "Disabled" status indicator. Below this is a "Banner Logo" section. It features a preview of a banner logo with the text "The ABCD Company" in a blue, italicized font, set against an orange background with a small graphic of four colored circles (red, yellow, green, blue). Below the preview is a text input field and a "Browse..." button. To the right of the input field is a "Clear" button. At the bottom of the window, there is a note: "Note - Image must be exactly 60 pixels tall and 800 to 1,680 pixels wide." and two buttons: "Save" and "Cancel".

FIGURE 3-34 Display of domain logo to be set

6. Click **Save**. The logo image will display in two places:
 - The banner bar of the IMHS login page (see [figure 3-35](#))
 - The banner bar of the IMHS Web EUQ login page (see [figure 3-36](#))

Note: Resellers can set different logos for different domains or allow system administrators of the domain to set the logo for that domain, separately from the reseller logo. The logo selected for a domain will also display in the banner bar of the IMHS Web EUQ associated with that domain.

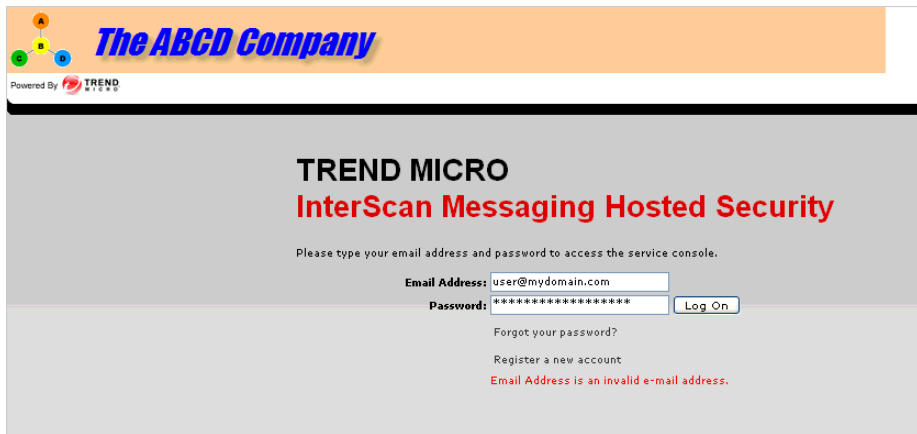


FIGURE 3-35 Sample reseller logo set in banner bar on login page of IMHS

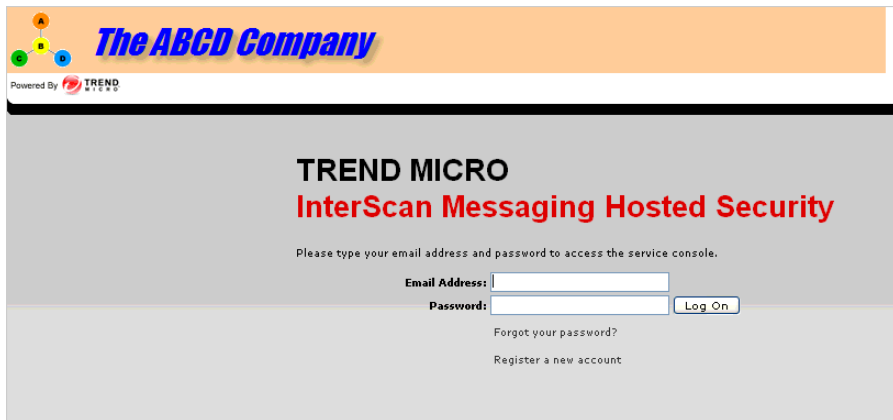


FIGURE 3-36 Domain logo displays in banner bar of login page of IMHS Web EUQ

7. To cancel the operation, click **Cancel**.
8. To remove the logo, click **Clear**.

Web Services

IMHS allows you to access IMHS Web Services applications through an installed IMHS Web Service client in your environment.

There are three steps you need to take before accessing IMHS Web Services applications. First, you need an APIKEY. APIKEY is the global unique identifier for your Web Service client to authenticate its access to IMHS Web Services. Second, you need to enable the IMHS Web Services. Third, you should select and install the Web Service client program in your environment.

To prepare your Web Services environment:

1. Click **Administration > Web Services**

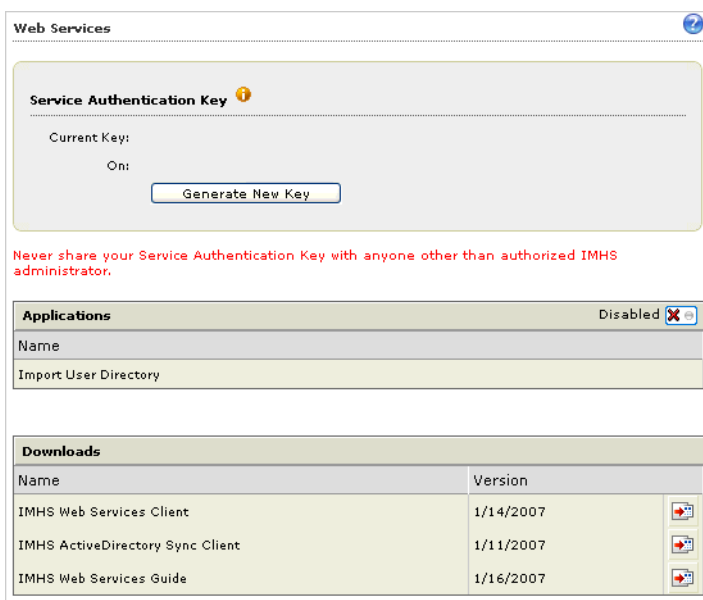
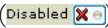




FIGURE 3-37 Web Services screen

2. Make sure an APIKEY is available. Current Key displays the APIKEY that the Web service client program should use. If you generate a new key, you must update your client program to use the new key. The APIKEY is like a password for your client to communicate with IMHS Web services. Please keep the key private to authorized IMHS administrators only.
 - If **Current Key** is blank, click Generate New Key to generate an APIKEY.
3. Click the “disabled” icon () in the right corner to enable () the feature.

It is disabled by default.
4. From the **Downloads** list, select the IMHS Web service client program to download. Click the download icon () to download the client.
5. Save the client on your local drive.
6. Follow the client installation steps to install the client.

Web End-User Quarantine

IMHS Web End-User Quarantine (EUQ) allows end users to:

- Create a new account
- Configure quarantine spam actions and an approved senders list
- Change passwords

End users can access the IMHS Web EUQ at the following URL:

<https://us.imhs-euq.trendmicro.com/>

More information about IMHS Web EUQ is available in [Introducing Web EUQ](#) on page C-1, the Web EUQ online help or in the *IMHS Web EUQ End-User Guide*.

End-User Password Reset

System email administrators can advise end users who have lost their password that they can use the [Forgot Password](#) link on the IMHS Web EUQ page to reset a password. For end users to successfully reset their passwords, they must answer the security question that they chose when creating the account.

If users cannot remember the security question, system email administrators can reset end-user passwords. When a system email administrator resets an end user's password, it

automatically activates the account. If an end user resets the password, he or she will receive an authentication email almost immediately that will enable login to Web EUQ.

Disabling InterScan Messaging Hosted Security

To disable InterScan Messaging Hosted Security, you need to follow the same process used when initiating the service and redirect your MX record to route all inbound SMTP traffic to your own mail server.

Changing Your MX Record

The Mail eXchange (MX) record determines the message routing for all email sent to your domain. To route messages destined for your domain so they no longer pass through the IMHS system, you must redirect your MX record. Your MX record is part of your DNS record. You will need to know the IP address for your inbound mail server.

The actual redirection of the MX record involves simply changing the IP address for all inbound SMTP traffic. This is either accomplished manually (smaller accounts) or through a support technician.

If you are unsure how to configure the MX records for your domain, contact your Internet Service Provider's (ISP) help desk or your Domain Name Service (DNS) technician for assistance.

Note: The full transition (DNS propagation) may take up to 48 hours. If you plan to no longer use InterScan Messaging Hosted Security, please let the IMHS Support team know and they will continue to pass your mail through the system without processing. This will ensure that you do not lose any messages while the DNS propagation takes place.



Frequently Asked Questions (FAQs)

The following FAQs apply to the current version of IMHS

Question 1: What is Trend Micro InterScan Messaging Hosted Security?

Answer: Trend Micro InterScan Messaging Hosted Security is a hosted email security service that can benefit any size organization. We provide the hardware, software, and messaging expertise to cleanse your email of spam, viruses, worms, Trojans, and phishing (identity theft) attacks. The cleaned mail stream is sent directly to your mail server for final delivery to your end users.

Question 2: What are the advantages of a hosted email security service?

Answer: As a hosted, off-site service, IMHS can stop attacks before they get a chance to reach your network. In addition to stopping spam, viruses, worm, Trojans, and other malware, IMHS can protect your network from attacks that:

- Attempt to block your Internet connection (Denial of Service)
- Steal your email addresses for spammers (Directory Harvest Attacks)

Question 3: Do I need to buy/upgrade any hardware or software?

IMHS is a hosted service, and there is no need to buy additional hardware or software. The service is managed by security professionals, relieving your IT staff of the burden of installing, maintaining, and fine-tuning a complex email security system.

Question 4: How much does the service cost?

Answer: Trend Micro InterScan Messaging Hosted Security is priced on a per user basis under an annual contract. The cost per user drops as the number of users increases. There is no set-up fee, or additional support costs from Trend Micro. Although unlikely, your Web-hosting company may charge a small fee for changing your MX record. Contact your Web-hosting service to review their pricing policies.

Question 5: How confidential is this service? I don't want anyone reading my email.

Answer: All messages are processed automatically and transparently. Many messages are rejected before they are even received based on the reputation of the IP that is attempting to send the message. Messages that are received are processed through a multi-layered spam and virus filtering system that does not include any human intervention. Messages are never stored unless your mail server becomes unavailable.

Question 6: Why should I trust Trend Micro with my email?

Answer: Trend Micro has been a recognized leader in threat management with over 10 years of experience in messaging and spam prevention and more than 16 years' experience in providing leading anti-virus solutions. Trend Micro has held #1 market share as a provider of Internet gateway solutions for the past six years and #1 market share in the mail server antivirus market for the past 4 years. We know and understand the issues involved in securing networks from all types of threats, both email-borne and non-email related. A secure messaging gateway is one component of a comprehensive network security solution.

Question 7: What do I need in order to use this service?

Answer: To use this service you only need to have an existing Internet gateway or workgroup email connection and a Web browser for accessing the online reporting and administrative console.

Question 8: How do I begin using the service? Do I need to install, configure, or maintain anything?

Answer: A simple redirection of your Mail eXchange (MX) record is all that is needed to start the service. Your email is processed by the Trend Micro InterScan Messaging Hosted Security to remove spam, viruses, worms, Trojans, and phishing attacks; the clean messages are then sent directly to your mail server.

Question 9: How do I redirect my email/mail exchange record?

Answer: If you manage your own DNS, you can easily redirect your MX record. If your DNS is managed by a third-party or ISP, either they can do this for you or they may have a simple Web interface allowing you to make the change yourself. It can take up to 48 hours for any changes to propagate throughout the system.

Question 10: Can I try the service on a limited number of users?

Answer: We recommend that you use a test domain for trial purposes. Doing so enables you to experience the service and test how it functions for different types of users.

Question 11: Will delivery of my email be delayed as a result of this service?

Answer: The time required to process each message is measured in milliseconds. Any delay in the delivery of your messages is negligible and will not be noticed by the end user.

Question 12: Do you store/archive email?

Answer: IMHS does not store or archive email by default. All messages are processed and immediately passed through to the customer's MTA. Messages are not spooled or stored in memory unless your mail server becomes unavailable. However, if you create a policy to quarantine messages (spam for example) these email messages will be stored at our data center for up to seven days.

Question 13: What happens to my messages if my mail server is unavailable for a period of time? Do you provide any solution towards disaster recovery?

Answer: If your mail server becomes unavailable for whatever reason, your message stream is automatically queued for up to five days or until such time that your server comes back online. You will not lose any of your valuable email due to hardware or software failure, power outages, network failure, or simple human error.


Question 14: Where does my outgoing email go?

Answer: By default, your outbound email stream is handled directly by your own mail server and is passed out to other networks as it is currently handled. However, at the IMHS Advanced level of service, you can choose to redirect your outbound email traffic through IMHS services. When you activate IMHS services, you will be informed of what mail server to send your outbound messages to if you choose to utilize IMHS outbound filtering. Contact imhs_support@trendmicro.com to request outbound filtering service. Our support specialist will make changes to allow your outbound mail stream to go through IMHS outbound filtering. You will be informed when IMHS is ready. At that

time, simply redirect your outbound email messages to the IMHS outbound email servers as instructed.

Question 15: Is there an SLA?

Answer: Trend Micro provides an aggressive Service Level Agreement (SLA) for InterScan Messaging Hosted Security that guarantees that organizations receive secure, uninterrupted email. Please contact Trend Micro for specific service-level guarantees included in the latest version of the SLA.



Appendix B

Contact Information and Web-Based Resources

This chapter provides information to optimize the InterScan™ Messaging Hosted Security performance and get further assistance with any technical support questions that you may have.

Topics in this chapter include:

- [Contacting Technical Support](#) on page B-2
- [Security Information Center](#) on page B-7
- [Supported Performance Levels](#) on page B-3
- [Sending Suspicious Code to Trend Micro](#) on page B-4
- [TrendLabs](#) on page B-6

Contacting Technical Support

Trend Micro offers online help for IMHS accounts through the administrative graphical user interface (GUI).

The very latest technical support contact information can always be found here:

<http://us.trendmicro.com/us/products/enterprise/interscan-messaging-hosted-security/support/index.html>

In addition, free support assistance for setup, configuration, and service usability is available as listed below.

In the United States, Trend Micro representatives can be reached by phone or email. You can also search our Knowledge Base at the following location:

<http://esupport.trendmicro.com/support/enterprise/search.do>

Email Support

Support Hours: 24 x 7

imhs_support@trendmicro.com

Please provide the following in your correspondence:

- Company name
- Administrator account name (only the account user name; do not send your password in an email)
- Contact information:
 - Name
 - Email address (if different)
- A brief description of your issue

Worry Free Business Security with IMHS

<http://us.trendmicro.com/us/products/enterprise/network-reputation-services/support/index.html>

General Contact Information

General US phone and fax numbers follow:

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Our US headquarters is located in the heart of Silicon Valley:

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014

Supported Performance Levels

Trend Micro provides the following levels of performance for IMHS.

Service Availability

Scheduled downtime for ongoing maintenance may occur from time to time with at least 24 hours written notification provided. In the event of unscheduled downtime, no less than 99.99 percent availability is guaranteed on an annual basis.

Email Delivery

Delivery is guaranteed even when your mail server is temporarily unavailable. The service continues to scan and process email in the event of downstream disaster recovery with valid messages stored for up to five days, depending on volume. Once your local email servers are available, email is delivered with intelligent flow control to ensure downstream manageability, avoiding unnecessary flooding of downstream resources.

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do to. New solutions are added daily.

Also available in Knowledge Base are product FAQs, hot tips, preventive antivirus advice, and regional contact information for support and sales.

<http://esupport.trendmicro.com/>

And, in case if you cannot find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question in an email message. Response time is typically 24 hours or less.

Sending Suspicious Code to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

<http://subwiz.trendmicro.com/SubWiz>

Click the **Submit a suspicious file/undetected virus** link.

TREND MICRO

United States/Canada Search

日本語 繁体中文 简体中文

Home Products & Services Purchase **Support** Security Info Partners About Us

Home > Support > Submission Wizard >

Submission Wizard

Trend Micro Submission Wizard is a FREE anti-virus service where people can request assistance from security experts or learn more about viruses and security threats.

Are you a Premium Support Customer or a regular Trend Micro Customer?

Submission Wizard cases need longer processing time than Premium Support or standard support cases.

Therefore, if you are a Premium Support Customer, submit virus cases through [Premium Support Online](#) for faster service. Non-Premium Trend Micro customers should contact their local [technical support representatives](#).

Submit a Sample

Suspicious file
Send us your suspicious files for analysis.

Spam Mail
Send us your spam mail to help improve our anti-spam solution.

Learn More

Pattern File
Download the latest pattern files.

Virus Description
Read up-to-date information on new viruses.

Virus Behavior
Verify a possible virus behavior or characteristic.

Help Yourself

Manual Removal Instruction
Clean an infected PC on your own

Manual Removal Problem
Report any issues with our manual removal instructions.

Others
Report other anti-virus concerns

Other Resources

[Virus Encyclopedia](#)
[Knowledge Base](#)
[Update Center](#)

Copyright (c) 1989-2005 Trend Micro Incorporated. All rights reserved. [Legal Notice](#) | [Privacy Policy](#) | [Contact Us](#) | [Site Map](#)

FIGURE B-1 Submission Wizard screen

You are prompted to supply the following information:

- **Email:** Your email address where you would like to receive a response from the antivirus team.
- **Product:** The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Number of Infected Seats:** The number of users in your organization that are infected.
- **Upload File:** Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word “virus” as the password—then select the protected zip file in the **Upload File** field.
- **Description:** Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will “dissect” the file to identify and characterize any risks it may contain and return the cleaned file to you, usually within 48 hours.

Note: Submissions made through the Submission Wizard/Virus Doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you click **Next**, an acknowledgement screen displays. This screen also displays a Tracking Number for the problem you submitted.

If you prefer to communicate by email, send a query to the following address:

virusresponse@trendmicro.com

In the United States, you can also call the following toll-free telephone number:

(877) TRENDAY, or 877-873-6328

TrendLabs

TrendLabs is Trend Micro’s global infrastructure of antivirus research and product support centers that provide customers with up-to-the minute security information.

The “virus doctors” at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging risks. The daily

culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA.

Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

<http://www.trendmicro.com/vinfo/>

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of risks expected to trigger in the current week, and describes the 10 most prevalent risks around the globe for the current week
- Consult the Virus Encyclopedia, a compilation of known risks including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the risk, as well as information about computer hoaxes
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
 - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other risks
 - The Trend Micro *Safe Computing Guide*
 - A description of risk ratings to help you understand the damage potential for a risk rated Very Low or Low as opposed to Medium or High.
 - A glossary of virus and other security risk terminology
 - Download comprehensive industry white papers

Security Information

No Malware Alert
There are no medium or high risk alerts at this time.

Recent Updates
Virus Pattern File Jan 29
[4,969.00](#)
Scan Engine 8.500

[> Visit the Update Center](#)

Malware Advisories
**Spyware/
Grayware**
Security Advisories

MALWARE NAME	RISK RATING	ADVISORY DATE	PATTERN FILE
■ WORM_ONLINEG.DJO	Low	Jan 30, 2008	4.969.00
■ WORM_IRCBOT.SN	Low	Jan 26, 2008	4.957.00
■ WORM_AGENT.TBH	Low	Jan 25, 2008	4.579.00
■ SYMBOS_BESELO.A	Low	Jan 23, 2008	4.961.00
■ WORM_IMBOT.AC	Low	Jan 22, 2008	4.961.00
■ BKDR_IRCBOT.RB	Low	Jan 22, 2008	4.957.00
■ HTML_IFRAME.IY	Low	Jan 18, 2008	4.949.00
■ WORM_NUWAR.BK	Low	Jan 15, 2008	4.967.00
■ TROJ_AGENT.HJS	Low	Jan 13, 2008	4.957.00
■ TROJ_DROPPER.NH	Low	Jan 13, 2008	4.943.00

[> See all Malware Advisories](#)

FIGURE B-2 Trend Micro Security Information screen

- Subscribe, for free, to the Trend Micro Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Webmasters

Appendix C

Introducing Web EUQ

InterScan Messaging Hosted Security (IMHS) Web End-user Quarantine (Web EUQ) is a user interface that helps end users manage spam email messages held in quarantine. End users can also set up a list of approved email senders whose messages should be delivered, not quarantined. It is easy to use, as shown in [Figure C-1](#).

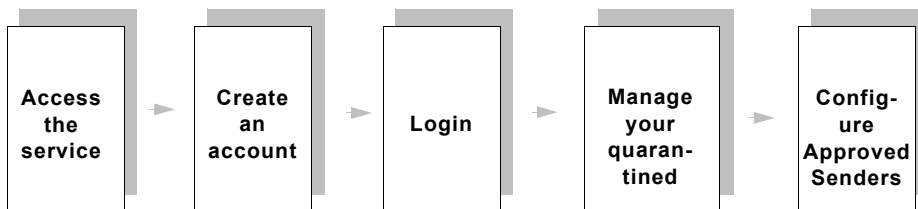


FIGURE C-1 Getting Started with IMHS Web EUQ

Accessing the Web EUQ Service

Accessing the Web EUQ Service requires Internet access and one of the following browsers:

- Microsoft® Internet Explorer®, minimal version 6.0
- Mozilla™ FireFox™, minimal version 2.0

To access the service:

1. Open your browser.
2. Go to the URL provided by your system email administrator.

Creating an Account

In order to use Web EUQ, you must have an account.

To register a new account:

1. Access the service.
2. Click the **Register a new account** link on the login page shown in [Figure C-2](#).

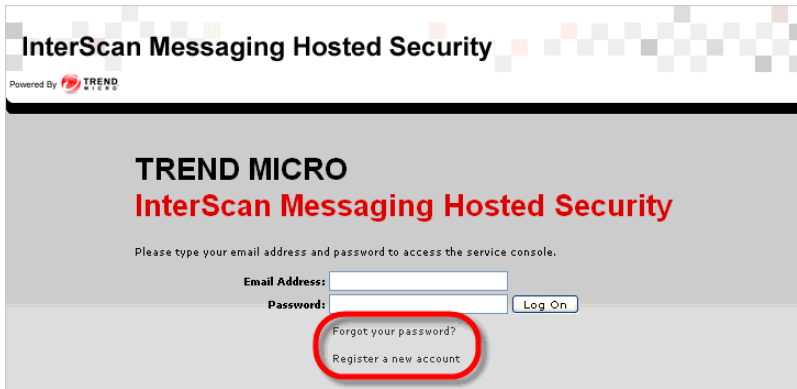


FIGURE C-2 IMHS Web EUQ Login screen

3. Type your last name and first name in the Personal Information fields shown in Figure C-3.

InterScan Messaging Hosted Security
Powered By TREND MICRO

Create a New Account [Help](#)

1. Personal Information
Last Name*:
First Name*:

2. Log-In Information
E-Mail Address*:
Confirm E-Mail Address*:

3. Password
Password*:
Confirm Password*:

4. Security Question
Security Question*: What's your mother's maiden name?
Answer*:

5. Verification
Image Text*:

FIGURE C-3 Create a new account

4. Type and confirm your email address in the Log-in Information fields.
5. Type and re-type the password to be associated with the new account.
6. Select a security question and type the answer.
7. Type the text displayed in the image.
8. Click **Finish**.

When your information is successfully authenticated, you will receive an email with an activation URL. Click on the URL to activate your new password. Log on to the Web EUQ console with the password that you chose in [Step 5](#).

Logging into IMHS Web EUQ

After creating a new account, you will receive an email message notifying you that your information has been authenticated and that your account has been created.

To log on to Web EUQ for the first time:

1. Open the email that you received that verifies your account was created.
2. Click on the activation URL link.
You will see the Web EUQ login screen shown in [Figure C-2](#).
3. Type the email address that you used when setting up the account.
4. Type the password that you selected when creating the account.
5. Click **Log On**.

Working with Quarantined Spam

The Quarantined Spam screen is the first screen you see when you log on to IMHS Web EUQ. On this screen you can:

- View and sort a list of quarantined messages that were prevented from reaching your email In-box
- Perform one of three optional actions on your quarantined message(s):
 - Delete
 - Deliver (Not Spam)
 - Deliver & Approve Sender

The Quarantined Spam screen displays the number of currently approved sender addresses above the table. See [Using the Approved Senders Screen](#) on page C-6 to learn how to add or edit Approved Sender addresses.

InterScan Messaging Hosted Security

Powered By TREND MICRO | Logged on as **smartcustomer** | Log Off |Help|.....

Logged on as **smart@yourcompany.com** [Help](#)

Quarantined Spam

Approved Senders

Password

Approved Senders: 1 of max. 50
(Note: Messages will be deleted automatically after 7 days.) [Refresh](#)

Delete
 Deliver (Not Spam)
 Deliver & Approve Sender
 11 - 20 of 39 | 4 | page 2 | of 4 | 4

<input type="checkbox"/>	Date ▼	Sender	Subject
<input type="checkbox"/>	04/02/2007 10:36:47	lazboeingstorezen@boeingstore.com	Check out the wonders of pound melting
<input type="checkbox"/>	04/02/2007 07:50:05	lazboeselcanyonhousesen@boeselcanyonhouse.com	Look in the mirror and enjoy the new you
<input type="checkbox"/>	04/02/2007 01:07:53	lazbodylickersen@bodylicker.de	Getting thinner can be enjoyable
<input type="checkbox"/>	04/01/2007 21:43:47	qcoyulx@masfm.com	Re: battlefield threonine
<input type="checkbox"/>	04/01/2007 17:51:07	jewbluechipfeedgox@bluechipfeed.com	Getting thinner can be enjoyable
<input type="checkbox"/>	04/01/2007 12:17:16	accounting@bizenergy.com	And on thee most high priest answered and When
<input type="checkbox"/>	04/01/2007 05:09:46	eblueothij@rxsol.com	Tell me if it is right
<input type="checkbox"/>	04/01/2007 04:06:50	feedhouse@pacificvalleyfoods.com	alone
<input type="checkbox"/>	04/01/2007 03:16:16	jewbluedoggox@bluedog.net	Make yourself more attractive to others
<input type="checkbox"/>	04/01/2007 02:49:30	willard@gologos.com	Re:

Delete
 Deliver (Not Spam)
 Deliver & Approve Sender
 11 - 20 of 39 | 4 | page 2 | of 4 | 4


Rows per page 10

FIGURE C-4 Quarantined Spam screen

To view and sort quarantined items in the table:

- Optionally, toggle the number of message entries displayed (10, 25, 50, 100, 250, 500) using the drop-down list at the bottom right of the table.
- Navigate through the message entries by clicking on the images in the right side of the heading row:
 - < first page
 - < back one page
 - > forward one page
 - > last page
- Sort message entries by ascending or descending order in the following categories:
 - Time and date received (mm/dd/yy, hh:mm:ss)
 - Sender address
 - Subject

To perform one of three actions for quarantined item(s):

1. Select the message(s) in question by doing one of the following:
 - Select the check boxes to the left of each individual entry
 - Select the check box to the left of “Date” column heading to select all messages on the currently visible page
2. Select an action to be performed:
 - **Delete** (

Note: Trend Micro IMHS maintains up to seven days of quarantined messages, which would be subsequently deleted.

Using the Approved Senders Screen

On the Approved Senders screen you can:

- Display a list of the existing approved senders and sort them by date approved or by sender address.
- Approve specific addresses or domains to send email to your email address
- Delete existing approved sender addresses or domains
- Edit existing approved sender addresses or domains

When using the Approved Senders screen, the following conditions apply:

- IMHS will contain no more than 50 approved senders on the list.
- Email Reputation Services (ERS) will not block any email messages from the senders (or domains) specified.
- Content-based heuristic spam rules will not apply to email message received from the specified senders or domains.

- All virus, content-based, and attachment rules set by your administrator will still apply.

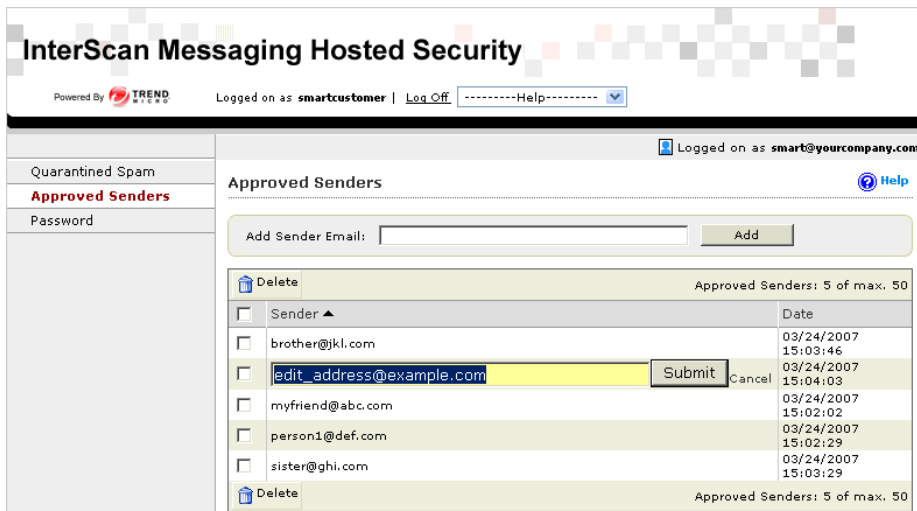


FIGURE C-5 Editing an address in the Approved Senders screen

Sorting Message Entries

You can view existing approved senders in ascending or descending order by:

- Time and date approved (mm/dd/yy, hh:mm:ss)
- Sender address

Adding or Editing Approved Senders

To add an approved sender:

1. Type a single address or domain in the **Add** field.
 - For a single address, use the following pattern: name@example.com
 - For a domain, use the following pattern: *@example.com

Note: The asterisk wildcard character is accepted only in the position preceding the “@” sign. The above two examples are the only formats allowed for an approved sender. *@* or other variable address formats are not accepted.

2. Click **Add**.

To edit existing Approved Senders addresses or domains:

1. Click on the link of the email address to be changed.
It becomes an editable field.
2. Edit the address or domain.
3. Click **Submit** to save the edited address or domain.

Changing Your Password

Trend Micro recommends changing the password regularly. In addition, IMHS Web EUQ requires a password between 4 and 32 characters.

Web EUQ offers two ways to change your password:

- [To change your password if you know your password:](#)
- [To reset your password:](#)

To change your password if you know your password:

1. Click **Password** in the left menu.
2. Type your current and old password.

Note: Trend Micro strongly recommends using passwords that contain multiple character types (a mix of letters, numbers, and special characters).

3. Type and confirm your new password.
4. Click **Save**.

To reset your Web EUQ password, you must remember the security question you chose when creating your account. If you don't know the question and answer, your system email administrator can reset your password for you.

To reset your password:

1. Go to the **Login screen** and click the **Forgot your password?** link.

The screen shown in [Figure C-6](#) appears.

InterScan Messaging Hosted Security
Powered By **TREND**
MICRO

Reset Password Request [Help](#)

1. Log-In Information
E-Mail Address*:

2. Password
New Password*:
Confirm Password*:

3. Security Question
Security Question*: What's your mother's maiden name?
Answer*:

4. Verification
Image Text*:

FIGURE C-6 Reset Password Request screen

2. Type your email address.

Note: The email address must match the contact email address that you entered when you activated the service.

3. Type the new password you prefer and confirm it.
4. Select the security question that you selected when you created your account.
5. Type the answer to the security question.
6. Type the text shown in the CAPTCHA image.

7. Click **Finish**. When your information is successfully authenticated, you will receive an email message containing an activation URL.
8. Click on the activation URL in the email message. IMHS Web EUQ activates your new password.
9. Log in to the Web EUQ console using the password that you chose in [Step 3](#).

Note: If your information cannot be authenticated, the password will not be reset. If you forgot your original email address or security question, please contact your system administrator. Your system administrator can reset your password for you.

Index

A

- accepted messages 2-14
- Accepted Size report 2-16
 - Not Quarantined field 2-16
 - Quarantined field 2-16
 - Total Size field 2-16
- activate the Email Encryption service 2-8
- activating Email Encryption service 2-4
- activation 2-2
- Activation Code 2-3, 2-7
- Add Keyword Expressions screen 3-9
- adding a new rule 3-25
- administration 3-47
- Administration menu
 - change password 3-47
 - policy 3-2
- Advanced level of service 1-4
 - features of 1-4
 - verifying that you have this service 2-5
- advanced service level 1-4–1-5
 - policy administration 3-2
 - user-level capabilities 2-11
- advantages of IMHS A-1
- APIKEY 3-56–3-57
- archived email A-3
- attachment, high-risk 3-5

B

- blocked 2-17
- blocked % of messages 2-15
- blocked messages
 - percentage of 2-19
- blocked traffic
 - percentage of 2-19
- botnet 1-3
- branding 3-53
- browser requirements C-1

C

- CAPTCHA C-9
- CAPTCHA image, with Email Encryption service 3-21
- case sensitive check box 3-12
- change password 3-47
- clean 2-17
- clean message, number of 2-19
- co-branding 3-53
- confidentiality of IMHS service A-2
- configuring
 - mail transfer agent 2-4
- configuring content filtering using regular expressions 3-8
- connection-level, reputation-based filtering 1-3
- contact
 - general information B-3
- content
 - filtering with keywords 3-6
- content filtering 3-6
 - keyword expression
 - weighting 3-11
 - keyword expressions
 - weighting 3-10
 - using regular expressions 3-8
 - with regular expressions 3-8
 - case sensitivity of 3-10, 3-12
- content-based filtering 1-3
- copying a rule 3-33
- cost A-1
- cost of using Trend Micro InterScan Messaging Hosted Security service A-1
- CSV directory file 3-50

D

- dashboard 2-13
 - graphics 2-14
- decrypting email 3-19
- default IMHS settings 1-6
- default policies 3-4
 - 3-6
 - high-risk attachment 3-5
 - message size 3-5
 - newsletter or spam-like 3-5
 - outbound filtering 3-6
 - spam or phish 3-5
 - virus
 - cleanable 3-4
 - mass mailing 3-4
 - uncleanable 3-4
- delay A-3
- deleting a rule 3-33
- delivery
 - email B-3
- Denial of Service (DOS) attack 3-5
- DHA. See directory harvest attacks
- Digest, spam 3-36–3-39
- digest, spam 3-36, 3-40–3-44
- directory harvest attacks 3-49, A-1
- Directory Management screen 3-49
- disable rules 3-3
- disabling IMHS 3-58
- disaster recovery A-3
- DNS propagation 3-58
- downtime B-3

E

- editing a rule 3-25, 3-30
- EICAR test file B-7
- email
 - archived A-3
 - connection-level reputation 1-3
 - connection-level reputation-based filtering 1-3
 - connection-level, reputation-based filtering 1-3
 - content-based filtering 1-3
 - delay A-3
 - delivery B-3
 - encryption 3-18–3-19, 3-21–3-22, 3-24
 - store A-3
 - email connection-level reputation-based filtering 1-3
 - email delivery, time required for A-3
 - email encryption
 - common uses of 3-18
 - configuring 3-18
 - decrypting 3-19
 - reading encrypted email 3-19, 3-22
 - rule action 3-24
 - system requirements 3-19
 - Email Encryption Client 3-19
 - Email Encryption service 1-4, 3-18, 3-24
 - activating 2-4–2-5, 2-8
 - activating a free trial 2-6
 - add-on component 2-2
 - CAPTCHA 3-21
 - notification of receipt of an encrypted message 3-20
 - Open my email button 3-21
 - purchasing 2-7
 - request a free trial of 2-6
 - requesting a free trial from the Trend Micro Web site
 - 2-5
 - starting a free trial of 2-5
 - email message routing by IMHS servers 1-2
 - Email Reputation Services 1-3
 - email Technical Support B-2, B-4
 - enable rules 3-3
 - encrypt email message
 - rule action 3-18
 - encrypted message notification 3-20
 - encrypted message, decrypting 3-19
 - encryption, add-on service 1-4
 - encryption, email 3-18–3-19, 3-21–3-22, 3-24

- End User Quarantine site 3-43
 - ERS. See Email Reputation Services.
 - EUQ
 - Forgot Password link 3-57
 - password reset by system email administrator 3-57
 - EUQ. See End User Quarantine.
 - execution order of rules 3-23
 - exporting a user directory file 3-50
- F**
- FAQs A-1
 - features unique to the Advanced service 1-4
 - filtering content 1-3, 3-6
 - filtering content with regular expressions 3-8
 - free trial of the Email Encryption service 2-6
 - Frequently Asked Questions A-1
- G**
- gateway
 - Internet gateway solutions A-2
 - glossary (Security Information Center) B-7
- H**
- heuristic rules 1-3
 - high-risk attachment 3-5
 - hosted email security service A-1
 - hosted email security service, advantages of A-1
- I**
- IMHS
 - default settings 1-6
 - disable 3-58
 - message flow 1-2
 - system requirements 1-5
 - trial installation A-3
 - workflow 1-2
 - IMHS Advanced 1-4
 - features unique to 1-4
 - verifying that you have this level of service 2-5
 - IMHS server
 - routing email messages 1-2
 - IMHS Standard 1-4
 - Import User Directory 3-49
 - Imported User Directories section 3-50
 - importing a directory file 3-50
 - importing a user directory file 3-50–3-51
 - inline action 3-40, 3-42, 3-44
 - InterScan Messaging Hosted Security
 - description A-1
 - disable 3-58
 - IP address of IMHS 1-2
- K**
- keyword expression
 - weighting 3-11
 - keyword expressions link 3-7, 3-18
 - Keyword Expressions screen 3-7–3-8
 - keyword, using with content-filtering 3-6
 - Knowledge Base B-2, B-4
 - URL B-6
- L**
- layers of protection 1-3
 - email
 - connection-level reputation 1-3
 - content-based filtering 1-3
 - LDAP Data Interchange Format 3-49
 - LDIF 3-49–3-50
 - LDIFDE tool 3-50
 - instructions on using 3-50
 - levels of performance B-3
 - levels of service 1-4
 - advanced 1-5
 - standard 1-5
 - logging on 2-9
 - logo
 - display my company 3-54
 - displaying my company 3-53
 - usage 3-53
 - logs 3-45
 - mail tracking details 3-45

M

- machine learning 1-3
- Mail eXchange
 - redirect A-2
- Mail eXchange (MX) record 1-2, 2-3, A-2
 - change 3-58
- mail servers
 - What happens to my messages if my mail server is unavailable for a period of time? A-3
- Mail Tracking Details 3-45
 - accepted 3-45
 - accepted for processing 3-45
 - blocked or delayed 3-45
 - deleted with a virus 3-45
 - delivered 3-45
 - determine location 3-46
 - processed 3-45
 - unresolved 3-45
- mail transfer agent 2-4
- maintenance B-3
- message flow 1-2
- message size, default policy for 3-5
- messages
 - accepted 2-14
 - blocked 2-14, 2-17
 - blocked % 2-15
 - clean 2-17
 - not quarantined 2-16
 - phish 2-17
 - quarantined 2-16
 - spam 2-17
 - total 2-15, 2-17
 - total size 2-16
 - virus 2-17
 - What happens to my messages if my mail server is unavailable for a period of time? A-3
- messages cleaned, number of 2-19
- messages, number of 2-19
- MX
 - redirect A-2
- MX record 1-2, 2-3, A-1
 - change 3-58
 - configure 3-58
 - redirecting A-2

N

- Not quarantined field 2-16
- notification
 - of encrypted email message 3-20

O

- online help 2-12
- online registration site 2-7
- order of rules, execution 3-23
- Other messages, number of 2-19
- outbound email stream A-3
- outbound filtering 1-5, 2-4, 3-6
 - contacting Trend Micro to request 2-5, A-3
 - default policies 3-6

P

- password
 - change 2-10, 3-47
 - changing admin password 3-48
 - resetting end-user password 3-48
- password-protected zipped files 3-6
 - attachments 3-6
- pattern files 1-3
- performance levels B-3
- phish 2-17
- phish, default policy for 3-5
- phish, number of 2-19
- Policy Administration
 - Rules list 3-2
- policy administration 3-2
 - advanced 3-2
 - standard service level 3-2
- policy settings, default 3-4
- price A-1
- privacy of IMHS service A-2
- product maintenance B-7
- protection tiers 1-3
- purchase Email Encryption 2-7

Q

- Quarantine 3-35
- Quarantined field 2-16
- Quarantined Spam screen C-5

R

- reading an encrypted email 3-19
- Redirect mail
 - email, direct A-2
- regex 3-10
- register online 2-7
- Registration
 - Registration Key 2-2
- Registration Key (RK) 2-7
- regular expressions 3-9
 - available operators 3-9
- regular expressions, filtering content with 3-8
- regular expressions, using with content filtering 3-8
- reports
 - Accepted Size 2-16
 - dashboard 2-13
 - overview 2-12
 - summary 2-13
 - Threats Details 2-19
 - Threats Summary 2-17
 - Total Traffic 2-14
- reputation-based filtering 1-3
- reseller level 3-53
- risk ratings B-7
- RK. See Registration Key.
- routing of messages by IMHS servers 1-2
- rules
 - adding 3-25
 - copying 3-33
 - deleting 3-33
 - editing 3-25, 3-30
 - enable/disable 3-3
 - order of execution 3-23
- Rules list 3-2

S

- Safe Computing Guide B-7
- scan engine refinements B-7
- secure messaging gateway, trustworthiness of A-2
- Security Information Center B-7–B-8
- sending suspicious code to Trend Micro B-4
- service availability B-3
- Service Level Agreement
 - availability A-4
- service, levels of 1-4
- size of messages, default policy for 3-5
- spam 2-17
 - default policies 3-5
- Spam digest 3-36–3-39
- spam digest 3-36, 3-40–3-44
 - approving senders or messages from within 3-40, 3-44
 - inline action 3-42
 - plain text 3-41
 - system requirements 3-43
- spam recipients
 - most received (report) 2-21
- spam, number of 2-19
- Standard level of service 1-4
- standard service level 1-4–1-5, 3-2
 - user-level capabilities 2-11
- store email A-3
- Submission Wizard B-4–B-5
- Support
 - contact email B-2
 - Please provide the following in your correspondence B-2
 - contacting B-2
 - Web-based resources B-1
- support by email B-4
- Support contact email A-3
- suspicious code B-4
 - how to submit B-6
- suspicious files B-4
- system requirements 1-5

T

- Technical Support
 - contacting B-2
- Threat Details report
 - Totals table 2-19
- Threats Details
 - Totals table 2-19
- Threats Details report 2-19
 - blocked traffic, percentage of 2-19
 - clean, number of 2-19
 - daily total 2-19
 - messages, number of 2-19
 - other message, number of 2-19
 - phish, number of 2-19
 - spam, number of 2-19
 - virus, number of 2-19
- Threats Summary report 2-17
 - Blocked field 2-17
 - Clean field 2-17
 - Others field 2-17
 - Phish field 2-17
 - spam 2-17
 - total 2-17
 - Virus field 2-17
- tiers of protection 1-3
- time required for email delivery A-3
- Top Spam Recipients report 2-21
- Top Virus Recipients 2-22
- Total messages field 2-15
- Total Size field 2-16
- Total Traffic report 2-14
- Totals table
 - blocked messages, number of 2-19
 - blocked messages, percentage of 2-19
 - cleaned messages, number of 2-19
 - other messages, number of 2-19
 - phish, number of 2-19
 - spam, number of 2-19
 - virus, number of 2-19
- Trend Micro
 - contact information B-3
 - market share of Internet gateway solutions A-2
- TrendLabs B-6
- trial 2-5
 - activating a free trial of Email Encryption service 2-6
- trial form on the Trend Micro Web site 2-5
- trial installation A-3

U

- unavailable
 - What happens to my messages if my mail server is unavailable for a period of time? A-3
- URL reputation 1-3
- URLs
 - Knowledge Base B-4
 - Security Information Center B-7
- user directory
 - verifying 3-52
- user directory file
 - exporting 3-50
 - importing 3-50–3-51
- user-level capabilities 2-11

V

- verifying user directory 3-52
- virus 2-17
 - default rule 3-4
- Virus Alert service B-8
- Virus Doctor B-6
- Virus Doctor. See TrendLabs
- Virus Encyclopedia B-7
- virus pattern file updates B-7
- Virus Primer B-7
- virus recipients
 - most received 2-22
- Virus, number of 2-19
- virusresponse@trendmicro.com B-6

W

- Web End-user Quarantine. See Web EUQ
- Web EUQ 3-57, C-1, C-3–C-4
 - actions C-6
 - Approved Senders screen C-6–C-7
 - changing your password C-8
 - create a new account C-3
 - discussed in detail C-1
 - edit existing approved senders' addresses or domains C-8
 - logging on C-4
 - Login screen C-2
 - Quarantined Spam screen C-4
- Web EUQ End-User Guide 3-57
- Web EUQ online help 3-57
- Web EUQ service C-1

Web services 3-56
 APIKEY 3-56–3-57
Web services client 3-56
Web-based resources B-1
weekly virus report B-7
white papers B-7
workflow 1-2
Worry Free Business Security B-2

Z

Zip of Death 3-5
zipped files
 password-protected 3-6
zombie 1-3

