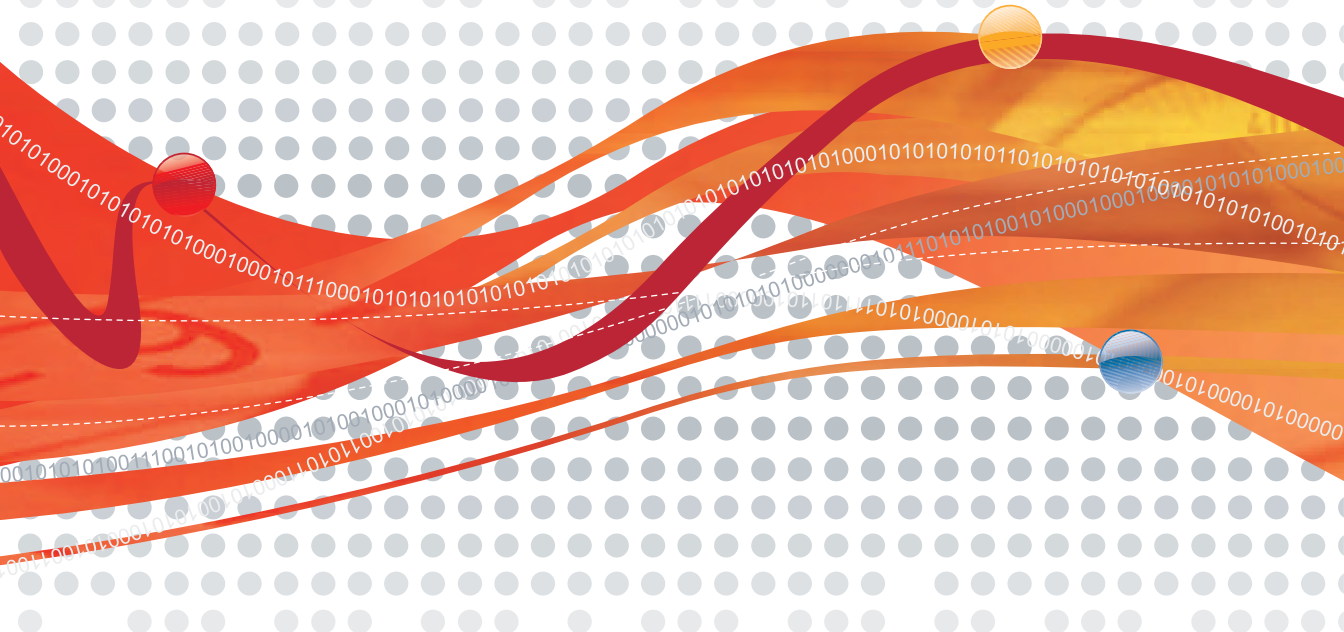
TREND MICRO™

Hosted Email Security

Integrated email threat protection in a hosted service

Administrator's Guide



Messaging Security

Document Part No. HSEM04283_91229

Publication Date: March 18, 2010

Document Version No.: 1.2

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

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

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

Chapter 1: Introducing Trend Micro Hosted Email Security

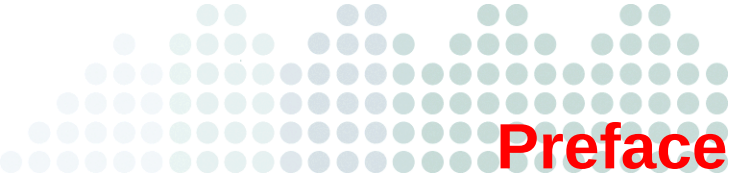
Chapter 2: Using Hosted Email Security

Chapter 3: Managing Policies

Chapter 4: Approved Senders, Quarantine, and Logs

Chapter 5: Administration and IP Reputation

Appendix A: Frequently Asked Questions



Preface

Welcome to the *Trend Micro™ Hosted Email Security Administrator's Guide*. This book contains information about service settings and service levels.

Topics in this preface include:

What's New

At the time of publication of this manual, the major changes in Trend Micro Hosted Email Security in the last 6 months include the following:

- New Service Name (April 1, 2010)—The former "Trend Micro InterScan Messaging Hosted Security" is now called "Trend Micro Hosted Email Security."
- *Simplified Way to Enable Outbound Filtering* (December 19, 2009)—With a Trend Micro Online Registration account, you can add outbound filtering through the administrative console.[1]

Simplified Way to Enable Outbound Filtering

If you have a Trend Micro Online Registration (OLR) account, you can enable Hosted Email Security (full version) outbound filtering from within the Hosted Email Security administrative console. If you have not yet obtained an OLR account, you can still request outbound filtering using the manual method.Outbound filtering is unavailable to customers with the Hosted Email Security–Inbound Filtering version.

For more information on the simplified way to enable outbound filtering, see *If You Have an Online Registration Account* on page 2-7.

1. Outbound filtering is available in the full version only; not in the Inbound Filtering version.

Hosted Email Security Documentation

The Trend Micro™ Hosted Email Security 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 ( ).

Administrator's Guide—Helps you to set up and configure all service settings.

Note: As of the April 1, 2010 release, the service name "InterScan Messaging Hosted Security" is now changed, to "Hosted Email Security."

Web Services Guide—Helps you to automate Hosted Email Security administrative tasks.

Web End User Quarantine Guide—Helps you understand how to manage spam mail held in quarantine using the Trend Micro Web End User Quarantine.

The *Administrator's Guide* and *Web End User Quarantine User Guide* are available at:

http://us.trendmicro.com/us/products/enterprise/hosted-email-security/index.html

Audience

This 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.

Document Conventions

To help you locate and interpret information easily, this documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, file names, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Introducing Trend Micro Hosted Email Security

Trend Micro™ Hosted Email Security 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 include:

Hosted Email Security Message Flow

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

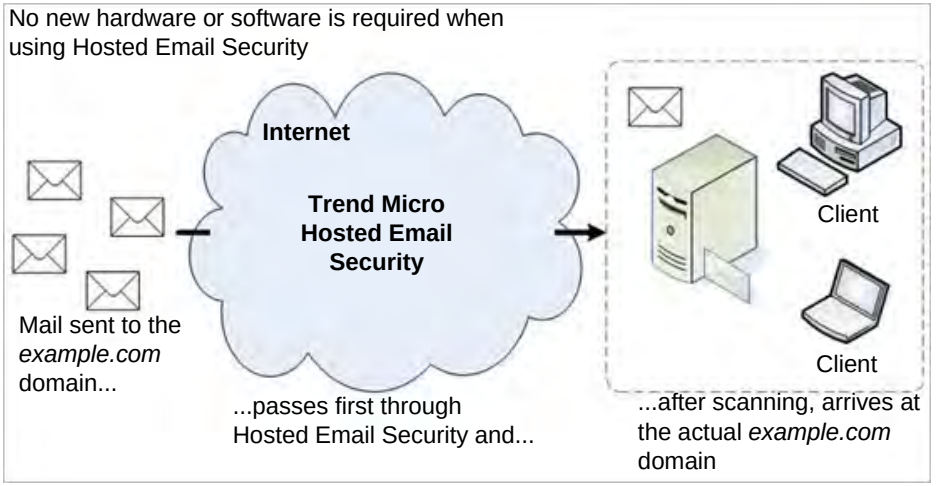


FIGURE 1-1 Hosted Email Security workflow diagram

Hosted Email Security performs the following processes:

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 Hosted Email Security instead of the original IP address for example.com, since Hosted Email Security must first scan your company's mail before final delivery to your local email server.
2. The originating mail server routes the mail to Hosted Email Security.
3. Hosted Email Security servers accept the message and perform message filtering and policy matching on your behalf.
4. Assuming that a message is slated for delivery according to its security policy or validity status, the Hosted Email Security servers route the message to the original example.com mail servers.

Tiers of Protection

Hosted Email Security 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 a Hosted Email Security server, the Hosted Email Security server queries the Trend Micro Email Reputation server to determine whether the IP address of the connecting sender is "trustworthy." Hosted Email Security 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 is marked "untrustworthy." Hosted Email Security permanently rejects the connection attempt from this IP address.

If the sender's computer is part of a botnet or is a zombie PC, the IP address can be found in the Email Reputation Services (ERS) dynamic database that identifies spam sources as they emerge and for as long as they are active. Hosted Email Security informs the sending server that Hosted Email Security 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, Hosted Email Security 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

Hosted Email Security 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

Hosted Email Security is available in two basic levels of service:

- Hosted Email Security (full version)
- Hosted Email Security—Inbound Filtering

For a comparison of features available in each version, see Table 1-1 on page 1-5.

Hosted Email Security—Inbound Filtering

This service level provides several default settings to provide immediate protection upon deployment. In this version, only the spam action can be changed, minimizing the administration needed.

Hosted Email Security (Full Version)

The full 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 this service level include the following:

- Customized threat filtering,Outbound email filtering (optional)
- 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 Hosted Email Security (full version) that is available for purchase. Email Encryption is seamlessly integrated with the content-filtering capabilities of Hosted Email Security. The service does not automatically encrypt email. When enabled, Email Encryption appears as a rule enforcement option within the Hosted Email Security administrative console. You will need to configure rules that apply encryption as a rule action. See *Encrypt Email Message* on page 3-20 for guidelines on creating rules that apply encryption.

In order to use the email encryption service, you must first deploy Hosted Email Security (full version) with outbound filtering.

TABLE 1-1 Hosted Email Security features, by account type

Features	Inbound Filtering	Full version
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 settings and is updated and tuned by Trend Micro. ** Full version customers also begin with default rules but can modify them and create new rules.*	✓	✓
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.	✓	✓
Provides in-depth content filtering and policy management for more granular access and control. *Optional: Outbound message scanning.*		✓
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, domain, or individual and can set the appropriate enforcement action for each policy.		✓
Optional add-on feature: Email encryption. Provides policy-based encryption to secure email.		✓

System Requirements

Hosted Email Security does not require additional hardware (other than your mail gateway) on your premises. All scanning hardware is off-site at secure Trend Micro network operations centers. To access your web-based Hosted Email Security administration account, you need a personal computer with access to the Internet.

Software Required for Accessing Your Account

Use of the Hosted Email Security web console requires Java Script™ and Hosted Email Security 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 Hosted Email Security can be activated:

- An existing Internet gateway or workgroup SMTP connection
- Access to the DNS mail exchange record, 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 Hosted Email Security 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
- Total embedded layers within a compressed file: 20 layers
- Total decompressed message size: 30 MB
- Total files in a compressed archive: 353 files
- Total of quarantine storage per seat: 50 MB
- Total approved senders entries per seat: 50

Chapter 2

Using Hosted Email Security

This chapter presents basic guidance on accessing and using the Hosted Email Security administrative console and understanding the reports available from the console.

Topics in this chapter include:

Getting Started

Hosted Email Security must be configured to work properly and effectively. This configuration process includes the following basic steps:

TABLE 2-1. Hosted Email Security setup checklist

STEP	FOR MORE INFORMATION	
1. Submit account activation information	*Submitting Account Activation Information* on page 2-3	❑
2. Log on to web-based admin console	*Logging on for the First Time* on page 2-11	❑
3. Add one or more domains to account	*Managing Domains* on page 5-16	❑
4. Confirm mail delivery through Hosted Email Security	*Confirming Mail Delivery Through the Service* on page 5-19	❑
5. Redirect MX record for your domain	*Redirecting Your MX Record* on page 2-5	❑
6. Configure your MTA, if applicable	*Configuring Your Mail Transfer Agent* on page 2-6	❑

Registering and Activating Hosted Email Security

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

You must register your service before you can use it. 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 Hosted Email Security and must be purchased separately.

Submitting Account Activation Information

Before using Hosted Email Security, you must activate the account.

To activate the Hosted Email Security account:

1. Locate your confirmation of purchase and a registration key in the email message received from Trend Micro.
2. Visit the Trend Micro Online Registration site (URL provided in email message) and choose a user name and password, complete the registration process.
3. Trend Micro sends you an email with the user name that you chose and the URL of the Hosted Email Security administrative console.
4. Log on to the console with that user name. You are prompted to enter domain and IP information.
5. Click **Submit**. Trend Micro will set up your account and send you a confirmation email. (Allow 24-48 hours.) This email will contain information about where to direct your MX record.
6. Send a test email to your test email address to verify that email can pass through Hosted Email Security.
7. Redirect your MX record as explained in the email mentioned above.

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

Customers in North American, Europe, the Middle East, and Africa need a registration key (RK) to register Hosted Email Security. This key uses 22 characters, including hyphens, in the following format:

XX-XXXX-XXXX-XXXX-XXXX

Customers in the above regions must register Hosted Email Security using your registration key before receiving an activation code, which enables you to begin using the service.

Activation Code

For all customers, an activation code (AC) is required. The web console displays the status of your license. An AC uses 37 characters, including hyphens, in the following format:

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

After you have registered Hosted Email Security, Trend Micro sends your AC.

Activating the Hosted Email Security Service

When setting up Hosted Email Security for the first time, the first screen that you see is the Service Activation screen, shown in *figure 2-1*. Use this screen to enter the domains to manage through the Hosted Email Security service.

Note: Hosted Email Security must have a record of your company domains in order to apply IP reputation settings to mail coming in to them.

To add a domain for Hosted Email Security to manage:

1. Type the following information in the fields provided (required fields shown in bold):
   - The new **domain name**
   - **IP address or FQDN**(fully qualified domain name)
   - **Port number** of its mail server
   - Number of **seats assigned** to this domain
   - The test email account (Use this email address as the recipient for a test message to confirm delivery through Hosted Email Security.)
2. Select **Disable** or **Enable** from the **Outbound email scan** drop-down list (unavailable to Hosted Email Security—Inbound Filtering accounts).
3. Click **Activate Domain.** The domain appears in the Domains table at the bottom of the screen.
4. Click **Submit.** If the domain is valid and there is an MX record for the domain, the new domain, IP address or FQDN, port number, seats, and other information appear in the Domains table at the bottom of the screen and Trend Micro sends a "welcome" email to the administrative email address on record.

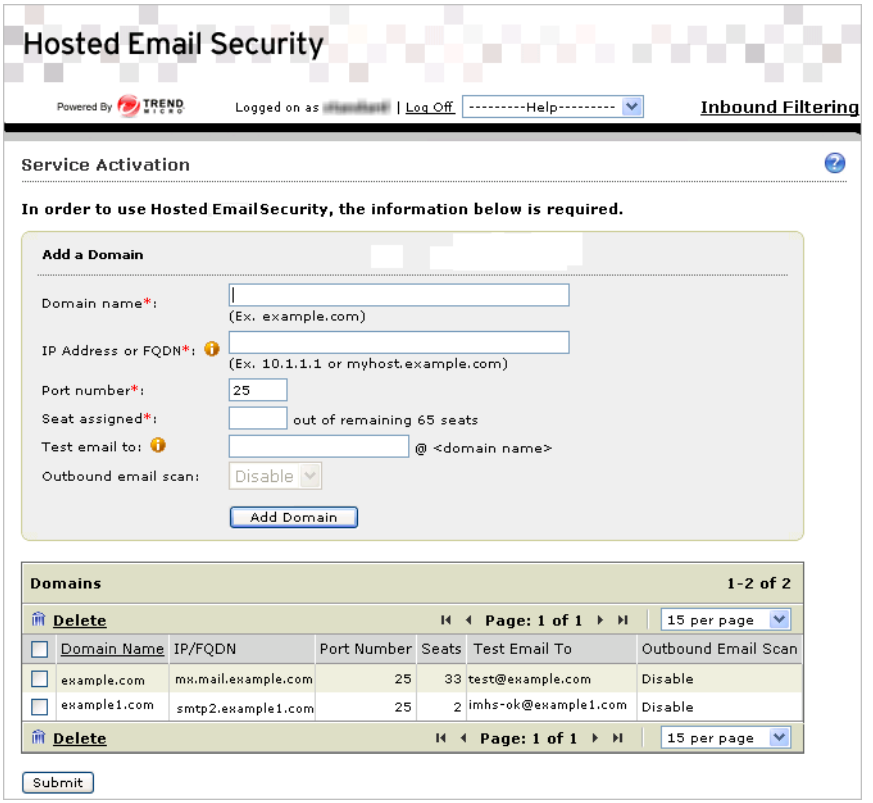


FIGURE 2-1. Service Activation screen for Hosted Email Security—Inbound Filtering accounts

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 Hosted Email Security servers, you must redirect your MX record. The welcome email that you receive tells you where to redirect your MX record.

To redirect the MX record, change your current MX record to the record provided in the "Welcome" email that Trend Micro sent you after you registered. You can make this change manually (typical 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 or your DNS technician.

Note: DNS propagation may take up to 48 hours. During this time, do not turn off any on-premise security. You may receive some email directly for a short time until the transition completes.

Configuring Your Mail Transfer Agent

For all Hosted Email Security customers, all "spam or phish" messages are initially deleted by default. If you have the full version, you can modify this rule. (See *Editing an Existing Rule* on page 3-35.)

Note: Hosted Email Security—Inbound Filtering users 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.

Enabling Outbound Filtering

Trend Micro Email Encryption is available only as an add-on service for Hosted Email Security (full version) with outbound filtering. Outbound filtering is available at no extra cost.

If you do not have a Trend Micro Online Registration (OLR) account, enabling this feature involves contacting Trend Micro Technical Support. With an OLR account, you can accomplish this task from within the Hosted Email Security administrative console.

If You Have an Online Registration Account

With an Online Registration Account (OLR) account, enabling outbound filtering is easy.

To enable outbound filtering:

1. Ensure that you have the full version of Hosted Email Security by viewing the version information at the top of the administrative console, at the bottom right of the title banner, as shown in *figure 2-3*.
2. From the left menu select **Administration > Domain Management** to open the Domain Management screen.
3. In the Domains table at the bottom of the screen, click the hyperlinked domain name to enable outbound filtering for. The **Domain Management > {your-domain-name}** screen appears, with its fields prepopulated with the information on record for that domain.
4. In the **Outbound email scan** drop-down list, select **Enable.**
5. Click **Save**. Hosted Email Security begins the process of enabling outbound filtering for that domain, and the status of the domain changes to "Modifying."

Tip: After you click **Save**, the enabling process begins. It may take up to 2 hours to complete. When the process is complete, Hosted Email Security changes the status of the domain from "Modifying" to "Activated."

If You Do Not Have an Online Registration Account

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.

Before contacting Trend Micro Technical Support to set up outbound filtering, you will need to supply the following information:

- Account name
- Domain name and valid email address under the domain
- Your name
- Your email address
- IP address of outbound mail server

Trend Micro support staff will make changes to allow your outbound mail stream to go through Hosted Email Security outbound filtering and will notify you by email when it is ready. You will then receive further instruction on how to redirect your outbound mail to the Hosted Email Security outbound mail servers.

Note: Ensure that reverse DNS is set up and configured correctly before requesting outbound filtering. Hosted Email Security relay servers will not accept emails from mail servers that fail the RDNS checking.

For more information on enabling outbound filtering, or to request outbound filtering service, contact Trend Micro Technical Support.

Verifying Outbound Filtering

When Trend Micro Support has finished enabling outbound filtering for your account, Support will notify you by email. Check the **Administration > Domain Management** screen to verify that outbound filtering is enabled, as shown in *Figure 2-2* on page 2-9. If outbound filtering is enabled, the drop-down list will display a value of "Disable."

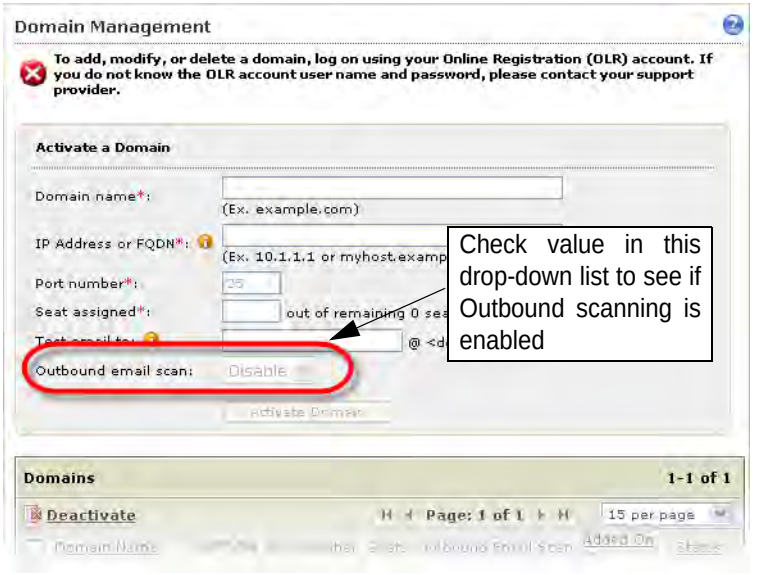


FIGURE 2-2. Domain Management screen showing "Outbound email scan" drop-down list

FIGURE 2-3. Hosted Email Security (full version) initial screen after logging on

---

Note: If you have Hosted Email Security—Inbound Filtering and want the Email Encryption service, contact Trend Micro to upgrade to the full version.

Purchasing Email Encryption

To purchase Email Encryption, you must have purchased Hosted Email Security (full version) with outbound filtering. You can conduct a free trial of Email Encryption while in the trial period for Hosted Email Security (full version), but you cannot purchase Email Encryption until you have purchased Hosted Email Security (full version) 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

Disabling Hosted Email Security

To disable Hosted Email 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. See *Redirecting Your MX Record* on page 2-5.

Logging on to the Administrative Console

You can view reports and use the mail tracking tool to locate messages by logging on the Hosted Email Security Web console. As an Hosted Email Security (full version) user, you can also make changes to your messaging security policy

Logging on for the First Time

The welcome packet that you received after signing up for Hosted Email Security contains a user name and password for you to use when logging on for the first time.

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 2-3) to access the logon page.

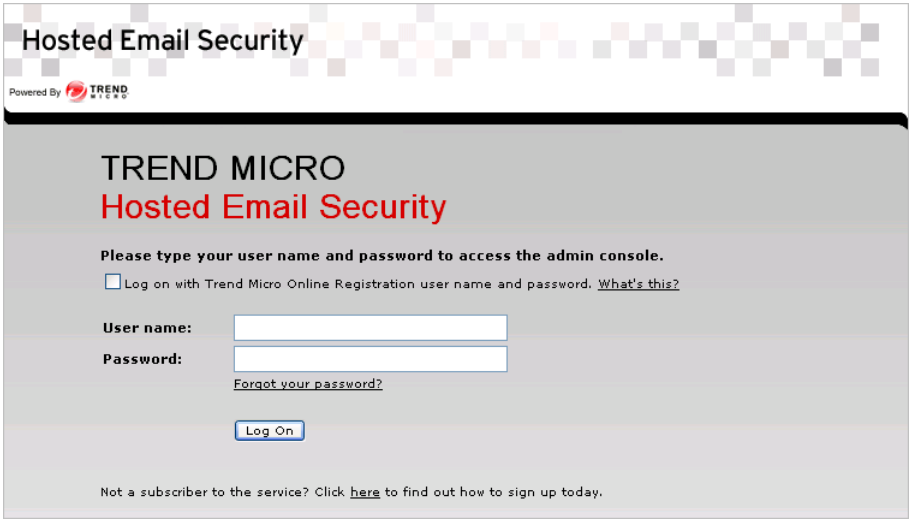


FIGURE 2-4. Hosted Email Security logon screen

2. If you have a Trend Micro Online Registration account, select **Log on with Trend Micro Online Registration user name and password.**
3. Type your **User name** and **Password**.
4. Click **Log On**.

> **Tip:** To help ensure the security of your Hosted Email Security account, Trend Micro recommends changing your password after you have logged on for the first time. (See *Administration* on page 5-10.)

Using the Hosted Email Security Web Console

The Hosted Email Security Web console enables mail administrators to create reports, view logs, perform administrative tasks, and set or alter policies (full version customers only).

See *table 2-2* below for a summary of user-level capabilities.

TABLE 2-2. Summary of features available in the two different service levels

INBOUND FILTERING VERSION	• Antivirus and IP connection spam prevention • Heuristic, content-based spam prevention filter • Default 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
FULL VERSION	All of the Inbound Filtering 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 Hosted Email Security Web console. You can access the complete online 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 screen (*figure 2-6*) displays when you log on to Hosted Email Security. *Table 2-3* on page 2-15 describes the Dashboard graphs.

Hosted Email Security—Inbound Filtering users can query Hosted Email Security for information about incoming mail. Hosted Email Security (full version) users can query both incoming and outgoing mail. Select **Incoming** or **Outgoing** from the "Mail Traffic Direction" drop-down list.

For specifics concerning Hosted Email Security actions, click the appropriate tab or double-click the image in the Dashboard screen.

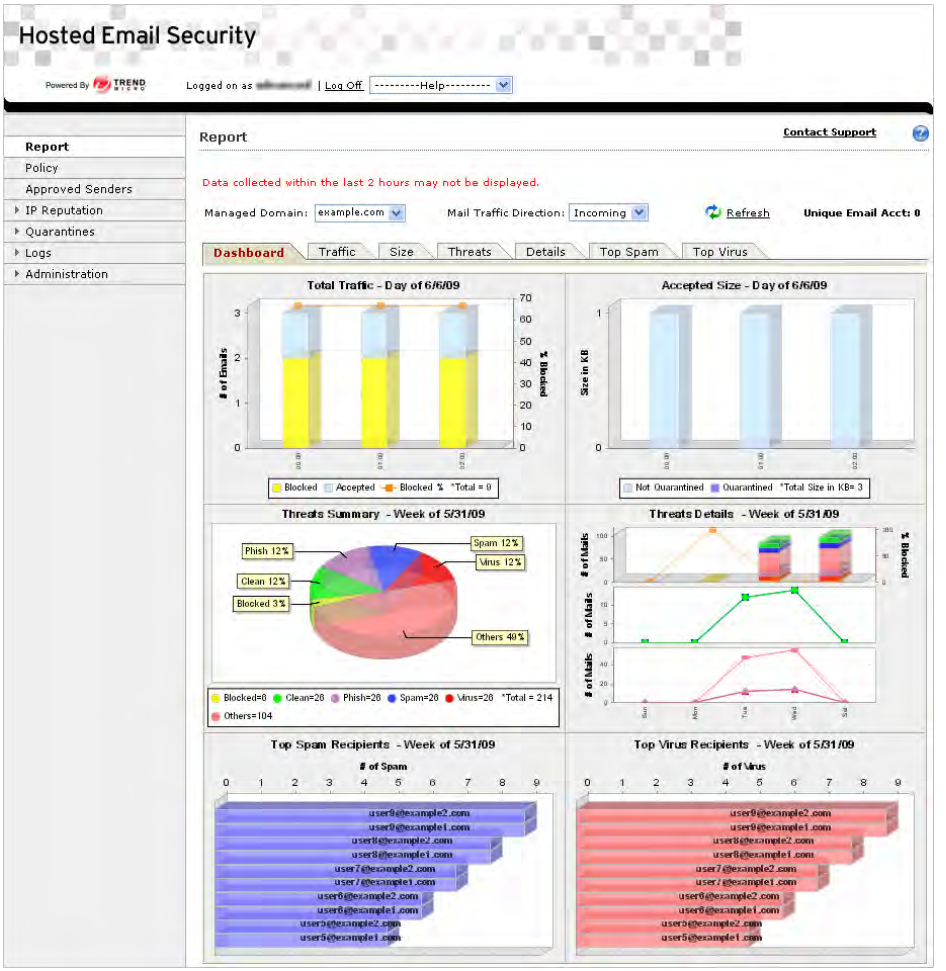


FIGURE 2-6. Summary report screen (incoming traffic)

Table 2-3 on page 2-15 describes the Dashboard tab screen charts.

TABLE 2-3. Dashboard screen charts

CHART NAME	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 Senders	Top Spam	Shows the top spam message recipients (or senders, for outgoing mail) for the selected mail domain
Top Virus Recipients Top Virus Senders	Top Virus	Shows the top virus message recipients (or senders, for outgoing mail) for the selected mail domain

*. To avoid clutter, the dashboard view of this report omits the legend.

Traffic Tab

Click the **Traffic** tab to display the Total Traffic screen (*figure 2-7*), which shows 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.

Note: The display of "blocked" traffic has different meanings for incoming and outgoing traffic. Incoming traffic is filtered by Trend Micro Email Reputation Services; outgoing traffic is not. If messages are blocked in outgoing traffic, the reason for blocking is unrelated to email reputation but may be related instead to issues with the Hosted Email Security relay mail service, as explained further below.

For incoming mail:

- **Blocked** — The number of "bad" message attempts to send to the selected domain. This "bad" message attempts 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 Hosted Email Security.
- **Blocked %** — The percentage of message traffic blocked by ERS for the selected mail domain.
- **Total** —The total number of messages processed by Hosted Email Security for the selected mail domain. This is the sum of blocked and accepted traffic.

For outgoing mail only:

- **Blocked** — The number of message attempts rejected by the Hosted Email Security relay mail server. Possible reasons for blocking include:
  - Recipient address is not resolvable ("`someone@???.com`").
  - Spammers forged the mail sender address so that the message appears to be coming from the customer domain.
  - Customer mail server is compromised (for example, an open relay) and is sending spam messages.

Note: Outgoing messages are not blocked by Trend Micro Email Reputation Services (ERS) filter but by the Hosted Email Security relay mail service.

- **Accepted** — The number of messages that were accepted for further processing by Trend Micro Hosted Email Security.
- **Blocked %** — The percentage of message traffic blocked by the Hosted Email Security relay mail service for the selected mail domain.
- **Total** —The total number of messages processed by Hosted Email Securityfor the selected mail domain. This is the sum of blocked and accepted traffic.

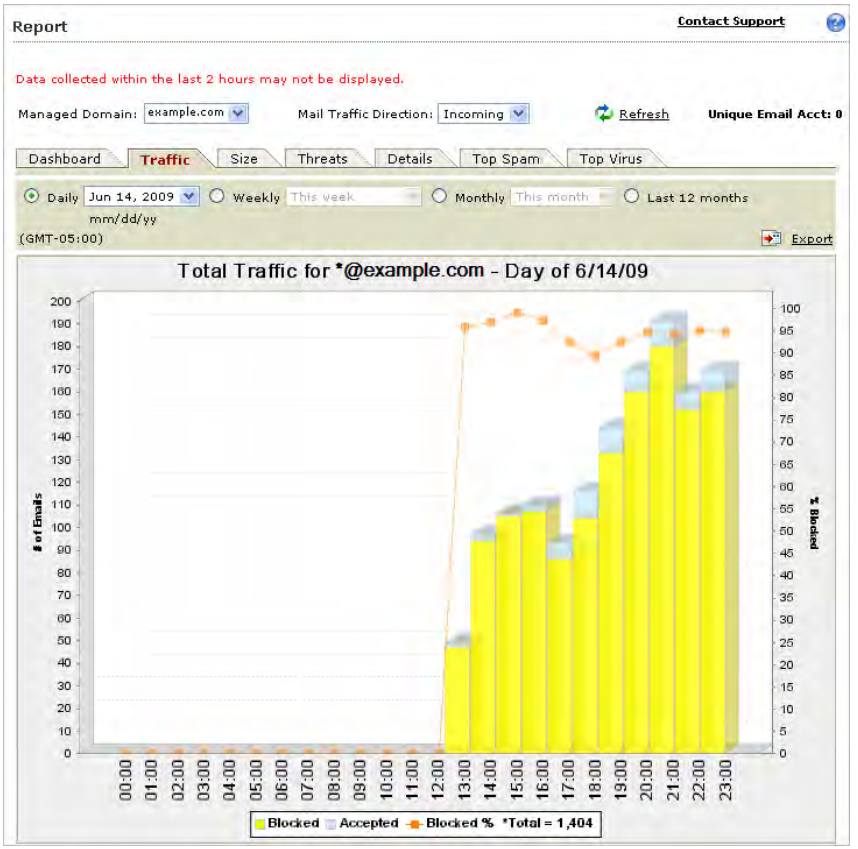


FIGURE 2-7. Total Traffic report screen (incoming traffic)

Size Tab

Click the **Size** tab to display the Accepted Size report (*figure 2-8*), which shows the total size (in KB) of accepted email traffic for the selected domain. The default reporting period is *today* (the current day). The legend indicates the total size of non-quarantined messages, quarantined messages, and total size of accepted messages. This tab can display a chart for either incoming or outgoing traffic, depending on the selected mail traffic direction.

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.

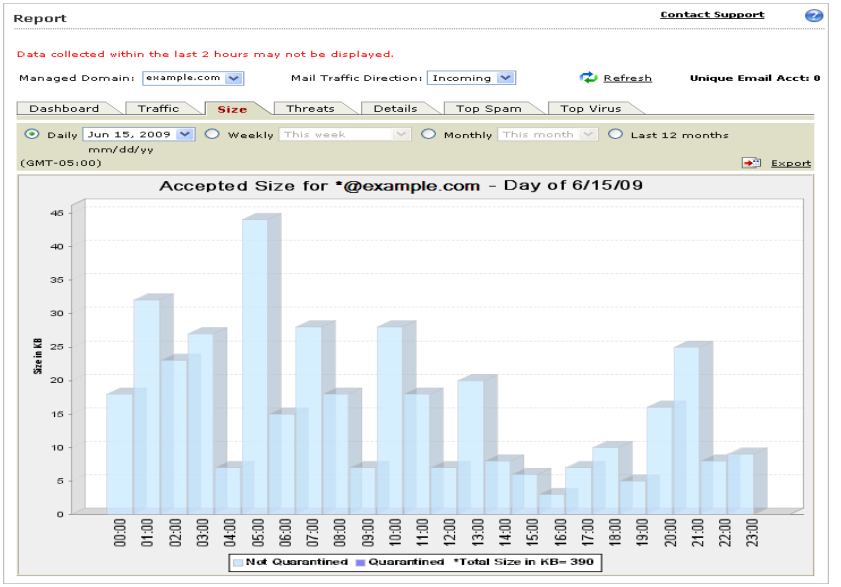


FIGURE 2-8. Accepted Size report screen (incoming traffic)

Threats Tab

Click the **Threats** tab to display the Threats Summary report (*figure 2-9*), which for the selected domain shows the share of messages by type. The default reporting period is the current week. The pie chart shows the percentage make-up of different kinds of messages for the selected domain.

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

- **Blocked** — For the selected mail domain, the number of email connections blocked by Trend Micro ERS (for incoming mail) or by Trend Micro Hosted Email Security relay mail service (for outgoing mail).
- **Clean** — For the selected mail domain, the number of email messages that Hosted Email Security deemed as "clean".
- **Phish** — For the selected mail domain, the number of email messages that Hosted Email Security identified as phishing messages.
- **Spam** — For the selected mail domain, the number of email messages that the Hosted Email Security heuristic spam prevention engine identified as spam.
- **Virus** — For the selected mail domain, the number of email messages that Hosted Email Security identified as carrying a virus.
- **Others** — For the selected mail domain, the number of email messages that were filtered by other Hosted Email Security content filters (such as the attachment size filter).
- **Total** — The total number of email messages for the selected mail domain. This number is the sum of all six categories.

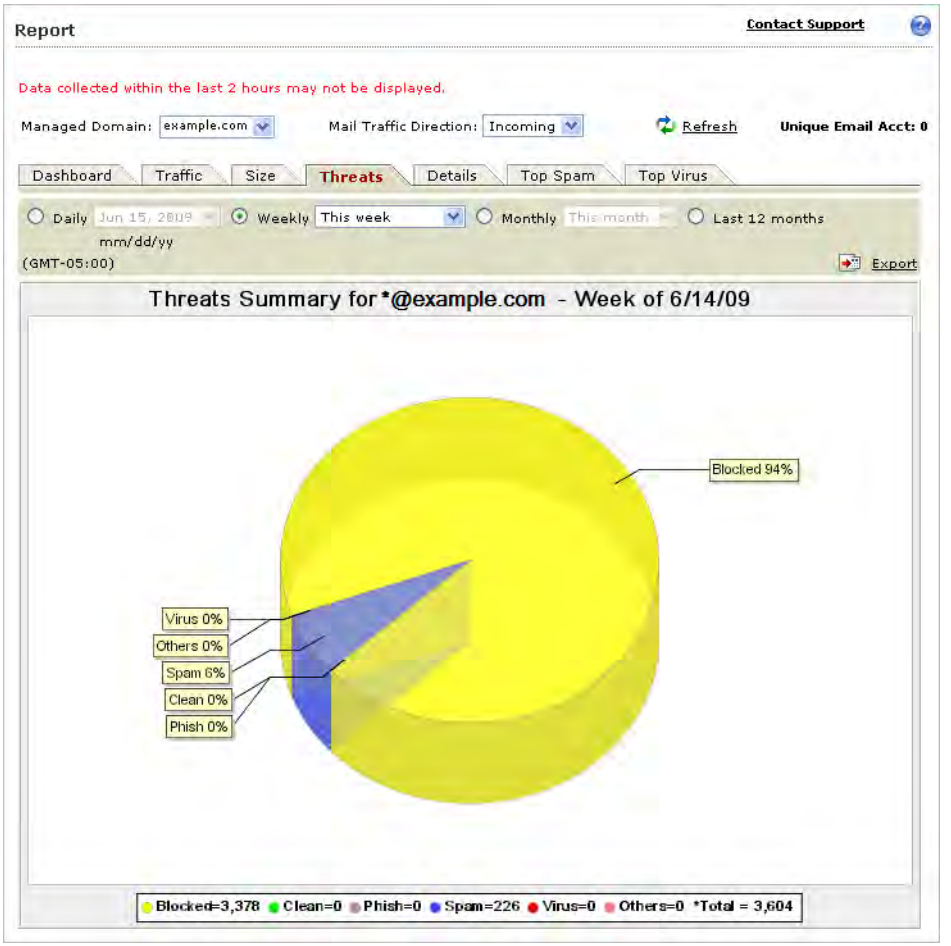


FIGURE 2-9. Threats Summary report screen (incoming traffic)

Details Tab

Click the **Details** tab to display the Threats Details report (*figure 2-14*), which 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. There are three detailed graphs and a Totals table:

Graph 1 — Number of messages and percentage of blocked traffic, as shown in *figure 2-10*.

Note: The display of "blocked" traffic has different meanings for incoming and outgoing traffic, as explained in detail in *Traffic Tab* starting on page 2-15.

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.

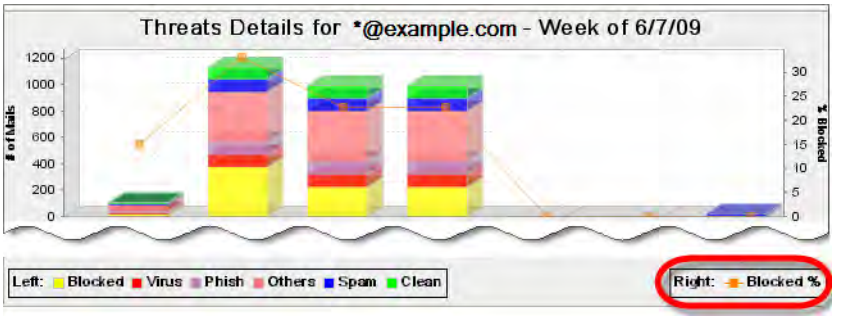


FIGURE 2-10. Threats Details report, graph 1 (incoming traffic)

Graph 2 —Number of each kind of email: "spam" and "clean" only

Each line represents the number of a kind of email at each interval, as shown in *figure 2-11*.

FIGURE 2-11. Threats Details report, graph 2 (incoming traffic)

Graph 3 — Number of each kind of email threats: "virus," "phish," and "others" only

Each line represents the number of a kind of email threat at each interval, as shown in *figure 2-12*.

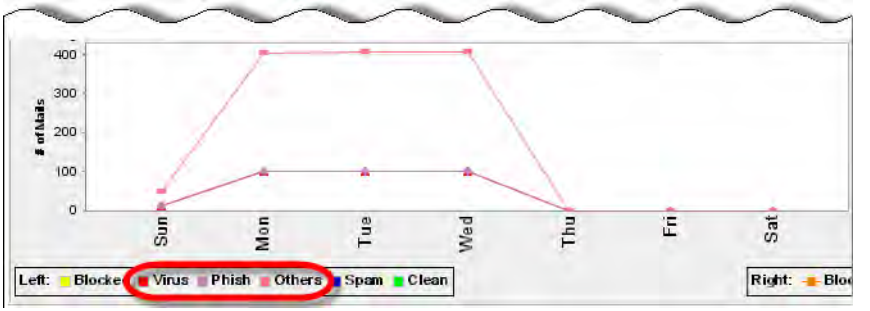
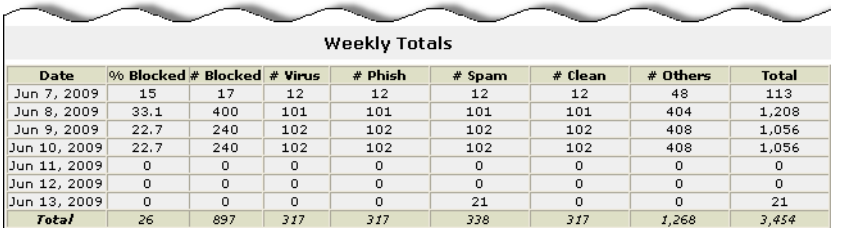


FIGURE 2-12. Threats Details report, graph 3

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

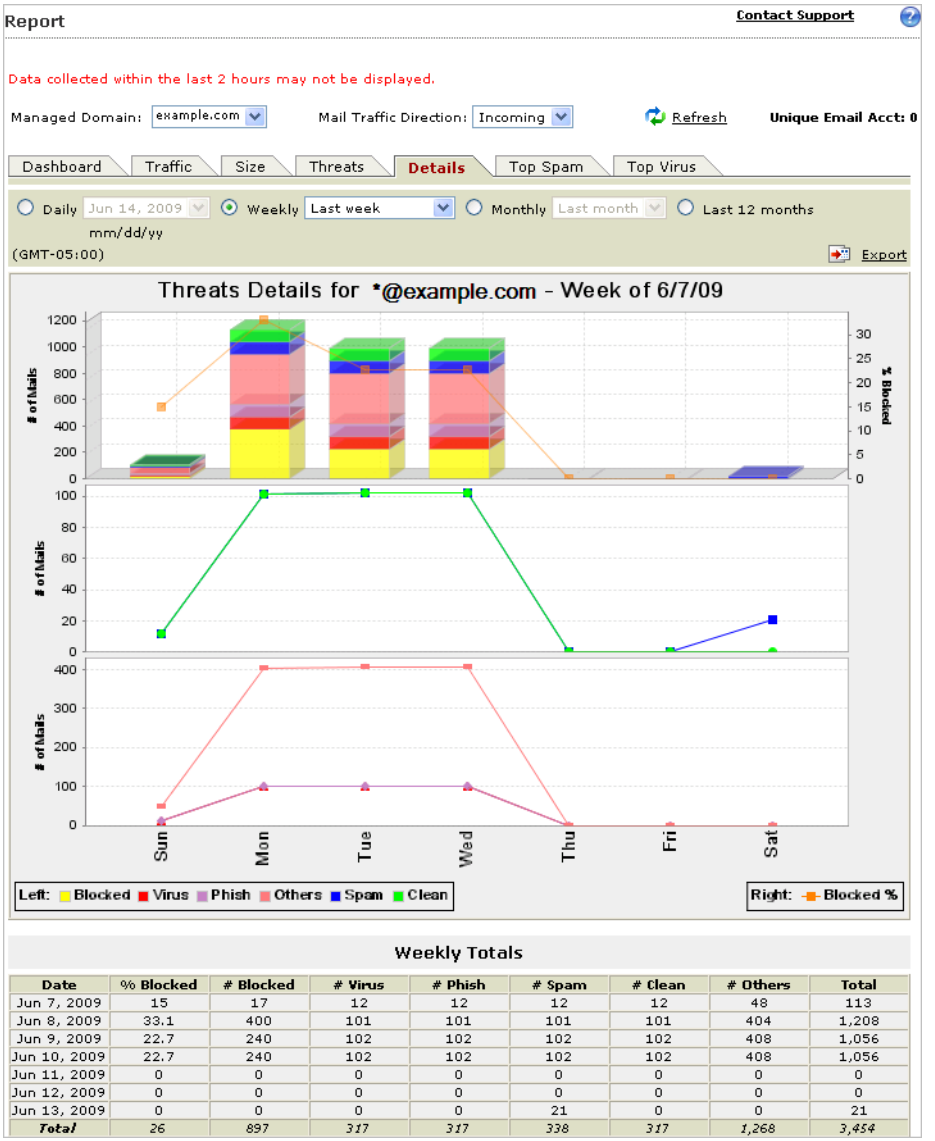


Weekly Totals

Date	% Blocked	# Blocked	# Virus	# Phish	# Spam	# Clean	# Others	Total
Jun 7, 2009	15	17	12	12	12	12	48	113
Jun 8, 2009	33.1	400	101	101	101	101	404	1,208
Jun 9, 2009	22.7	240	102	102	102	102	408	1,056
Jun 10, 2009	22.7	240	102	102	102	102	408	1,056
Jun 11, 2009	0	0	0	0	0	0	0	0
Jun 12, 2009	0	0	0	0	0	0	0	0
Jun 13, 2009	0	0	0	0	21	0	0	21
Total	*26*	*897*	*317*	*317*	*338*	*317*	*1,268*	*3,454*

FIGURE 2-13. Threats Details report, totals table

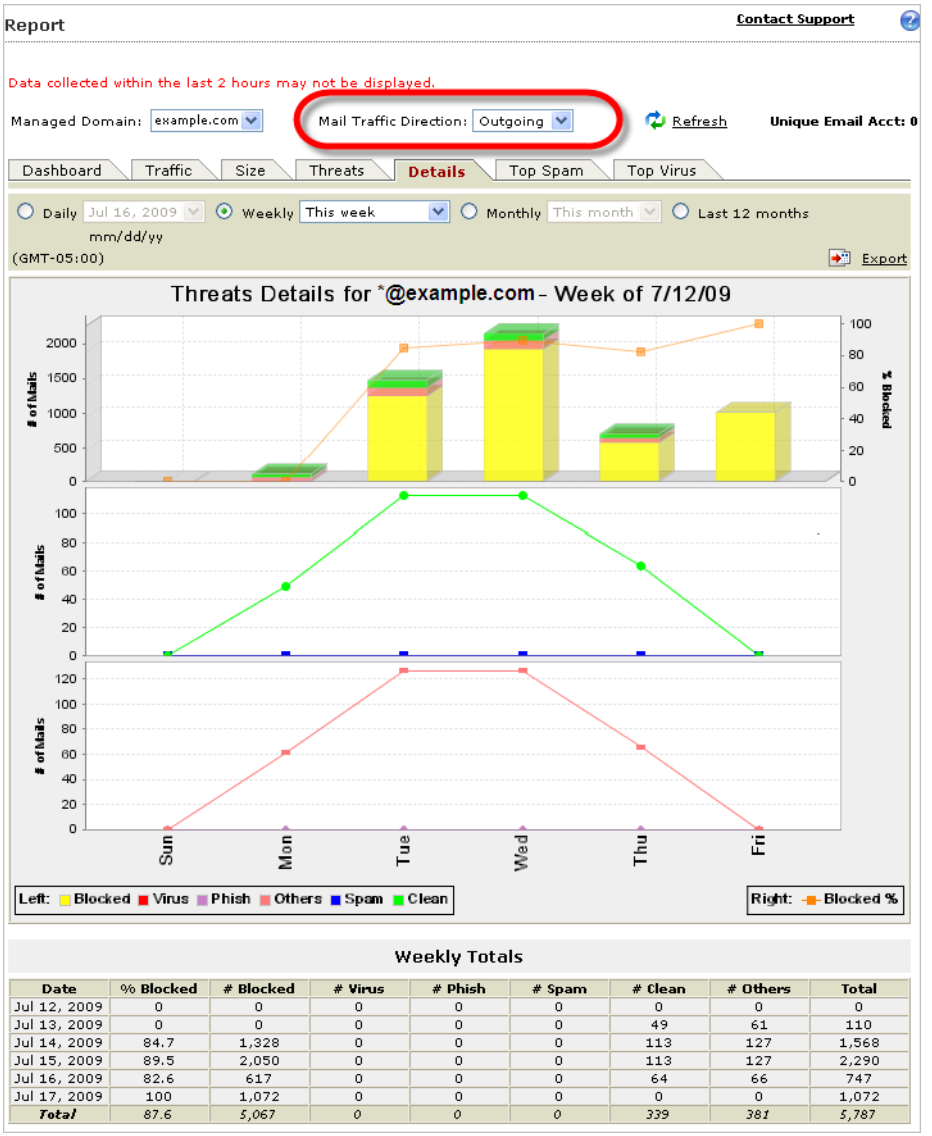
Note: To avoid clutter, the dashboard view of this report omits the legend.



Weekly Totals

Date	% Blocked	# Blocked	# Virus	# Phish	# Spam	# Clean	# Others	Total
Jun 7, 2009	15	17	12	12	12	12	48	113
Jun 8, 2009	33.1	400	101	101	101	101	404	1,208
Jun 9, 2009	22.7	240	102	102	102	102	408	1,056
Jun 10, 2009	22.7	240	102	102	102	102	408	1,056
Jun 11, 2009	0	0	0	0	0	0	0	0
Jun 12, 2009	0	0	0	0	0	0	0	0
Jun 13, 2009	0	0	0	0	21	0	0	21
Total	*26*	*897*	*317*	*317*	*338*	*317*	*1,268*	*3,454*

FIGURE 2-14. Threats Details report screen (incoming traffic)



Weekly Totals

Date	% Blocked	# Blocked	# Virus	# Phish	# Spam	# Clean	# Others	Total
Jul 12, 2009	0	0	0	0	0	0	0	0
Jul 13, 2009	0	0	0	0	0	49	61	110
Jul 14, 2009	84.7	1,328	0	0	0	113	127	1,568
Jul 15, 2009	89.5	2,050	0	0	0	113	127	2,290
Jul 16, 2009	82.6	617	0	0	0	64	66	747
Jul 17, 2009	100	1,072	0	0	0	0	0	1,072
Total	*87.6*	*5,067*	*0*	*0*	*0*	*339*	*381*	*5,787*

FIGURE 2-15. Threats Details report screen (outgoing traffic)

Top Spam Tab

Click the **Top Spam** tab to display the Top Spam Recipients (*figure 2-16*) or the Top Spam Senders report, which show the top spam recipients or senders for the selected mail domain depending on the selected mail traffic direction. The default reporting period is the *current week*. Top spam recipient reports are displayed in GMT time.

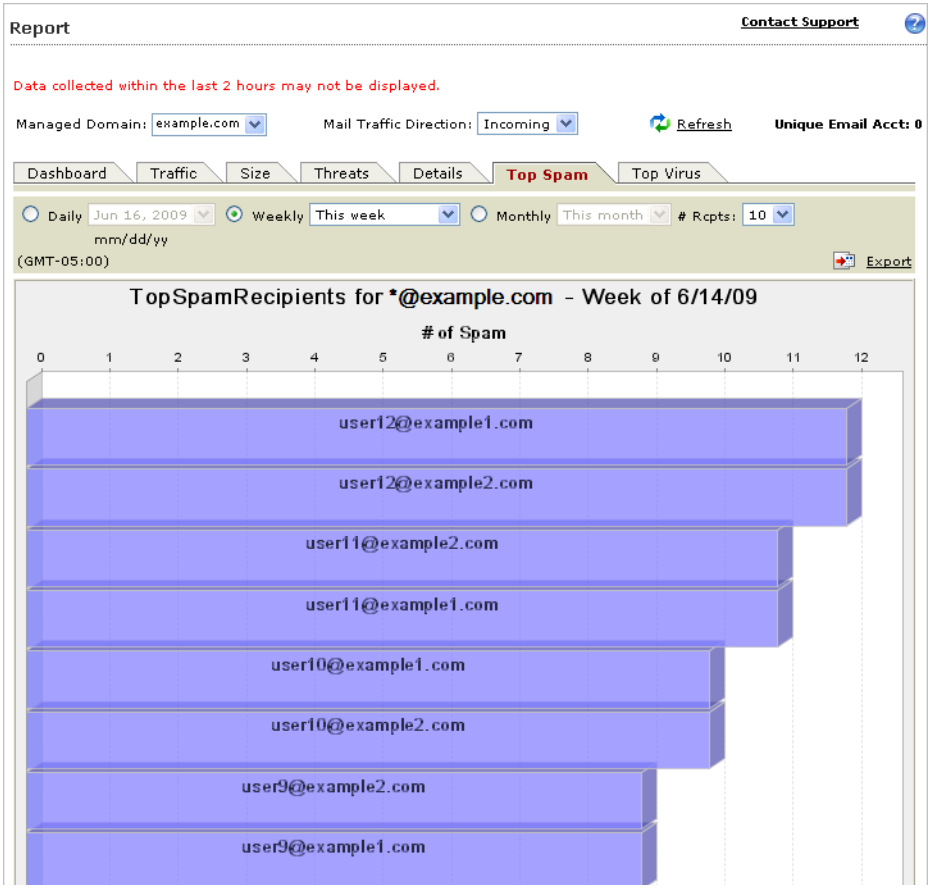


FIGURE 2-16. Top Spam Recipients report screen (incoming traffic)

Top Virus Tab

Click the **Top Virus** tab to display the Top Virus Recipients (*figure 2-17*) or the Top Virus Senders report for the selected mail domain. Select "incoming" in the mail traffic direction drop-down list to display the recipients report and "outgoing" for the senders report. The default reporting period is the *current week*. Top virus recipient/sender reports are displayed in GMT time.

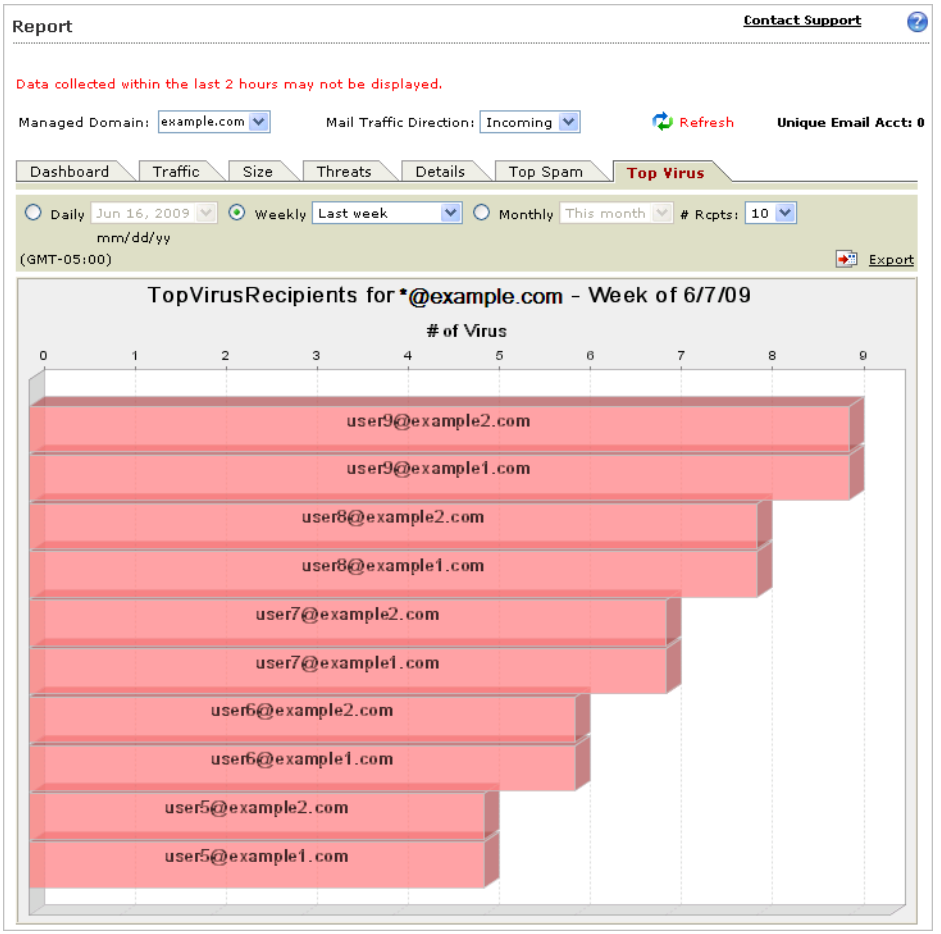


FIGURE 2-17. Top Virus Recipients report screen (incoming traffic)

Chapter 3

Managing Policies

This chapter provides guidelines for creating and managing scanning policies using the Hosted Email Security administrative console.

Topics in his chapter include:

Policy Overview

A Hosted Email Security 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.

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

Full Version customers have creation and modification rights.

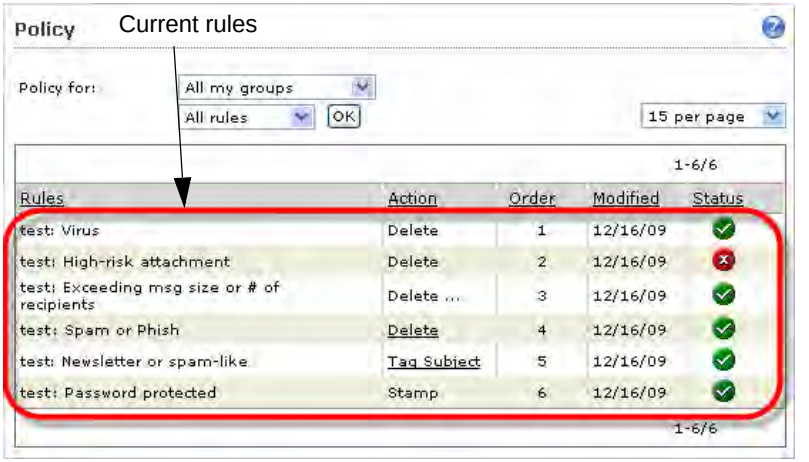


FIGURE 3-1. Policy screen, full version

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 a 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 Hosted Email Security. 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 Hosted Email Security—Inbound Filtering 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*.

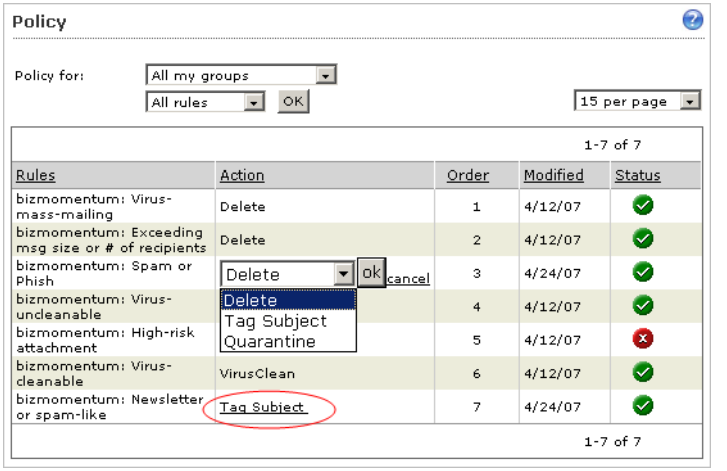


FIGURE 3-2. Spam rule options for users of Hosted Email Security—Inbound Filtering version

Default Policy Settings

The following rules makes up the default policy for all Hosted Email Security customers.

Hosted Email Security (full version) customers can edit the default rules as well as create new rules.

Hosted Email Security—Inbound Filtering 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 50MB or it has been sent to more than 50 recipients, then the message is deleted and Hosted Email Security notifies the sender about the deleted email. Hosted Email Security (full version) customers may modify this rule up to the system limit of 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 Hosted Email Security 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 in the Hosted Email Security Web-accessible quarantine for 21 days in the EMEA region and 15 days in all other regions.

Hosted Email Security (full version) 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 Hosted Email Security (full version) 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 in the Hosted Email Security Web-accessible quarantine for 21 days in the EMEA region and 15 days in all other regions.

Hosted Email Security (full version) 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 full version 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

For all Hosted Email Security (full version) users, 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

Hosted Email Security (full version) users can apply content filtering rules to email messages. Hosted Email 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 Hosted Email Security rules to match content as part of their operating logic. Hosted Email Security 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.

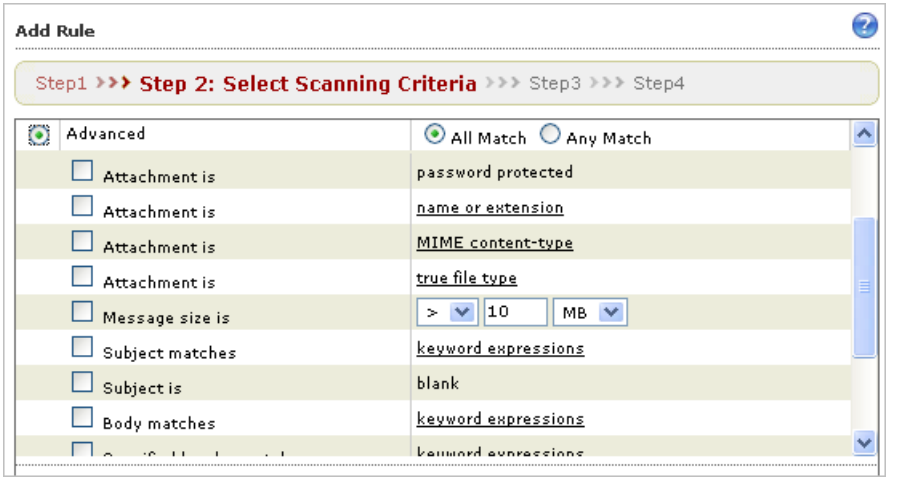


FIGURE 3-3. Content filtering options

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.

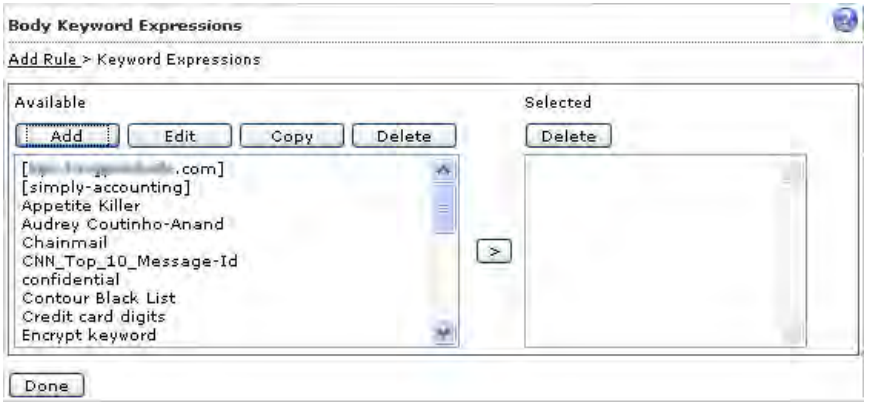


FIGURE 3-4. Keyword Expressions screen

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**. Hosted Email Security records your selections and redisplays 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* on page 3-27.

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 redisplays 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, Hosted Email Security 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. Hosted Email Security cannot accept expressions inputted in incorrect regex syntax.

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

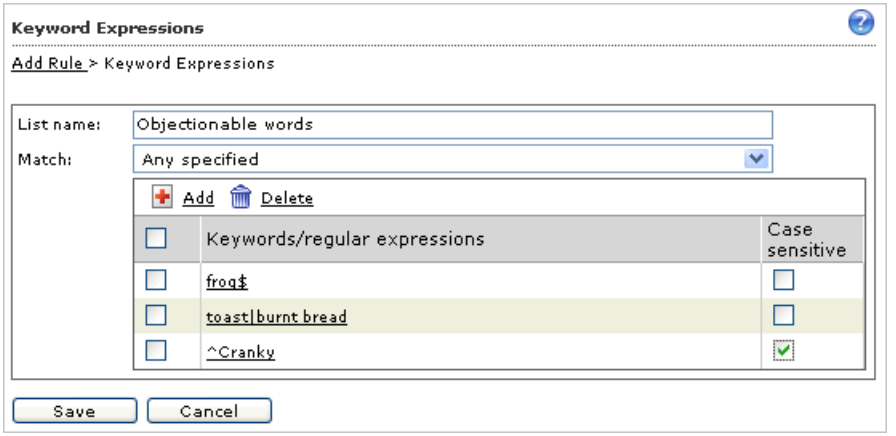


FIGURE 3-6. Keyword expressions have just been added

8. 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 3-12.

9. 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.

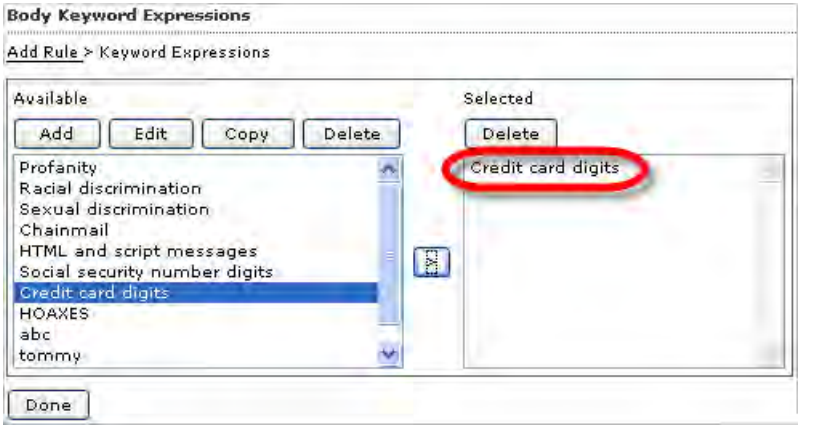


FIGURE 3-7. Adding a keyword expression to a rule

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.** Hosted Email Security adds your criteria to the rule that you are creating.
11. Click **Next** and complete the rule as explained in *Adding a New Rule* on page 3-27.

Weighting Keyword Expression Lists

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

When 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.

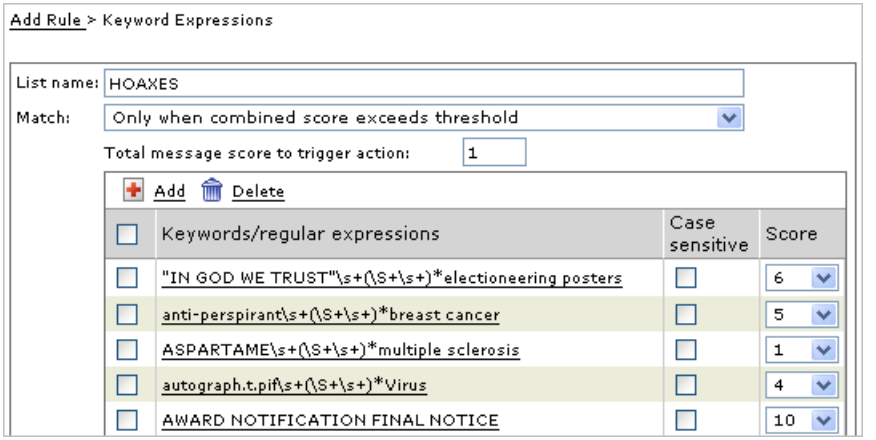


FIGURE 3-8. Weighting keyword expressions

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, Hosted Email Security 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, and then the rule will be triggered.

Rule Actions

Hosted Email Security provides a number of actions that you can use when building or modifying a rule. Actions available to Hosted Email Security (full version) users are:

These actions are executed in a pre-set order based on processing logic built into Hosted Email Security. For more information on execution order, see *Execution Order of Rules* on page 3-25.

Delete Entire Message

This action deletes the message and all attachments. The message is recorded as deleted in the Hosted Email Security logs, but once deleted, the message cannot be recovered. It falls into the Intercept category of actions (see *Intercept Actions* on page 3-25).

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, Hosted Email Security 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 Hosted Email Security 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 3-25).

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 Hosted Email Security. 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 Hosted Email Security 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 3-26).

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 screen, 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 3-26).

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 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 Hosted Email Security variables), whether they are to be inserted at the beginning or the end of the message body, and whether or not to avoid stamping Transport Neutral Encapsulation Format (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 3-26).

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 3-26).

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 Hosted Email Security 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 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 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 3-26).

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 screen, 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.**

Reject the Message

The Reject action blocks the message with certain types of attachments from the upstream MTA. The message is recorded as rejected in the Hosted Email Security logs, but once rejected, the message cannot be recovered.

Note: The "reject the message" action is only available in policies that protect against viruses or malware.

To configure a Scan Limitation rule action to reject a message:

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

Bypass a Rule

The Bypass action skips the specified rule and continues to check the message against the remaining rules in the policy. The action is recorded as bypassed in the Hosted Email Security logs.

Note: The "bypass this rule" action is only available in policies that protect against viruses or malware.

To configure a Scan Limitation rule action to bypass a message:

1. Select the **Bypass this rule** action from the Scan Limitation section.

   WARNING! The delivered message may contain a security risk.

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

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 Hosted Email Security. When an email message triggers a content-filtering rule that has encryption as its action, Hosted Email Security sends the email to the Hosted Email Security 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 3-7.

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 3-7.
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.** Hosted Email Security returns you to the Policy screen 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 3-22.

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

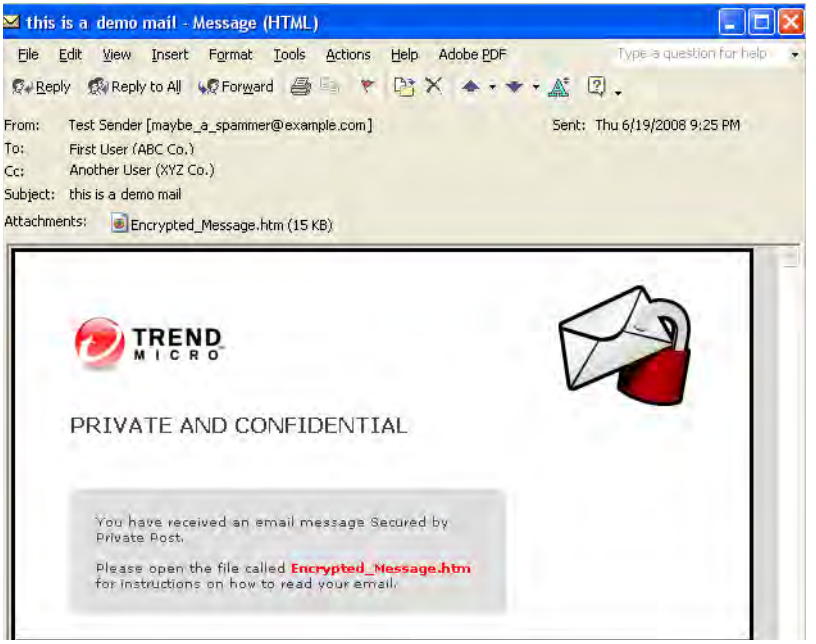


FIGURE 3-9. Encrypted message notification

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 verification 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 3-24.

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 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*
- *Scan Limitations*
- *Email Encryption Action*

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 3-30.)
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

There are two monitor actions:

- Send a notification message
- BCC another recipient

You can combine the first action with any other kind of action. You can combine the BCC action with "modify" actions (and with the first "monitor" action). However, the BCC action cannot be combined with terminal (intercept) actions.

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

Scan Limitations

There are two scan limitation triggers:

- Office 2007 file contains more than 353 files.
- Compressed archive contains more than 353 files.

Scan limitations can only be used with policies that protect against viruses/malware. They can be combined with any terminal or modify actions.

Email Encryption Action

This feature is available only to users with Hosted Email Security (full version).

The Trend Micro Email Encryption action option is enabled if you have purchased this separate service. The Email Encryption service is available only to Hosted Email Security (full version) 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, Hosted Email Security 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 and Modifying Rules

Only if you have Hosted Email Security (full version) can you add, modify, copy, or delete rules. For detailed guidelines, please see the sections below.

Adding a New Rule

Rules are the means by which messaging policies are applied to message traffic in Hosted Email Security. 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 Hosted Email Security 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.

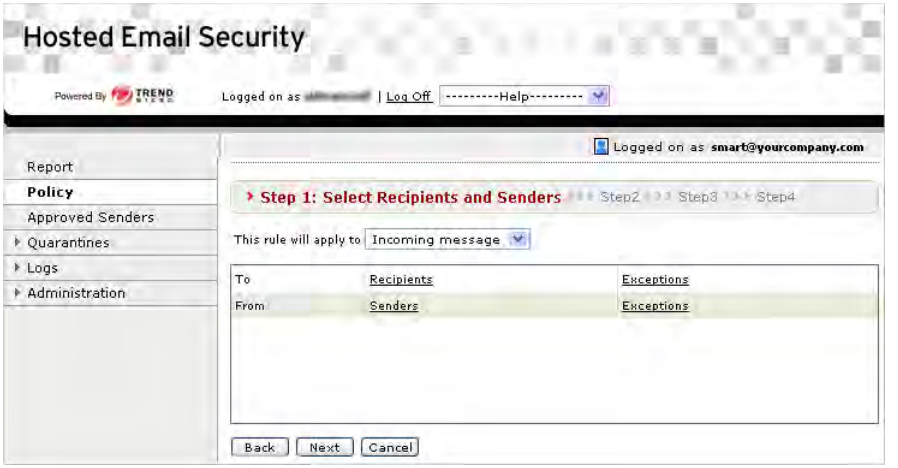


FIGURE 3-12. Add Rule screen

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

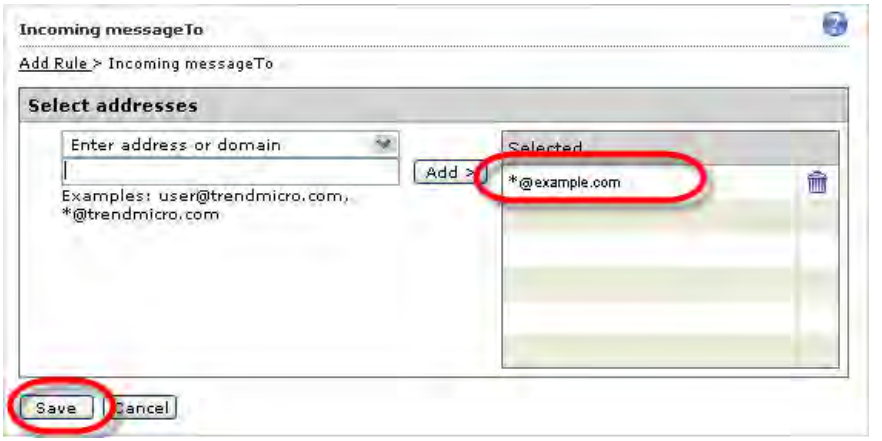


FIGURE 3-13. Adding domain and users on this screen.

3. Select and configure the criteria.

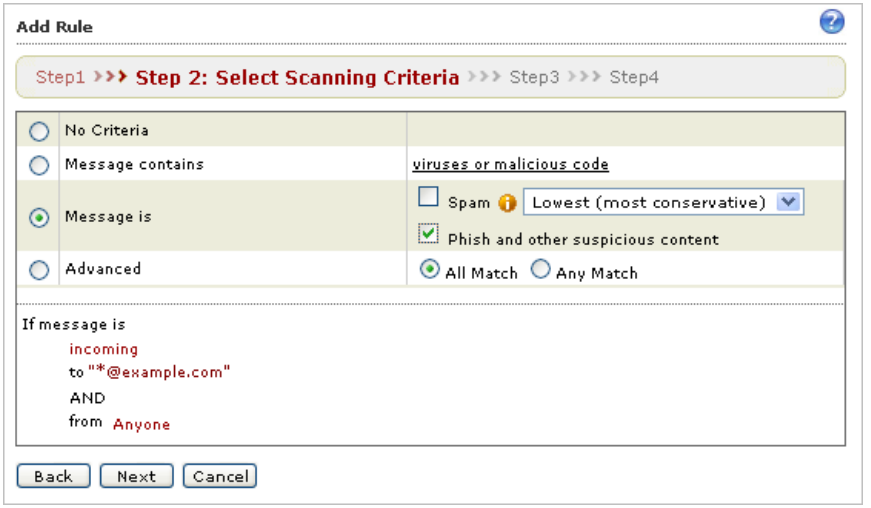


FIGURE 3-14. Select criteria for the rule on this screen.

4. Select and configure the intercept action.

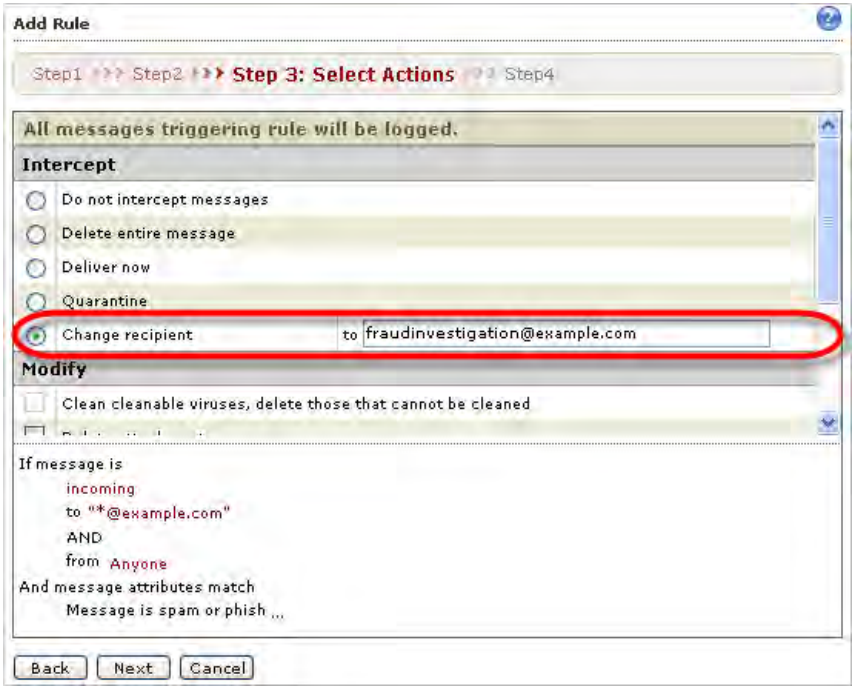


FIGURE 3-15. Select action on this screen

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 *figure 3-16* appears.

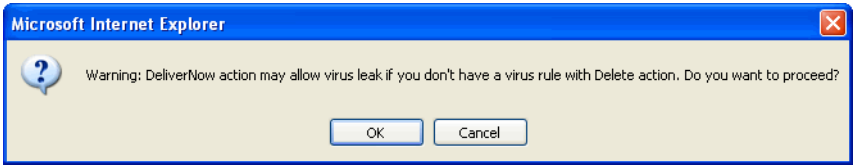


FIGURE 3-16. Deliver Now warning message

5. Optionally, select any Modify or Monitor actions, as shown in *figure 3-17* below. For virus policies you can also select Scan Limitation actions.

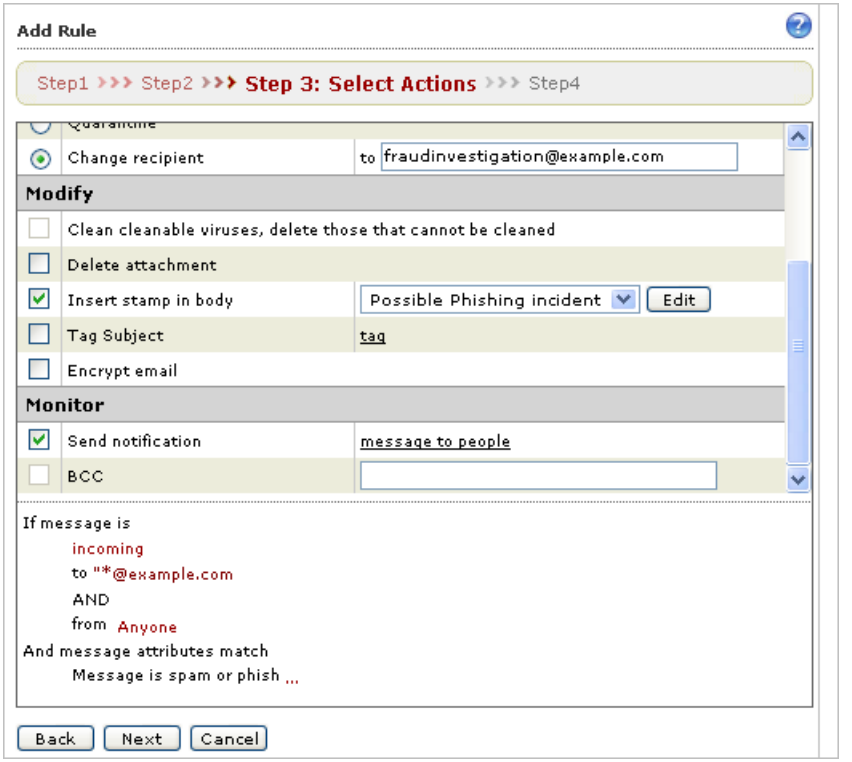


FIGURE 3-17. Step 3: Selecting Modify and Monitor actions

6. Name and enable the rule.

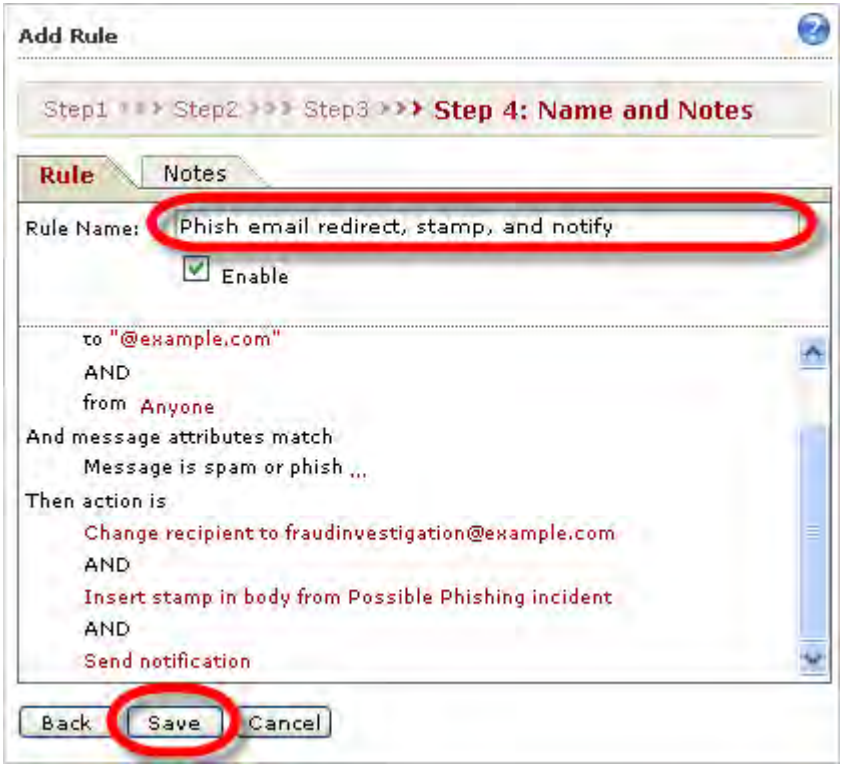


FIGURE 3-18. Name and save the rule on this screen

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.

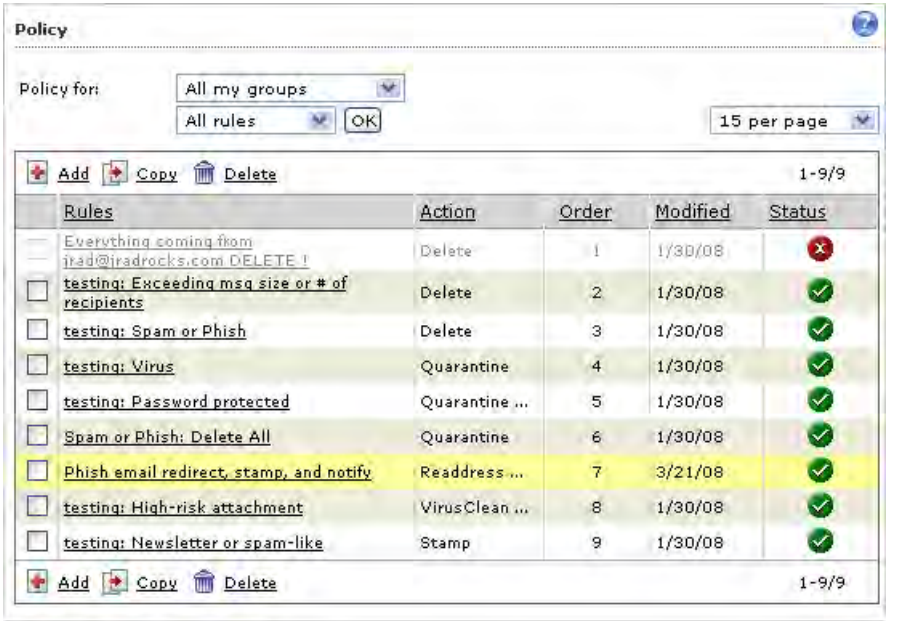


FIGURE 3-19. Policy screen showing newly created policy

Editing an Existing Rule

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 the example shown in *figure 3-20* on page 3-35, "ceo@example.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.

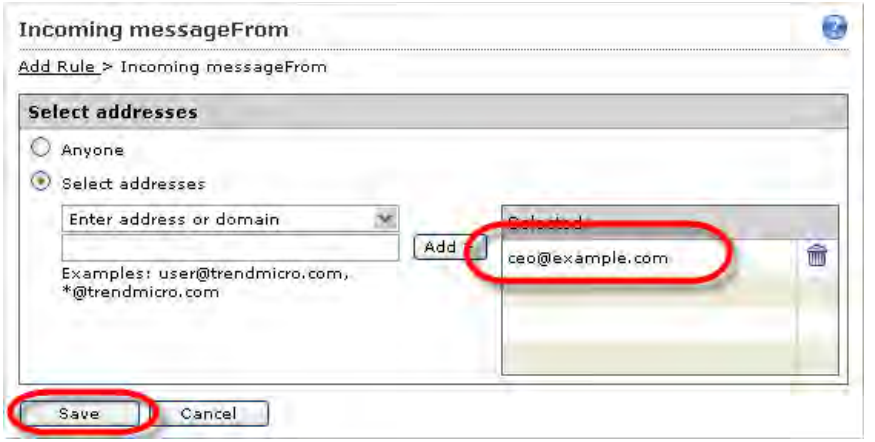


FIGURE 3-20. Edit sender exceptions on this screen.

4. Click **Save** to continue.

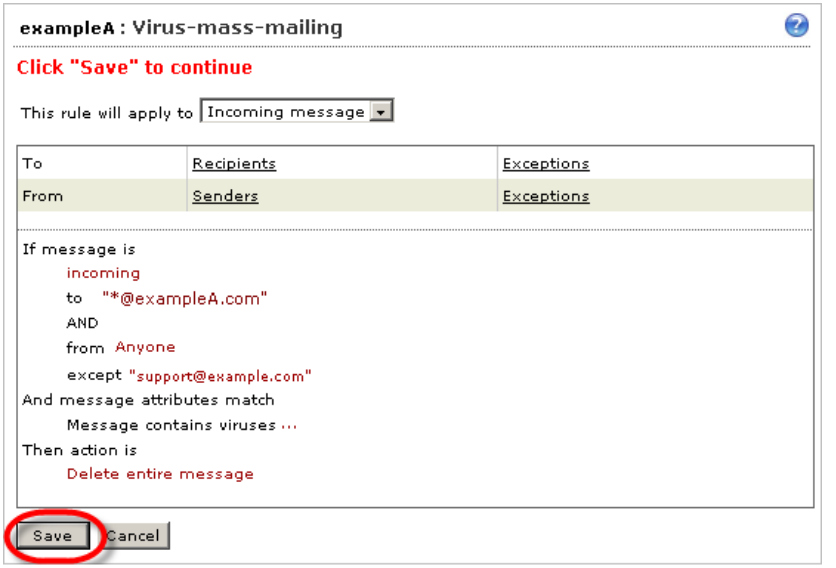


FIGURE 3-21. Edit Policy screen

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

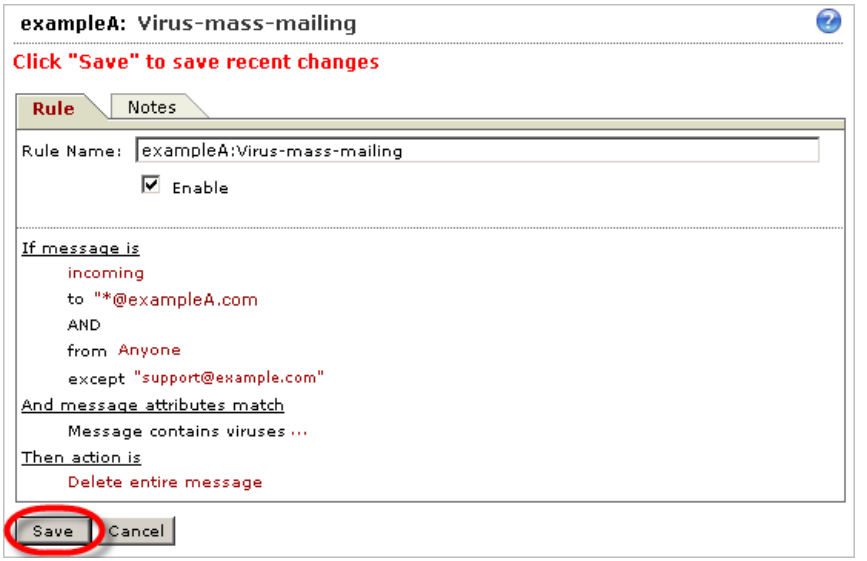


FIGURE 3-22. Save Policy changes on this screen

Copying an Existing Rule

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

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**.

Chapter 4

Approved Senders, Quarantine, and Logs

This chapter provides guidance on setting approved senders, accessing the quarantine, using the spam digest email, using the Web End User Quarantine, and interpreting Hosted Email Security logs.

Topics in this chapter include:

Approved Senders

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

Note: This screen is separate from the IP Reputation Approved/Blocked lists (**IP Reputation > Approved/Blocked**). On this screen you can approve email addresses or domains so that they are not scanned; the Approved/Blocked screen under IP Reputation applies to IP reputation checks only.

For approved senders:

- Hosted Email Security 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

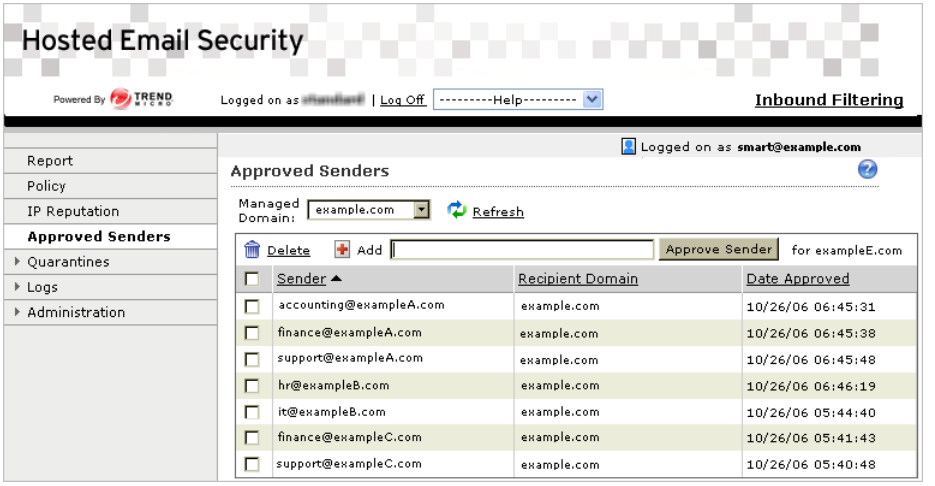


FIGURE 4-1. Approved Senders screen

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

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 Hosted Email Security (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. Hosted Email Security selects all messages on the screen.
2. Click **Delete** or **Deliver (Not Spam)**. Hosted Email Security deletes all the messages in the list.

Quarantine Settings

On the Quarantine settings screen (Figure 4-2) 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.

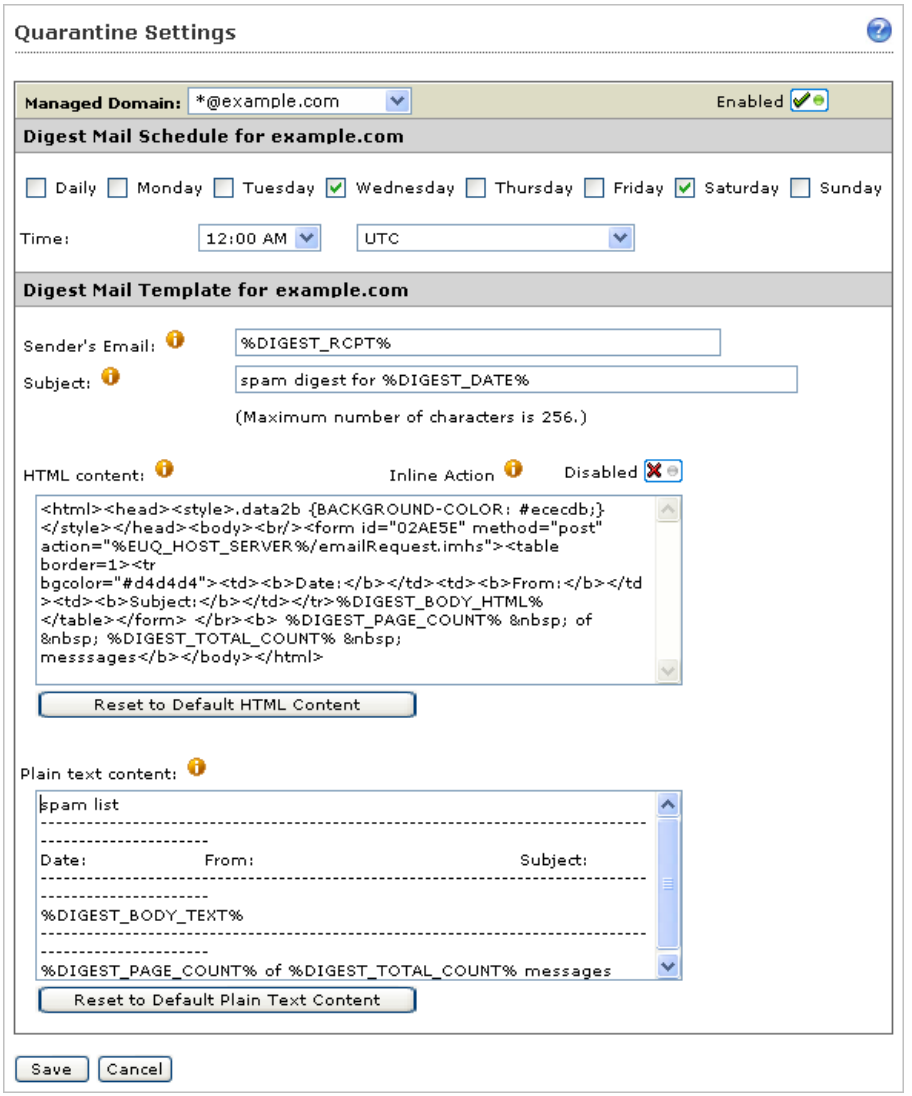


FIGURE 4-2. Quarantine Settings for spam digest message configuration

To configure the spam 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 spam 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 in the Hosted Email Security Web-accessible quarantine for 21 days in the EMEA region and 15 days in all other regions.

---

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 4-4*.)
   - **Plain text content** — Content that will appear if the email client of the end user allows only plain text email messages (See *figure 4-3*.)
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 4-1*.

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 4-1. 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 4-1. 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 () 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 4-4. The icon changes to the "Enabled" icon () 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.

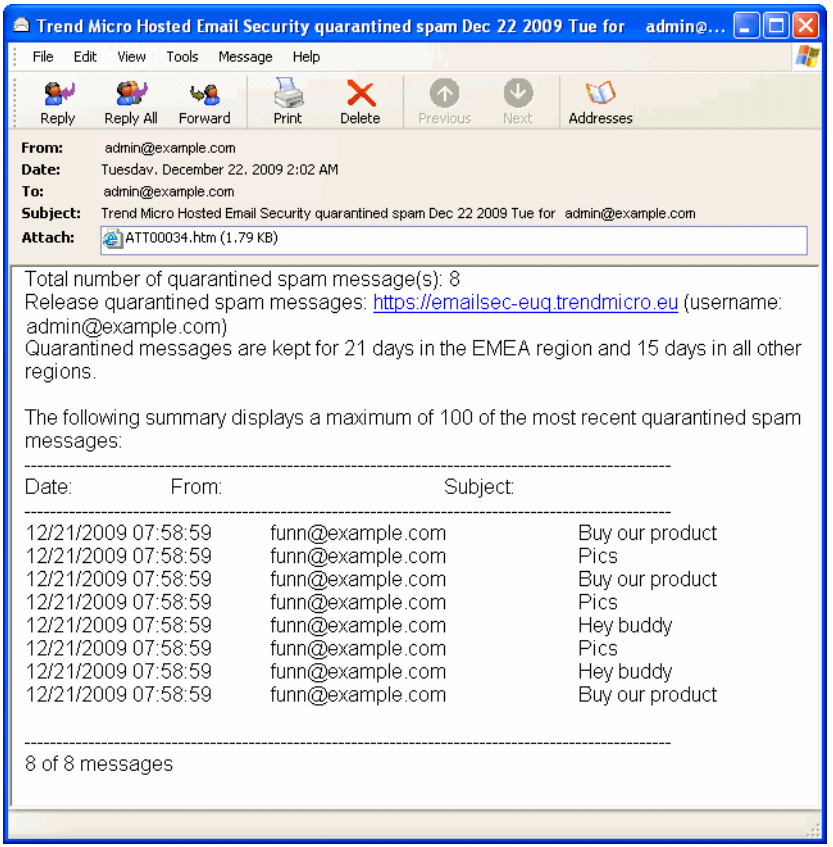


FIGURE 4-3. Sample of plain text spam digest email message

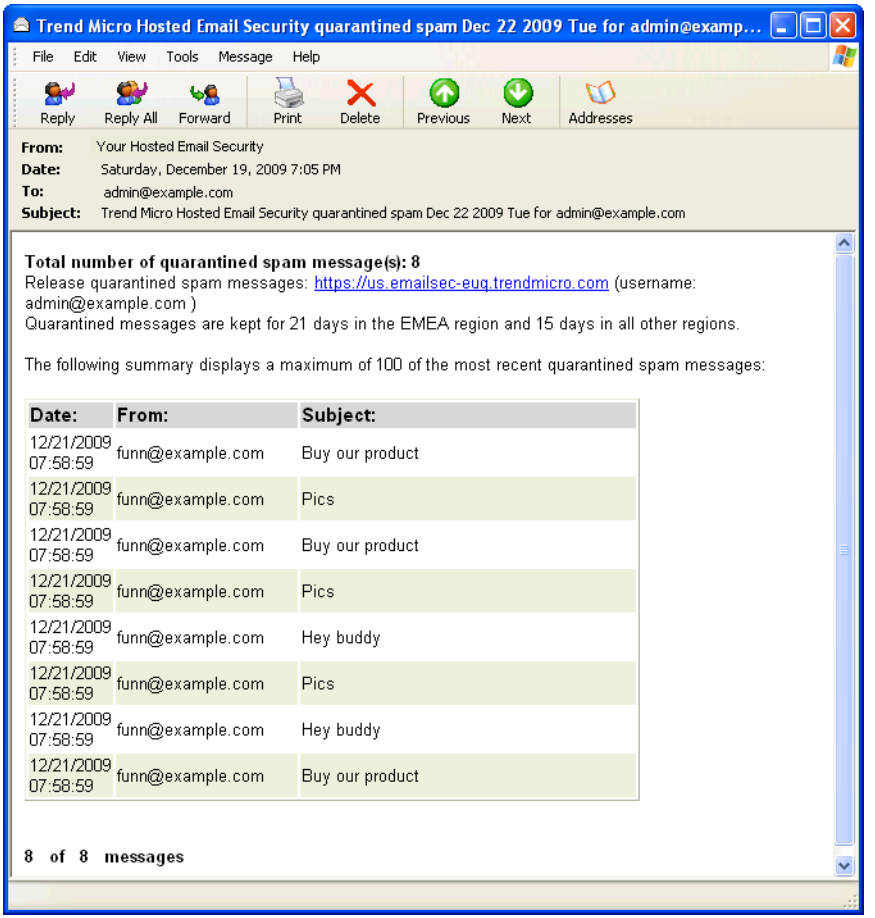


FIGURE 4-4. Sample HTML digest email message with inline action disabled (shortened list for readability)

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 logon screen.
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, Hosted Email Security will not add the sender to the approved sender list, because the message itself is no longer in the quarantine, and so Hosted Email Security has no way of identifying the sender. You will still see the response screen message as before, however:

   ```
   Hosted Email Security 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.**

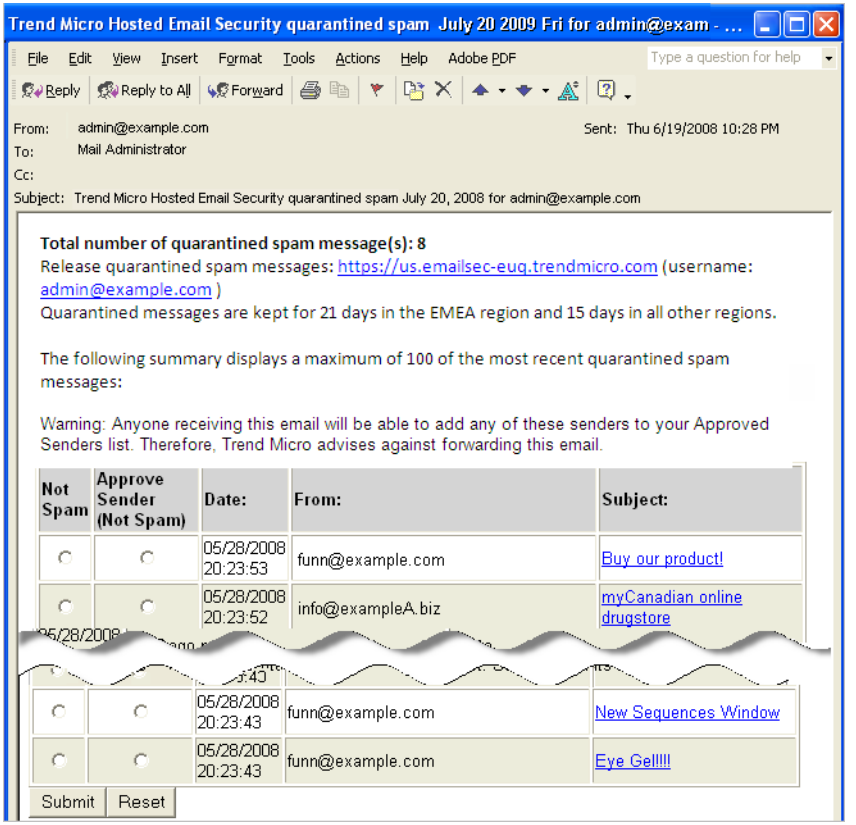


FIGURE 4-5. Sample HTML spam digest email message with inline action enabled (truncated for readability)

Web End-User Quarantine

The Hosted Email Security 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 Hosted Email Security Web EUQ at the following URLs.

For users in Europe, the Middle East, and Africa (EMEA):

http://emailsec-euq.trendmicro.eu

For users in the United States and regions other than EMEA:

https://us.emailsec-euq.trendmicro.com

More information about Hosted Email Security Web EUQ is available in *Introducing Web EUQ* on page C-1, the Web EUQ online help or in the *Hosted Email Security 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 Hosted Email Security Web EUQ screen 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. An end user who resets the password will receive an authentication email almost immediately that will enable him or her to log on to Web EUQ.

Logs

The Logs section allows you to search for and view mail tracking logs based on a specific date or date range, sender, direction (incoming and, for Hosted Email Security (full version) customers, outgoing), or recipient. Mail tracking information is only available for the previous seven days.

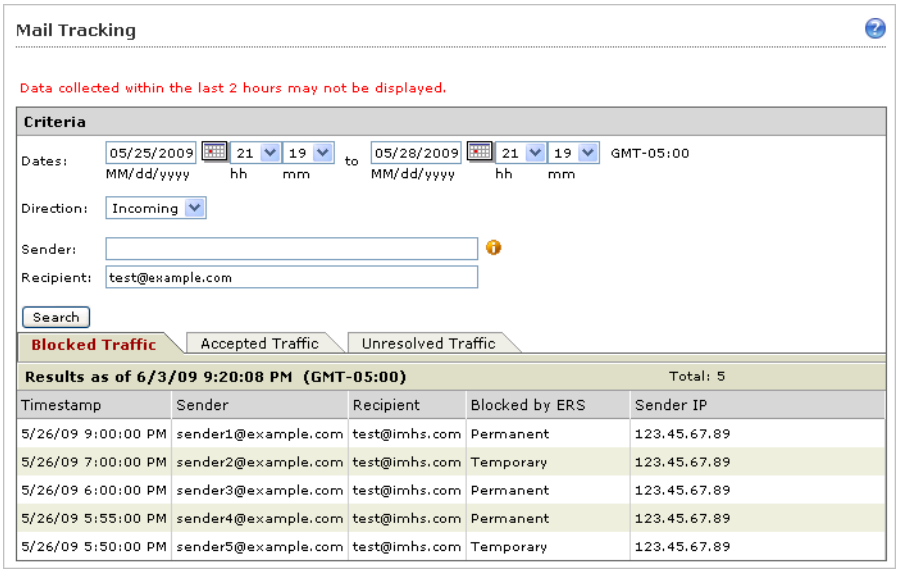


FIGURE 4-6. Mail Tracking screen showing results of query of incoming traffic

Mail Tracking Details

On the Mail Tracking screen, you can locate any message within the system using sender and recipient information. Hosted Email Security—Inbound Filtering users can query incoming mail. Hosted Email Security (full version) users can query either incoming or outgoing mail. The results table shows the status and the action taken on the message such as:

- Blocked or delayed at the system edge by reputation service (for incoming mail) or by the Hosted Email Security relay mail service (for outgoing mail)
- Accepted for processing and deleted with a virus
- Accepted, processed, and delivered
- Unresolved

Chapter 5

Administration and IP Reputation

This chapter provides guidance on configuring IP reputation settings and on several administrative tasks grouped under the Administration menu.

Topics in this chapter include:

IP Reputation Settings

Hosted Email Security can make use of the IP reputation features of Trend Micro Email Reputation Services (ERS), a separate Trend Micro service. Access these services by clicking **IP Reputation** on the left menu.

You can use the dynamic reputation slider to adjust how aggressively ERS blocks email connections. You can also choose how aggressively to block high-volume mail servers, as discussed in *Adjusting the IP Exclusion Settings* on page 5-4.

FIGURE 5-1. IP Reputation Settings screen

Using the Dynamic Reputation Slider

You can use the dynamic reputation slider to set blocking levels as follows:

- **More aggressive**—If too much spam is reaching your network, select a more aggressive setting. However, this setting may increase false positives by blocking connections from legitimate email senders.
- **Less aggressive**—If legitimate email is being blocked, select a less aggressive setting.

Tip: Trend Micro recommends that you make changes to the Dynamic Settings carefully and in small increments. You can then fine-tune your settings based on the increased amount of spam and legitimate messages received.

To adjust dynamic reputation settings:

1. From the left menu, choose **IP Reputation.** The IP Reputation Settings screen appears.
2. Move the slider to one of the following points:

   Level 4: The most aggressive setting. If Email Reputation Services (ERS) detects even a single spam message from a sender IP address, it adds the sender address into the dynamic reputation database. The length of time that the IP address stays in the database depends on whether ERS detects additional spam from the sender.

   Level 3: A moderately aggressive setting. ERS allows a small volume of spam from senders with a good rating. However, if ERS detects an increase in spam beyond the allowable threshold from such a sender, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database depends on whether ERS detects additional spam from the sender. The length of time may be extended up to maximum as in Level 4.

   Level 2: A moderately tolerant setting. ERS allows a larger volume of spam from a sender with a good rating. However, if ERS detects an increase in spam above the allowable threshold from such a sender, it adds the sender to the dynamic reputation database. The length of time that the IP address stays in the database is generally shorter than the time for level 3.

Level 1: The least aggressive setting. ERS allows the same amount of spam from a sender with a good rating as in level 2. The length of time that an IP address stays in the database is shorter, in general, than that for level 2.

Level 0: Queries the dynamic reputation database but does not block any IP addresses.

3. Click **Save**.

Note: The default setting is level 2, a moderately tolerant setting.

Adjusting the IP Exclusion Settings

High-volume mail servers can send a very large amount of mail, some of which will inevitably be spam. A high-volume mail server (typically, one for a large ISP) may send a high enough number of spam messages that Email Reputation Services (ERS) places the IP of the mail server on a blocking list. You may wish to prevent ERS from blocking such a high-volume mail server, however, because of the possibility of blocking too many legitimate messages.

In addition to adjusting the general aggressiveness of the reputation settings by using the dynamic reputation slider, you can set ERS to block only those high-volume mail servers that have a minimal spam reputation level of medium, low, or very low.

IP Exclusion Section

These "IP exclusion" settings work together with the dynamic reputation slider setting on the left. You can opt out of this feature by clearing the check box next to **Do not block high-volume mail servers (such as ISPs) if they have a reputation of.**

To select an exclusion level for high-volume mail servers:

1. On the IP Reputation Settings screen, on the right side of the Dynamic Settings section, ensure that the check box next to **Do not block high-volume mail servers (such as ISPs) if they have a reputation of** remains selected (the default) and then select from the following options:
   - Medium Spam Rate
   - Low Spam Rate
   - Very Low Spam Rate (the default)
2. Click **Save.** ERS will exclude from automatic blocking any high-volume mail servers that meet the selected option.

Valid Mail Servers

If you select this check box, ERS will allow connections from all mail servers designated as "valid mail servers," whether they send spam or not. This list is based on customer submissions of their MTAs.

Selecting Standard IP Reputation Lists

You can choose which lists to enable from those that make up the standard email reputation database. By default, all lists are enabled. The default setting is the most effective combination for reducing spam levels, and it meets the needs of most customers.

WARNING! **If you disable some portions of the standard IP reputation database, you may see an increase in the amount of spam messages that reach your internal mail server for additional content filtering.**

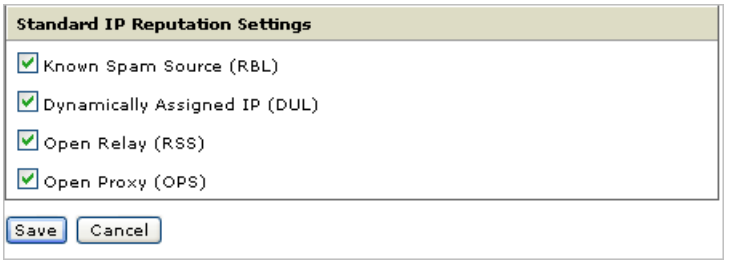


FIGURE 5-2. By default, all four standard IP reputation lists are selected

The standard IP reputation database includes the following four lists:

- **The Real-time Blackhole List (RBL)** is a list of IP addresses of mail servers that are known to be sources of spam.
- **The Dynamic User List (DUL)** is a list of dynamically assigned IP addresses, or those with an acceptable use policy that prohibits public mail servers. Most entries are maintained in cooperation with the ISP owning the network space. IP addresses in this list should not be sending email directly but should be using the mail servers of their ISP.

- **The Relay Spam Stopper (RSS)** is a list of IP addresses of mail servers that are open mail relays and are known to have sent spam. An open mail relay is a server that will accept mail from any user on the Internet that is addressed to any other user on the Internet, making it difficult or impossible to track spammers.
- **The Open Proxy Stopper (OPS)** is a list of IP addresses of servers that are open proxy servers and are known to have sent spam. An open proxy server is a server that will accept connections from any user on the Internet and will relay messages from those connections to any server on the Internet, making it difficult or impossible to track spammers.

Approved and Blocked Lists for IP Reputation

The "approved" and "blocked" lists for IP reputation, shown in *figure 5-4* on page 5-8, allow messages from the approved countries, ISPs, IP addresses, or CIDR ranges to bypass IP-level filtering. The approved and blocked lists are applied to your Hosted Email Security account, not to your MTA, but you can set up additional approved or blocked senders lists or perform additional filtering at your MTA.

The trade-off for bypassing IP filtering is the additional resources that are needed to process, filter, and store the higher levels of spam messages that would otherwise have been blocked. When using the approved and blocked lists, you may experience lower overall spam catch rates.

Note: The IP reputation "approved" lists are separate from the general "approved senders" list on the first level of the left menu. This screen applies to IP reputation checks only; on the general Approved Senders screen you can set up approved email addresses or domains so that Hosted Email Security does not scan them.

Block All Countries Except

In the Blocked tab there is one function not present in the Approved tab; you can choose to "block all countries except" a selected list of countries, as shown in *figure 5-3*.

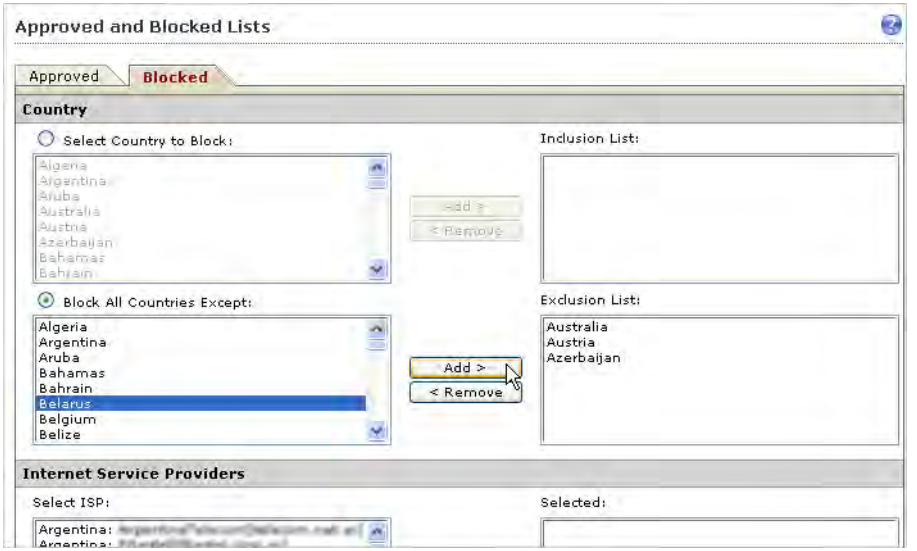


FIGURE 5-3. Approved and Blocked Lists screen: Block All Countries Except function

Using this function, you can configure Hosted Email Security to block mail from all countries except for the list of countries that your organization approves.

In the case of a standard reputation (RBL) service lookup, the order of the evaluation hierarchy is:

1. Approved IP
2. Blocked IP
3. Approved ISP or ASN
4. Blocked ISP or ASN
5. Approved country
6. Blocked country

For dynamic reputation (QIL) service lookup, the customer-defined "blocked policy lists" (IP, ISP/ASN, Country) are ignored; only the approved lists are checked. Otherwise, the order of policy lookup (first IP, then ISP/ASN, lastly country) is the same as for standard reputation (RBL) service.

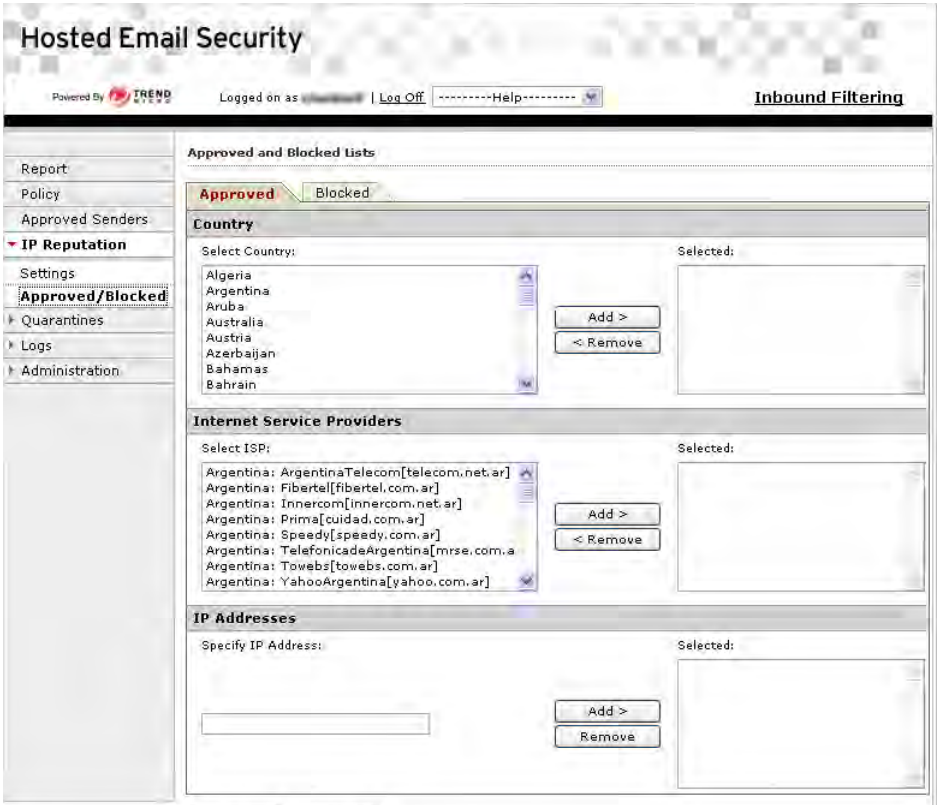


FIGURE 5-4. IP Reputation Approved and Blocked Lists screen

Troubleshooting IP Reputation Settings

If you encounter any unexpected errors while using the IP Reputation screen, you may be able to resolve the issue on your own. Please consult *table 5-1* below for guidance on resolving the problem before contacting technical support.

TABLE 5-1. IP Reputation Settings screen troubleshooting guide

ISSUE	POSSIBLE CAUSE	POSSIBLE SOLUTION
THE SAVE BUTTON IS DISABLED.	I do not have an Activation Code (AC).	Obtain a valid AC from your vendor.
	I have applied for an AC code, but it has not yet been added to the Hosted Email Security system.	Try again in a couple of hours.
	A temporary network issue is preventing Hosted Email Security from validating the AC code.	Try again in a few minutes.
I CANNOT SAVE MY IP REPUTATION SETTINGS.	There is a temporary network issue.	• Try again in a few minutes. • Log out, log on again, and retry.
	I have more than one browser window open to the IP Reputation screen of the Hosted Email Security site, and the session in the window that was opened first has expired.	Switch to the most recently opened window and close the other window.

Administration

In the Administration section, you can find links to screens pertaining to the following topics:

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 Hosted Email Security Web End-user Quarantine (EUQ) service.

All Hosted Email Security 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.)

FIGURE 5-5. 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 for the Web EUQ

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

To reset an end-user password:

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

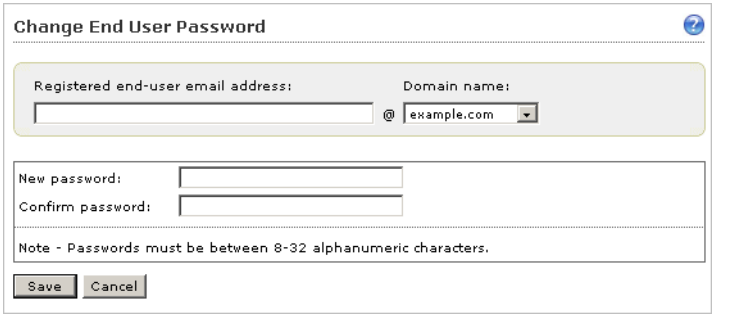


FIGURE 5-6. Change end-user password screen

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 on.

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 Hosted Email Security Web EUQ logon screen.

Managing Directories

Hosted Email Security uses user directories to help prevent backscatter (or "outscatter") spam and Directory Harvest Attacks (DHA). You can import user directories to let Hosted Email Security know legitimate email addresses and domains in your organization. Hosted Email Security 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 Hosted Email Security is using. Hosted Email Security 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 Hosted Email Security service with another administrator, that administrator will not see the directories for that account upon logging on.
- Every time you add more users to your network, you must import your updated user directories; otherwise, Hosted Email Security 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 Hosted Email Security; 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.

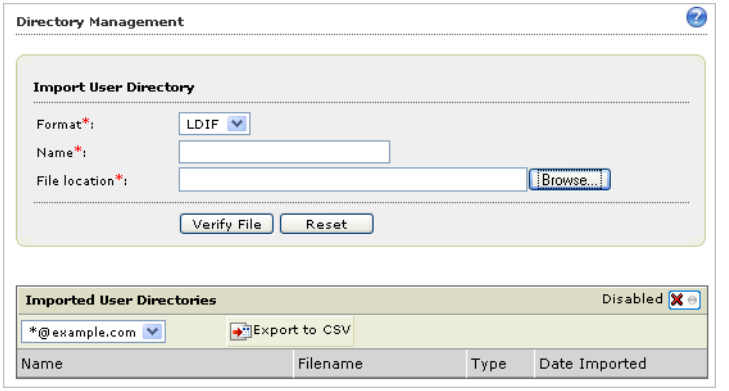


FIGURE 5-7. Directory management screen

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 Hosted Email Security service.
   - **Invalid domains**—Domains that are included in your directory file, but are not officially used on your Hosted Email Security service. Hosted Email Security 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:  . Hosted Email Security 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 5-14).
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 ().

Managing Domains

As an alternative to manually supplying Trend Micro Hosted Email Security technical support with your company domains, you can use the Domain Management screen to add, modify, or delete domains. Hosted Email Security uses the domain of the email sender to determine which IP reputation settings to apply (based on your settings).

Note: Hosted Email Security must have a record of your company domains in order to apply IP reputation settings to mail coming in to them.

Adding a Domain

To add a new domain:

1. Select **Administration > Domain Management** to open the Domain Management screen, as shown in *figure 5-8* below.

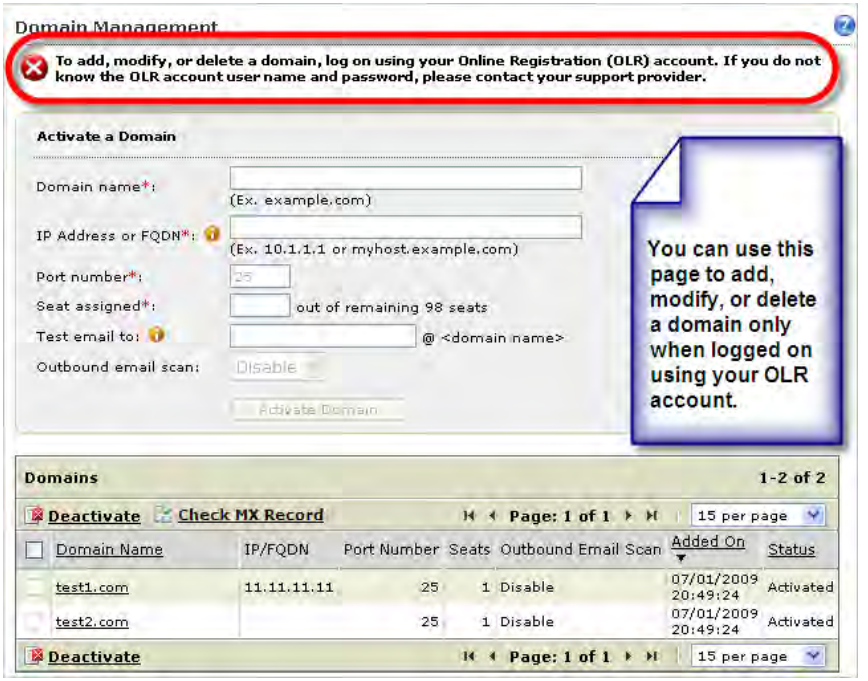


FIGURE 5-8. Hosted Email Security Domain Management screen, as seen when you log on using your old account (that is, not the OLR account)

2. Type the following information in the fields provided (required fields shown in bold):
   - The new **domain name**
   - **IP address or FQDN**(fully qualified domain name)
   - **Port number** of its mail server
   - Number of **seats assigned** to this domain

- The test email account (Use this email address as the recipient for a test message to confirm delivery through Hosted Email Security.)

3. If you have an Hosted Email Security (full version) account, select **Disable** or **Enable** from the **Outbound email scan** drop-down list.
4. Click **Activate Domain.** If the domain is valid and there is an MX record for the domain, the new domain, IP address or FQDN, port number, seats, and other information appear in the Domains table at the bottom of the screen and Hosted Email Security sends an email confirmation message to your administrative email address on record.

Note: The confirmation email that Hosted Email Security sends notifies you of whether the domain was successfully added. It may take 24-48 hours for the domain adding process to complete.

---

5. To immediately add the domain to the domain list:
   a. Wait for the confirmation email from Hosted Email Security.

WARNING! **Do not modify your MX record before receiving the confirmation email.**

---

   b. Modify your MX record to include the domain.
   c. Select **Administration > Domain Management** to open the Domain Management screen.
   d. Select the added domains in the domain list. The domain's status will be **Verifying**.
   e. Click **Check MX Record** to verify that the domain's MX record points to the Hosted Email Security Inbound MTA Server.

Confirming Mail Delivery Through the Service

When adding the first domain to Hosted Email Security, be sure to enter a test email address, as mentioned in *Step 2* in *Adding a Domain*. After adding the domain but before redirecting your MX record, send a test email message to the email account that you entered and confirm that mail is flowing freely through Hosted Email Security. If you do not receive the test message, contact your service provider.

WARNING! **Do not modify your MX record before receiving the confirmation email.**

Modifying a Domain

You can modify domain information on the **Domain Management > {your-domain}** screen, which you can access by clicking the domain name in the Domains table at the bottom of the screen. See *figure 5-9* for this screen.

To modify a domain:

1. Select **Administration > Domain Management** from the left menu to open the Domain Management screen, as shown in *figure 5-8*.
2. Click the domain name in the table at the bottom of the Domain Management screen. The **Domain Management > {your-domain-name}** screen appears, with its fields pre-filled with the information on record for that domain.
3. Modify the fields needed and click **Save.**

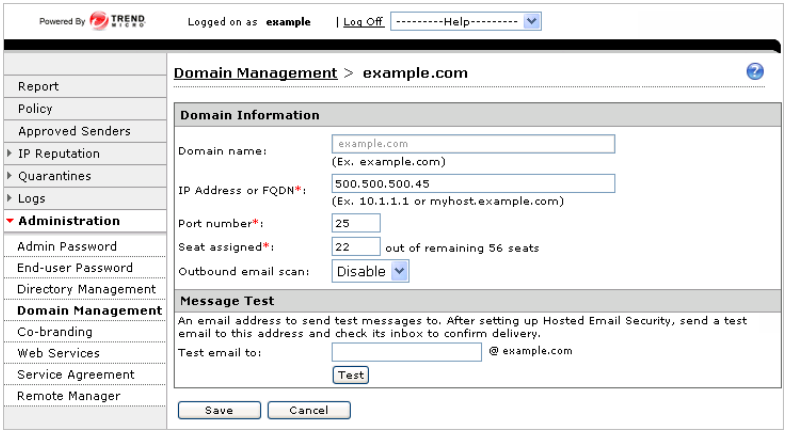


FIGURE 5-9. Modifying domain information on the Domain Management > {your-domain} screen (writable only when logged in with OLR account)

You can also de-activate a domain on the Domain Management screen.

To deactivate a domain:

1. Select **Administration > Domain Management** from the left menu to open the Domain Management screen, as shown in *figure 5-8*.
2. Select the check box next to the domain to de-activate.
3. Click the **Deactivate** link in the header or footer of the table, as shown in *figure 5-9* on page 5-20. Your de-activation request is submitted to Trend Micro for action.

Co-Branding

Hosted Email Security enables you to display your company logo on the web console top banner and in the logon page.

As a reseller, you can co-brand the Hosted Email Security administrative console, the Web EUQ interface, or both. You can set different domains with the same or different logos or can allow the domain administrators to set the logo to be displayed for their domain. You can also leave the feature disabled.

Logo Specifications

Before attempting to establish a co-branded site, 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

Co-branding the Administrative Console

1. Click **Administration > Co-branding.** The Co-branding screen appears, as shown in *figure 5-10*.
2. Click the "Disabled" icon (Disabled) in the upper right corner to enable the feature. The icon changes to its "enabled" form (Enabled).

Note: Co-branding is disabled by default.

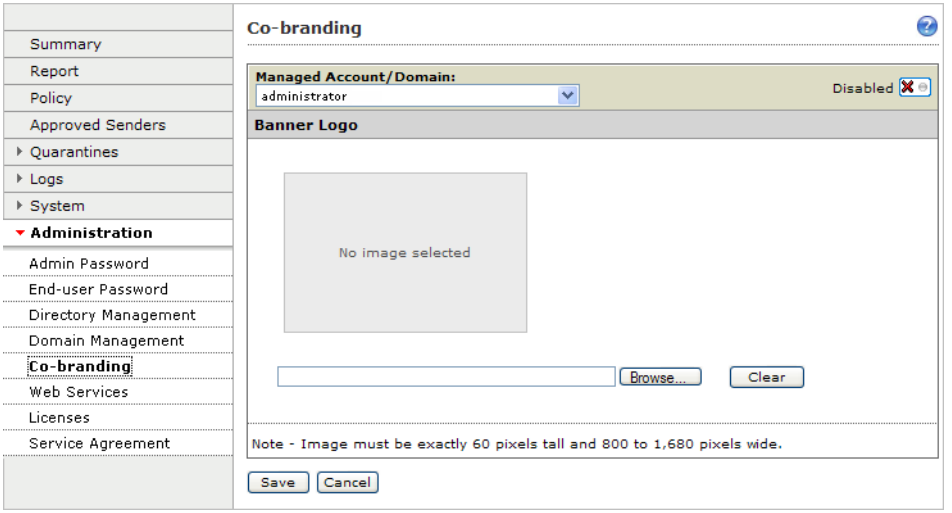


FIGURE 5-10. Co-branding screen

3. From the **Managed Account/Domain** drop-down list, select the name of the account that will display the logo, as shown in *figure 5-11*, below.

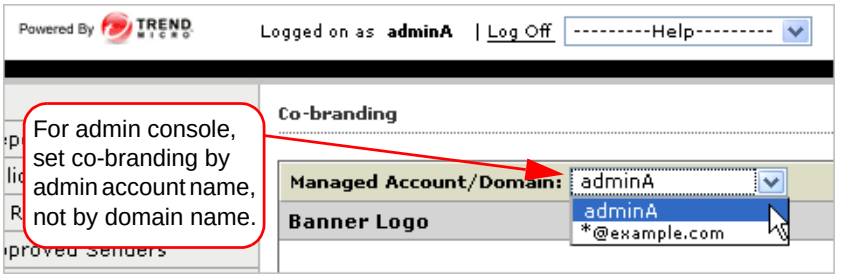


FIGURE 5-11. Co-branding the administrative console (select account name, not domain name)

4. Click **Browse** and browse to the location of the logo file. (To remove the logo, click **Clear.)**
5. Click **Open,** and a preview of the logo displays, as shown in *figure 5-12*.

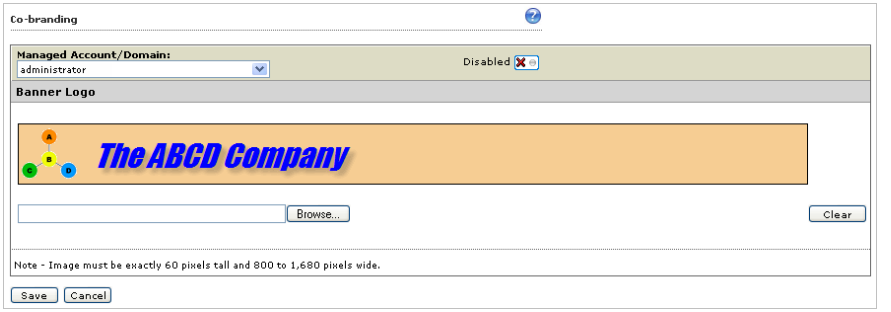


FIGURE 5-12. Display of domain logo to be set

6. Click **Save**. The logo image will display in the top banner of the Hosted Email Security administrative console (see *figure 5-14*) and in the logon screen when accessed as explained in *Accessing a Co-Branded Site* on page 5-25.

Co-Branding the Web EUQ Interface

As a reseller, you can also co-brand the Web EUQ interface. The procedure is almost identical to that for establishing a co-branded version of the Hosted Email Security administrative console, with one small exception, as explained below.

To set up a co-branded version of the Web EUQ:

1. Click **Administration > Co-branding.** The Co-branding screen appears, as shown in *figure 5-10*.
2. Click the "Disabled" icon (Disabled) in the upper right corner to enable the feature. The icon changes to its "enabled" form (Enabled).

Note: Co-branding is disabled by default.

---

3. From the **Managed Account/Domain** drop-down list, select the domain name for which the logo will display, as shown in *figure 5-13* below.

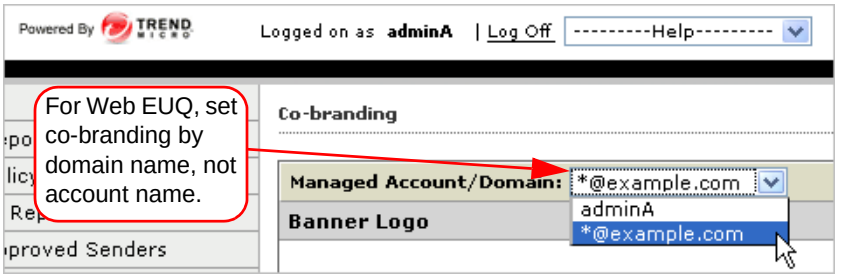


FIGURE 5-13. Co-branding the Web EUQ (select domain name, not account name)

4. Click **Browse** and browse to the location of the logo file. (To remove the logo, click **Clear.)**
5. Click **Open,** and a preview of the logo displays, as shown in *figure 5-12*.
6. Click **Save**. The logo image will display in the top banner of the Hosted Email Security Web EUQ and in the EUQ logon screen (see *figure 5-15*) when accessed as explained in *Accessing a Co-Branded Site* on page 5-25.

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 an account name will display only in the Hosted Email Security administrative console. The logo selected for a domain

will display only in the banner bar of the Hosted Email Security Web EUQ associated with that domain.

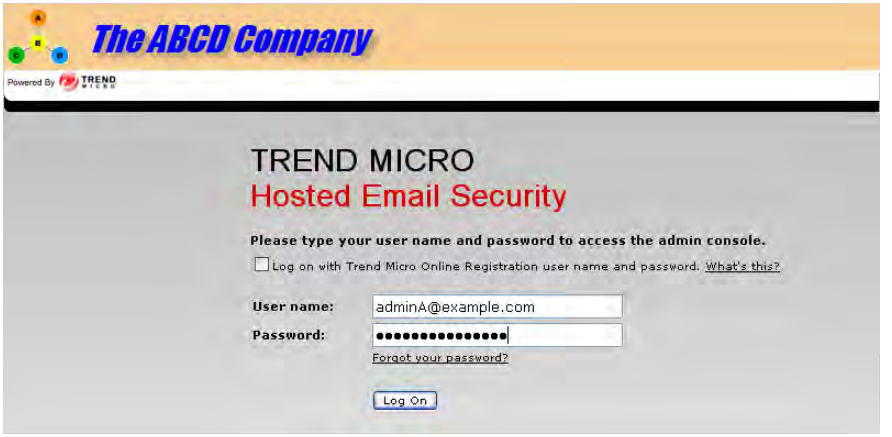


FIGURE 5-14. Sample reseller logo set in banner bar on logon screen of Hosted Email Security

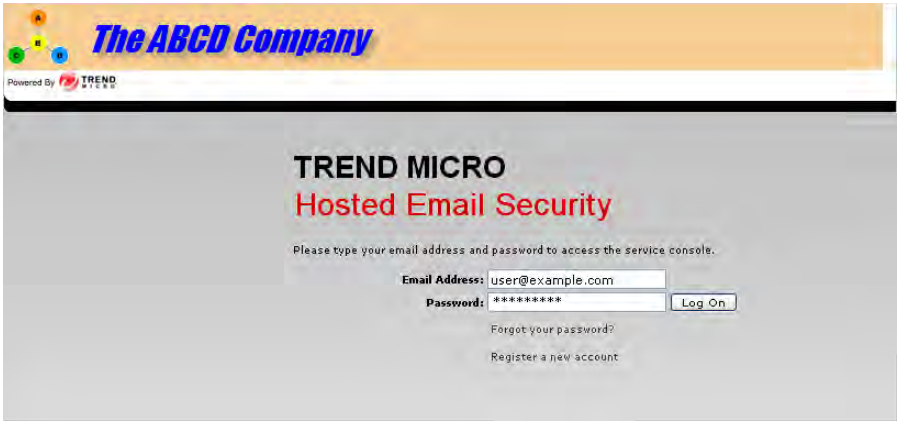


FIGURE 5-15. Domain logo displays in banner bar of logon screen of Hosted Email Security Web EUQ

Accessing a Co-Branded Site

As a reseller, you can supply your customers with a URL by which to access the co-branded site.

Accessing a Co-Branded Administrative Console

You have different options for accessing a co-branded administrative console, based on your logon type. If you registered your account using the Trend Micro Online Registration (OLR) Web site, append the OLR Hosted Email Security account name and "co-brand" to the base URL.

For example, assuming that "adminA" is the OLR Hosted Email Security account name, type the following into the browser address box:

"https://us.emailsec.trendmicro.com/**adminA/co-brand**"

If you did not register your account using the OLR Web site, you can still log on as before, by appending the original Hosted Email Security account name to the base URL as follows:

"https://us.emailsec.trendmicro.com/**adminA**"

Accessing a Co-Branded Web EUQ Site

To access a co-branded Web EUQ site, end users append the domain name to the base URL:

"https://us.emailsec-euq.trendmicro.com"

For example, assuming that "example.com" is the domain name, end users would type the following into their browser's address box:

"https://us.emailsec-euq.trendmicro.com/**example.com**"

Note: If an end user accesses a co-branded site without appending the account name or domain name, the site will still display and function, only without its co-branded appearance.

Web Services

Hosted Email Security enables you to access Hosted Email Security Web Services applications through an installed Hosted Email Security Web Service client in your environment.

There are three steps you need to take before accessing Hosted Email Security Web Services applications. First, you need a Service Authentication Key. This key is the global unique identifier for your Web Service client to authenticate its access to Hosted Email Security Web Services. Second, you need to enable the Hosted Email Security 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**

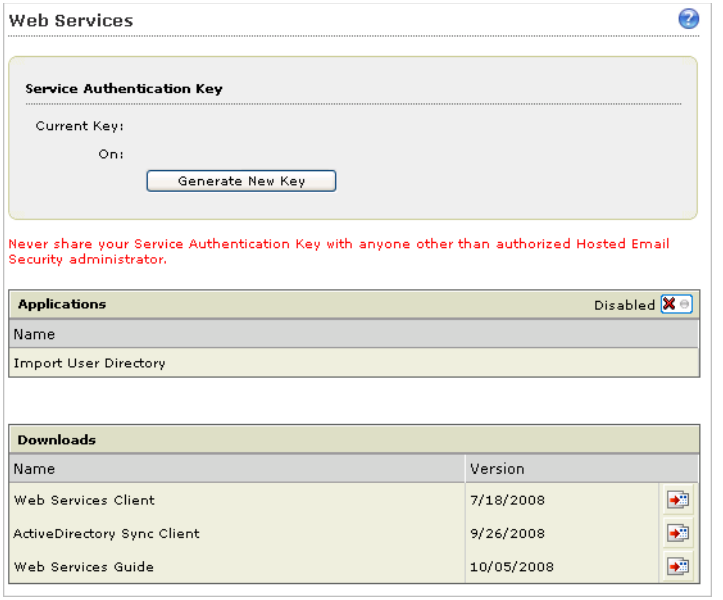
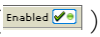


FIGURE 5-16. Web Services screen

2. Make sure a service authentication key is available. Current Key displays the key 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 service authentication key is like a password for your client to communicate with Hosted Email Security Web services. Please limit knowledge of this key to authorized Hosted Email Security administrators only.

   Note: If **Current Key** is blank, click **Generate New Key** to generate a service authentication key.

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 Hosted Email Security 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.

Downloading the Hosted Email Security Web Services Guide

Trend Micro has prepared a guide to help you understand and use the Web service. You can download the *Web Services Guide* in the Downloads section of the Web Services screen, as shown in *figure 5-17* on page 5-28.

Tip: Trend Micro recommends downloading and familiarizing yourself with the Web Services Guide before attempting any advanced Web services configuration.

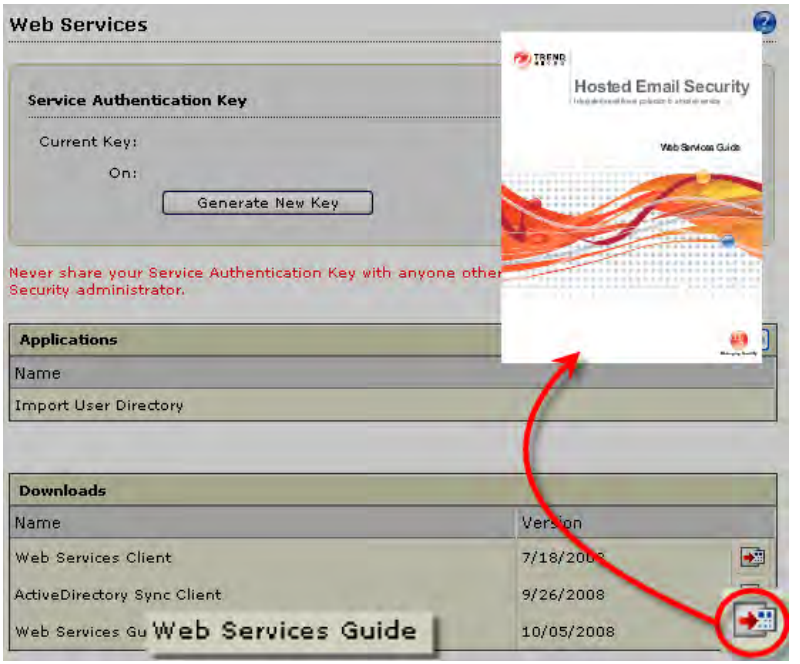


FIGURE 5-17. Download the Hosted Email Security Web Services Guide in the Downloads section of the Web Services screen

Viewing the Service Level Agreement

Trend Micro provides an aggressive Service Level Agreement (SLA) for Hosted Email Security that is intended to help your organization receive secure, uninterrupted email to support your business.

The Service Level Agreement covers availability, latency, spam blocking, false positives, antivirus, and support. Specific service-level guarantees are included in the most current version of the Hosted Email Security SLA, which you can view or download from the Service Level Agreement screen.

Note: Provisions of the SLA may vary among regions, so be sure to select your language and region when using this screen.

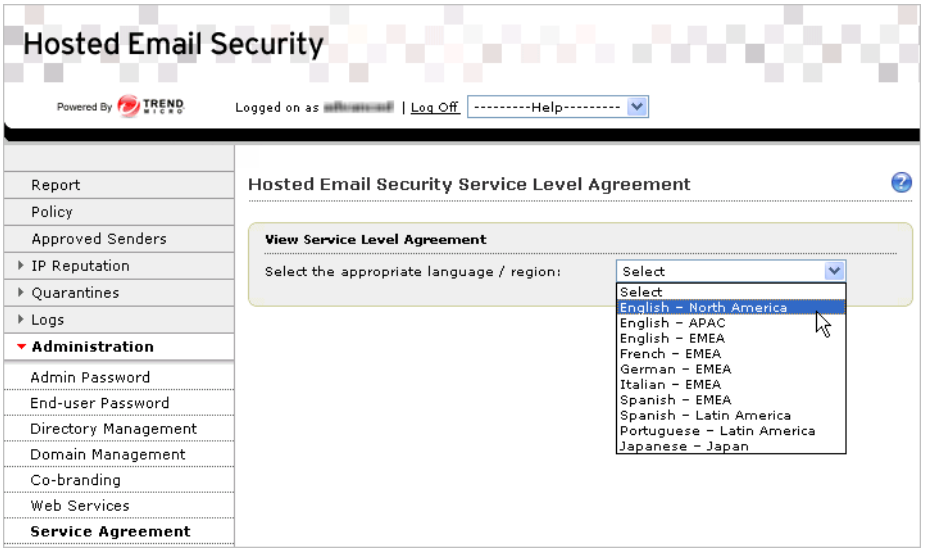


FIGURE 5-18. Hosted Email Security Service Level Agreement screen

To view the SLA for your region:

1. On the left menu, select **Administration > Service Agreement.** The Hosted Email Security Service Level Agreement screen appears, as shown in *figure 5-18*.

   Tip: Disable any pop-up blockers for your browser in order to download the SLA.

2. In the drop-down list, select your **language/region.** Hosted Email Security opens another browser window and displays an Adobe Reader (PDF) document of the appropriate SLA for your region, in the language that you have selected.

Note: Trend Micro reserves the right to modify the service at any time without prior notice. The current version of the Hosted Email Security service level agreement is available for review by paid customers and by customers conducting a trial.

Remote Management

You can use the Account Management Delegation screen, shown in *figure 5-19* to temporarily designate someone to manage the policies for your Hosted Email Security account. This feature can be useful for resellers, who often manage the accounts of several Hosted Email Security customers. Someone who has been delegated Hosted Email Security management ability can view and adjust all Hosted Email Security policies and settings by using a separate Trend Micro product, Trend Micro Worry-Free Remote Manager (WFRM).

Within the WFRM console, there is a summary display of Hosted Email Security settings. To manage Hosted Email Security from WFRM, the reseller clicks a link within WFRM that opens a Hosted Email Security window. From that window, the reseller can make any policy adjustments that you can make from the Hosted Email Security administrative console. (See the Trend Micro Web site for more information on this product.)

In order to delegate someone, you must know their Service Authorization Key. You can get that key from your reseller, who generates it from the WFRM product.

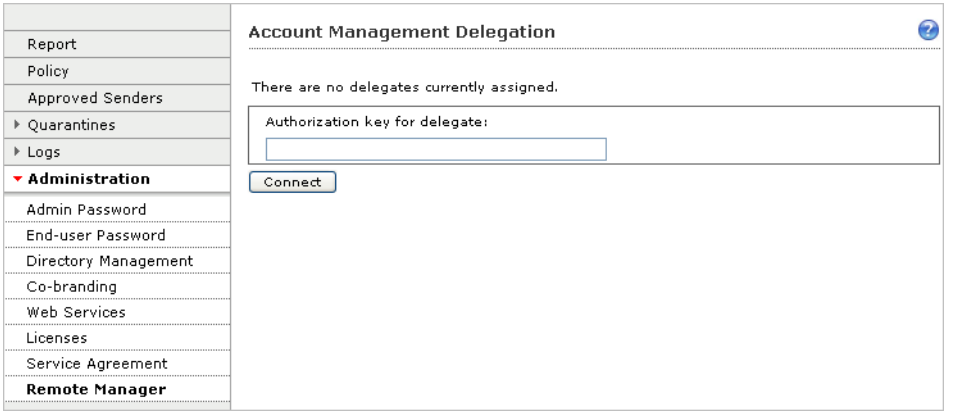


FIGURE 5-19. Remote management (Account Management Delegation) screen with no delegation

To delegate someone to manage an account remotely:

1. On the left menu, click **Administration > Remote Manager.** The Account Management Delegation screen appears, as shown in *figure 5-19* above.
2. Type or paste the service authorization key of the person to delegate account management to and click **Connect.** If the connection is successful, the screen will reload showing the name of the account and the designee, that person's street address, email address, mobile telephone number, the contract key, and the date that the delegation began, as shown in *figure 5-20* on page 5-31.

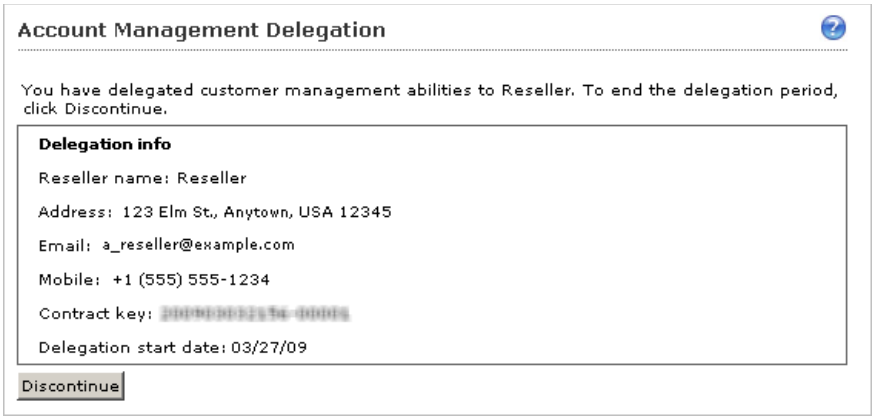


FIGURE 5-20. Remote management: account management delegated

You can discontinue the delegation at any time by clicking **Discontinue** on this screen.

The person to whom account management has been delegated can also discontinue the delegation from Worry Free Remote Manager. When the delegate discontinues remotely, the Account Management Delegation screen displays most of the information shown in the "delegated" version of the screen (*figure 5-20*) as well as the reason for discontinuing the delegation, as shown in *figure 5-21* below.

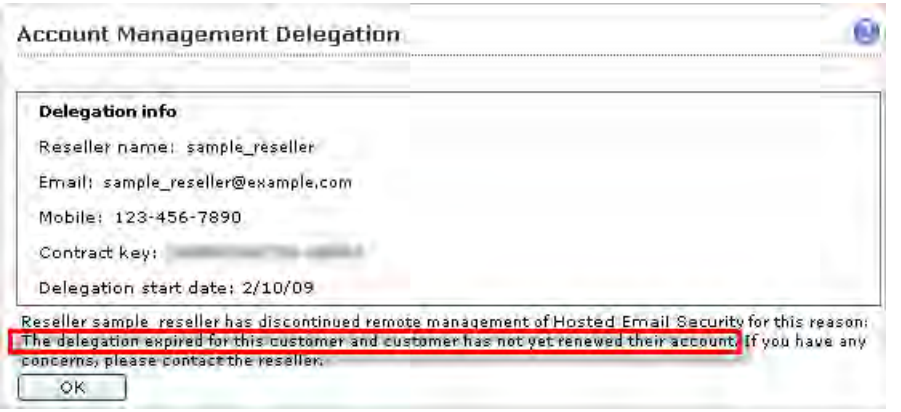


FIGURE 5-21. Account Management Delegation screen when remote delegate has discontinued the delegation

Appendix A

Frequently Asked Questions

The following FAQs apply to the current version of Hosted Email Security.

Question 1: What is Trend Micro™ Hosted Email Security?
Answer: Trend Micro Hosted Email 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, Hosted Email Security can stop attacks before they get a chance to reach your network. In addition to stopping spam, viruses, worm, Trojans, and other malware, Hosted Email Security 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?
Answer: Hosted Email Security 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 Hosted Email 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?
(And 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 Trend Micro Hosted Email 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: Does Trend Micro store/archive email?

Answer: Hosted Email Security 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 21 days in the EMEA region and 15 days in all other regions.

Question 13: How do I reset or resend an end-user password for the Web EUQ? (One of my users lost or cannot remember their password.)

Answer: Click **Administration** > **End-user Password** and fill out the Change End-User Password form. The end user will receive an email with an activation URL and will need to click the activation URL and then enter the appropriate email address and a new password in the Hosted Email Security Web EUQ logon screen. For more information, see *Resetting an End-User Password for the Web EUQ* on page 5-12.

Question 14: What happens to my messages if my mail server is unavailable for a period of time? (And 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 15: 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 full level of service, you can choose to redirect your outbound email traffic through Hosted Email Security services.

If you have a Trend Micro Online Registration (OLR) account, enabling outbound filtering is very easy, as explained in *If You Have an Online Registration Account* on page 2-7.

If you do not have an OLR account yet, follow the instructions in *If You Do Not Have an Online Registration Account* on page 2-8.

Question 16: Can Resellers and End User Customers Still Log On Using Existing Credentials?

Answer: Yes. There is no change for xSP reseller and end customers. xSP resellers still can use the "on behalf of" role to manage their end customers. xSP resellers and end customers cannot use the Domain Management screen to manage their managed domains, but they can use the command line to do that as before.

Question 17: How Can I Change a Managed Domain Name?

Answer: From the Domain Management screen you can manually change any domain information except domain name. To change a domain name, you must de-activate the existing domain and then add the new domain name.

Question 18: How Do I Use the "Test Email" Feature?

Answer: The purpose of the "test email" feature is to check whether the Hosted Email Security system is functioning properly. If you have not received any email for a period of time, you can verify that Hosted Email Security is working by sending a test email message. If the test message reaches you, then Hosted Email Security is working properly. If you cannot receive the message, contact your support provider.

Question 19: Why Is the Domain Management Screen Disabled?

Answer: This problem can occur if you log on using a local account. After you have created a Trend Micro Online Registration (OLR) account, you can still log on Hosted Email Security using your old logon credentials for a period of time. However, when logged on using your old account, you cannot make any changes on the Domain Management screen.

To add a new domain or manage an existing managed domain:

1. Access the Trend Micro Hosted Email Security logon screen.
2. Select **Log on with Trend Micro Online Registration user name and password.**
3. Type your OLR account user name and password.
4. Click **Log On.** The Reports screen appears.
5. Add or manage the domain as explained in *Managing Domains* on page 5-16.

Appendix B

Contact Information and Web-Based Resources

This appendix provides information on getting further assistance with any technical support questions that you may have.

Topics in this appendix include:

Contacting Technical Support

In addition to the Hosted Email Security online help through the administrative console, Trend Micro offers technical support through the Trend Micro Web site.

Trend Micro no longer offers support by email but instead offers support by means of an online submission system available at:

http://us.trendmicro.com/us/products/enterprise/hosted-email-security/index.html

At the site mentioned above, you can find the most current Support contact information as well as a link to the Trend Micro Knowledge Base.

Customers who have Hosted Email Security accounts through Worry Free Business Security with Hosted Email Security can also find contact information for that product at the above site.

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 Hosted Email Security:

- Hosted Email Security (full version)
- Hosted Email Security—Inbound Filtering

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 and services. 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 service 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.

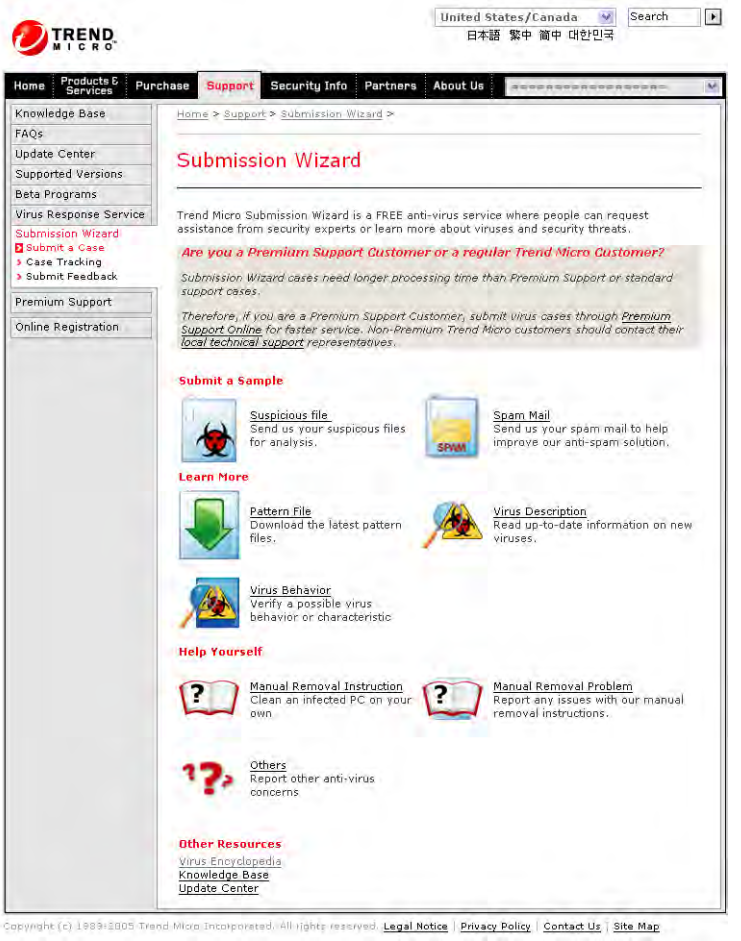


FIGURE B-22. Submission Wizard screen

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 or service that you are currently using. If you are using multiple Trend Micro products or services, select the one that has the most effect on the problem submitted, or the one 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) TRENDAV, or 877-873-6328

TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and technical 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 and services remain secure against emerging risks. The daily culmination of these efforts is 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 who provide technical support for a wide range of products and 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 or service 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.

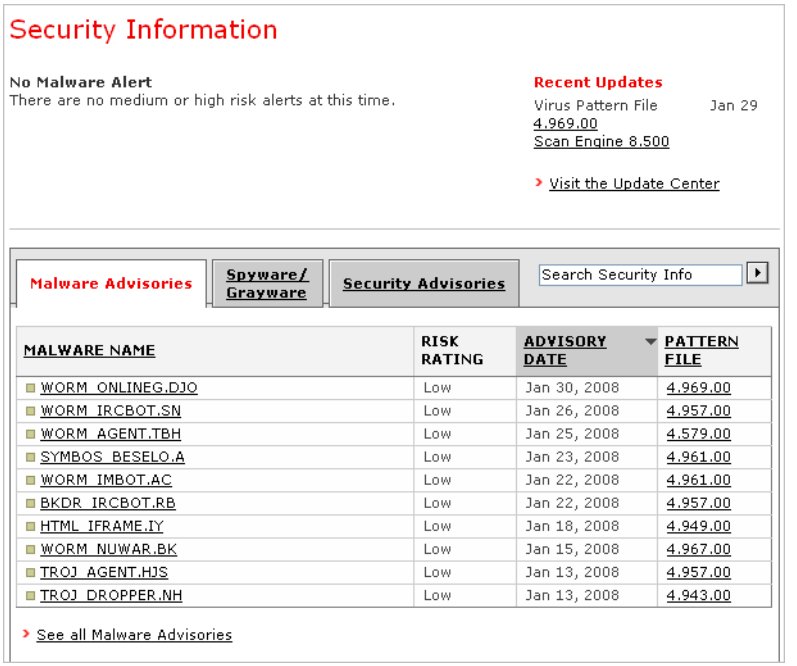


FIGURE B-23. Trend Micro Security Information screen

- 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

This appendix provides guidance on understanding and using the Hosted Email Security Web End-User Quarantine. It contains all of the content of the *Trend Micro Web End User Quarantine User Guide*, available for download as a separate PDF manual.

The Hosted Email Security Web End User Quarantine (EUQ) is a user interface that helps end users to 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*.

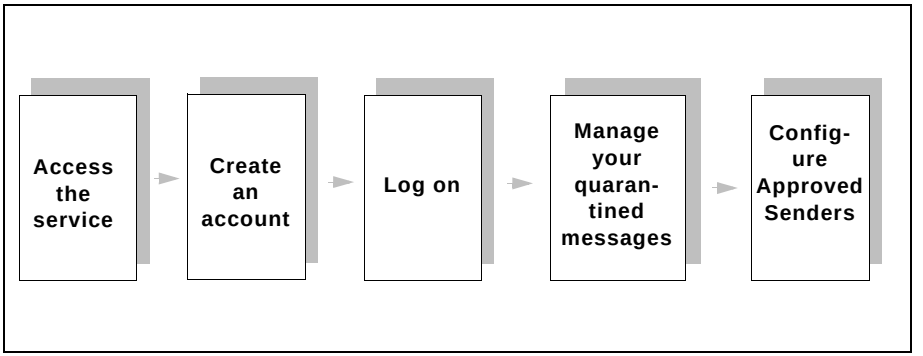


FIGURE C-1. Getting Started with Hosted Email Security Web EUQ

Accessing the Web End User Quarantine

To access the Web End User Quarantine, you need 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 logon page shown in *figure C-2*.

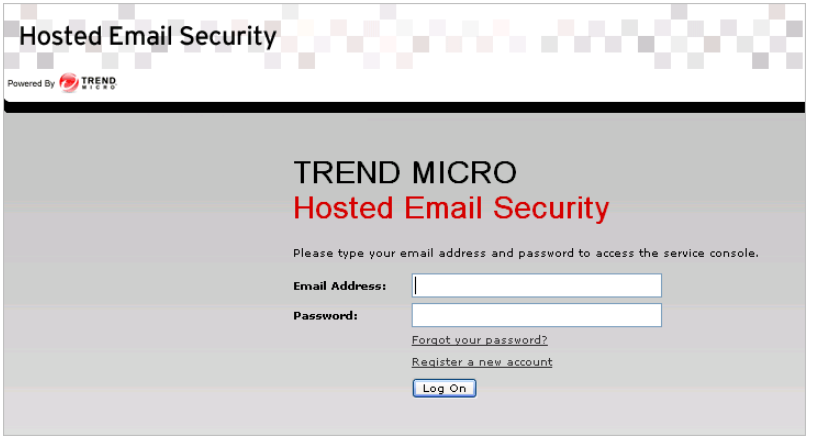


FIGURE C-2. Hosted Email Security Web EUQ logon screen

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

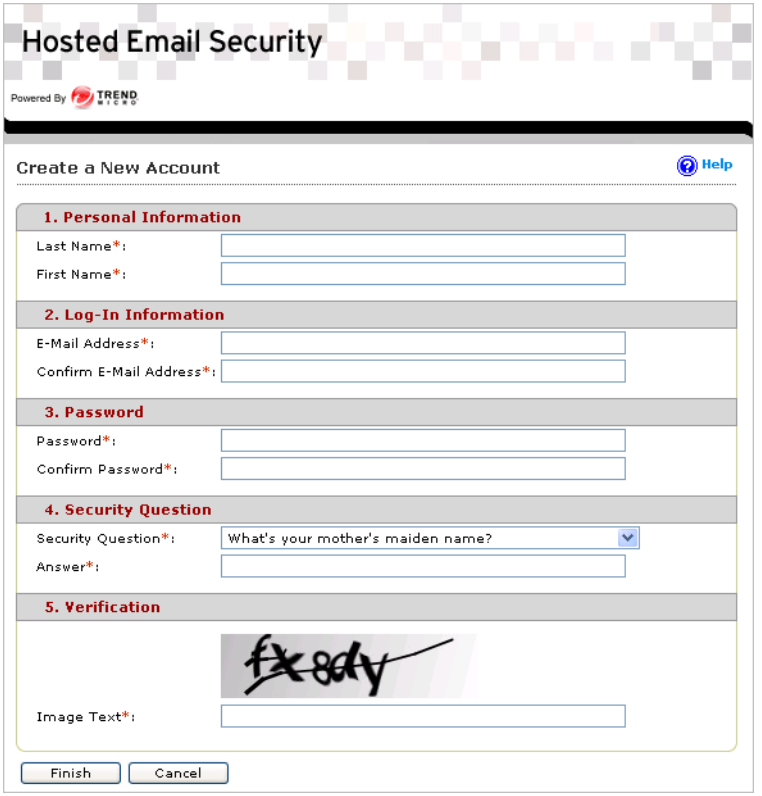


FIGURE C-3. Create a New Account screen

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 on to Hosted Email Security Web End User Quarantine

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 End User Quarantine 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 logon 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 Hosted Email Security Web EUQ. On this screen you can:

- View and sort a list of quarantined messages that were prevented from reaching your email inbox
- 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.

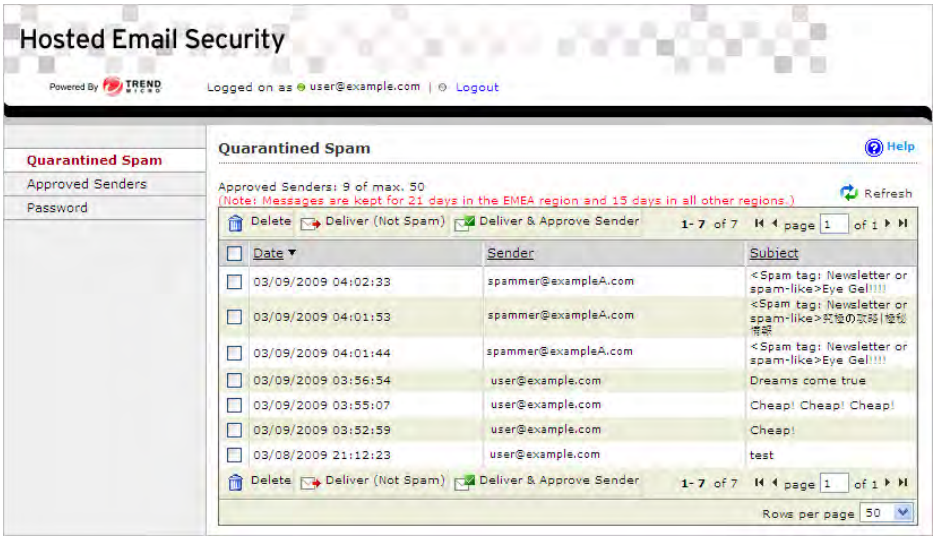


FIGURE C-4. Quarantined Spam screen

To view and sort quarantined items in the table:

1. 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.
2. 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
3. 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 ():** Selected message(s) are deleted.
   - **Deliver (Not Spam) ():** Selected message(s) are sent to your email account.
   - **Deliver and Approve Sender ():** Selected message(s) are sent to your email account and the sender's address will be added to your Approved Senders list.

Note: Trend Micro Hosted Email Security maintains up to 21 days of quarantined messages in the EMEA region and 15 days in all other regions. These messages 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:

- Hosted Email Security 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.

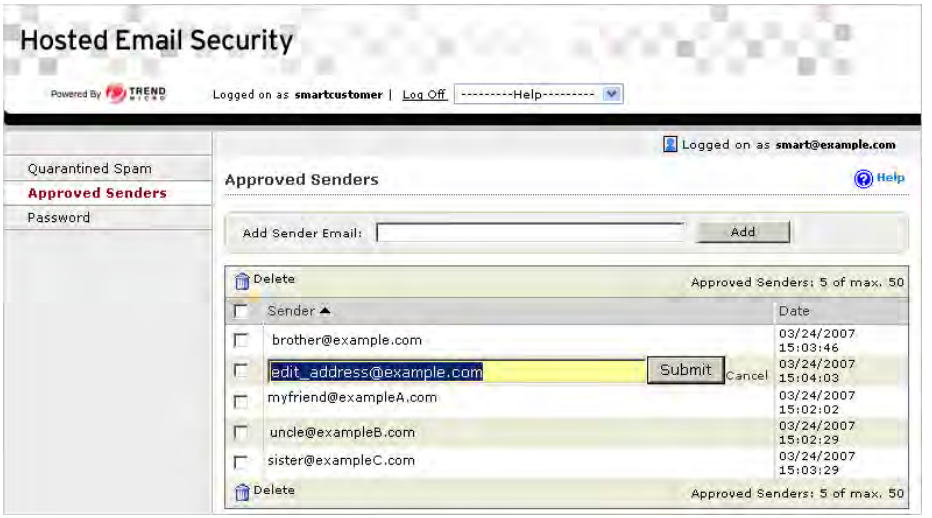


FIGURE C-5. Editing an address in the Approved Senders screen

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, Hosted Email Security Web End User Quarantine (EUQ) requires a password between 8 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 **Logon screen** and click the **Forgot your password?** link.

   The screen shown in *figure C-6* appears.

FIGURE C-6. Forgot Password dialog box

2. If you have a Trend Micro Online Registration (OLR) account, click **Yes**, and Web EUQ redirects you to the "Forgot Password" page on the OLR site.
3. If you do not have an OLR account, click **No**. The screen shown in figure C-7 on page C9 appears.

FIGURE C-7. Reset Password screen for users who do not have an OLR account

4. Type your Hosted Email Security user name and email address.

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

5. Type the text shown in the CAPTCHA verification image.
6. Click **Save**. When your information is successfully authenticated, you will receive an email message containing an activation URL.
7. Click on the activation URL in the email message. Hosted Email Security Web EUQ activates your new password and displays a confirmation page.
8. Click **Continue** in the confirmation page and log on to the Web EUQ console using the password that you chose in *Step 5*.

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.

Glossary

This glossary describes special terms used in this document or the online help.

TERM	EXPLANATION
action (*Also see* notification)	The operation to be performed when: • a virus has been detected • spam has been detected • a content violation has occurred • an attempt was made to access a blocked URL, or • file blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your software after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.
administrator	Refers to “system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.

TERM	EXPLANATION
administrator email address	The address used by the administrator of your Trend Micro product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a "backdoor"; tracking mechanism on the user's computer without the user's knowledge is called "spyware."
antivirus	Computer programs designed to detect and clean computer viruses.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from). The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
block	To prevent entry into your network.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.

TERM	EXPLANATION
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
damage routine	The destructive portion of virus code, also called the payload.
digital signature	Extra data that is appended to a message and that identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
(administrative) domain	A group of computers sharing a common database and security policy.

TERM	EXPLANATION
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
DUL (Dynamic User List)	Associated with Trend Micro Email Reputation Services, this list contains dynamically assigned IP addresses, or those with an acceptable use policy that prohibits public mail servers.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

TERM	EXPLANATION
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
End User Quarantine (EUQ, Web EUQ)	Also referred to as Web EUQ, a Web-based user interface that helps end users to manage spam email messages held in quarantine.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.
EUQ	See *End User Quarantine.*
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.

TERM	EXPLANATION
gateway	An interface between an information source and a Web server.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
heuristic rule-based scanning	Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.
incoming	Email messages or other data routed *into* your network.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.
KB	Kilobyte—1024 bytes of memory.
LDAP (Lightweight Directory Access Protocol)	An internet protocol that email programs use to locate contact information from a server. For example, suppose you want to locate all persons in Boston who have an email address containing the name "Bob." An LDAP search would enable you to view the email addresses that meet this criteria.
license	Authorization by law to use a Trend Micro product or service.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.

TERM	EXPLANATION
management console	The user interface for your Trend Micro product or service.
MB	Megabyte—1024 kilobytes of data.
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: • system administrator • sender of a message • recipient of a message, file download, or file transfer
online help	Documentation that is bundled with the graphical user interface.
Open Proxy Stopper (OPS)	Associated with Trend Micro Email Reputation Services, this list contains IP addresses of servers that are open proxy servers and are known to have sent spam.
outbound, outgoing	Email messages or other data *leaving* your network, routed out to the Internet.
outbound filtering	An optional feature of Hosted Email Security that filters outbound email messages for spam. This feature must be enabled before you can enable email encryption.
pattern file (also known as Official Pattern Release)	The pattern file, also referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified threats. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest threats. This pattern file is most effective when used with the latest scan engine.

TERM	EXPLANATION
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
policies	Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall.
proxy	A process providing a cache of items available on other servers that are presumably slower or more expensive to access.
proxy server	A World Wide Web server that accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
public-key encryption	An encryption scheme where each person gets a pair of "keys," called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
QIL (Quick IP List)	An early name for the Dynamic Reputation Database of Trend Micro Email Reputation Services.
Real-time Blackhole List (RBL)	A list of IP addresses of mail servers that are known to be sources of spam.
registration	The process of identifying yourself as a Trend Micro customer, in some regions using a product Registration Key, on the Trend Micro Online Registration screen. https://olr.trendmicro.com/registration

TERM	EXPLANATION
Registration Key	A 22-character code, including hyphens, that in some regions is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8. *Also see* Activation Code.
Relay Spam Stopper (RSS)	Associated with Trend Micro Email Reputation Services, this list contains IP addresses of mail servers that are open mail relays and are known to have sent spam.
RSS	See *Relay Spam Stopper.*
scan engine	The module that performs threat scanning and detection in the host product to which it is integrated.
seat	A license for one person to use a Trend Micro product.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.

TERM	EXPLANATION
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This detection may *trigger* the product or service to place the message in quarantine and to send a notification to the system administrator, message sender, and message recipient.
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
Web EUQ	See *End User Quarantine.*
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z