



# Secure Messaging Service

Powered by Trend Micro Email Security Platform for Service Providers



## Service Provider's Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products or services described herein without notice. Before using these products or services, review the latest version of the applicable user documentation, which are available from the service console or your service provider.

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

Copyright© 2010. Trend Micro Incorporated. All rights reserved.

Document Part No. ESEM14540/100723

Release Date: July 30, 2010

Service Name and Version: Trend Micro™ Secure Messaging Service 1.0

The user documentation for Trend Micro™ Secure Messaging Service 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 Knowledge Base at Trend Micro Web site.

Trend Micro is always seeking to improve its documentation and welcomes your feedback. Please evaluate this documentation on the following site:

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

# Contents

## Preface

Content Summary .....	viii
Audience .....	ix
Required Knowledge .....	ix
Additional Useful Knowledge .....	ix
Document Conventions .....	ix
Where to Look for More Information .....	x

## Chapter 1: Introducing Secure Messaging Service

Service Overview .....	1-2
Features and Benefits .....	1-3
Recipient and Sender Filtering .....	1-3
Reputation-Based Source Filtering .....	1-3
Malware Protection .....	1-4
Spam and Phishing Filtering .....	1-4
Attachment Control .....	1-4
Content Filtering .....	1-4
Tracking and Reporting .....	1-5
What's New .....	1-5
Glossary .....	1-6

## Chapter 2: Getting Started

Preparing Required Information .....	2-2
MTA Information .....	2-3
Logging On to the Console .....	2-5

Browser Requirements .....	2-5
Display Issues on Internet Explorer .....	2-5
Resetting Forgotten Passwords .....	2-6
Setting Up Email Security .....	2-7
Setting Up Inbound Filtering .....	2-7
Setting Up Outbound Filtering .....	2-7
Specifying Outbound Servers .....	2-8
General Console Tasks .....	2-9
Switching Accounts .....	2-9
Using the Search Function .....	2-10

### **Chapter 3: Managing Accounts**

Modifying Your Account Profile .....	3-2
Changing Your Email Address .....	3-3
Configuring Console Rebranding .....	3-3
Changing Your Password .....	3-5
Accounts Overview .....	3-5
Account Types .....	3-9
Creating or Modifying Accounts .....	3-10
Exporting the Account List .....	3-11

### **Chapter 4: Understanding Mail Filters**

System Limits .....	4-2
Types of Configurable Filters .....	4-3
Filter Criteria .....	4-4
Understanding Email Reputation Service .....	4-6
Email Reputation Service Standard .....	4-7
Email Reputation Service Advanced .....	4-7
Understanding Malware, Spam, and Phishing .....	4-7
Malware .....	4-7
Spam .....	4-8
Phishing .....	4-8
Understanding Rules .....	4-9

Filter Actions .....	4-9
Filtering Flow .....	4-11
Inbound Messages .....	4-12
Multiple Criteria and Filter Actions .....	4-13
Outbound Messages .....	4-14

## Chapter 5: Filtering Mail

Policies Overview .....	5-2
Searching for and Modifying Existing Policies .....	5-3
Creating Policies .....	5-4
Specifying Destination Servers .....	5-5
Destination Server Options .....	5-6
Specifying Valid Recipients .....	5-8
Specifying Approved and Blocked Senders .....	5-10
Enabling Email Reputation Service .....	5-12
Configuring the Antivirus Filter .....	5-13
Sending Antivirus Notifications .....	5-14
Configuring the Anti-spam Filter .....	5-15
Creating an Anti-spam Rule .....	5-16
Spam and Phishing Catch Rates .....	5-18
Configuring the Content Filter .....	5-20
Creating a Content Filter Rule .....	5-21
Regular Expressions .....	5-24
Configuring the Attachment Filter .....	5-27
Creating an Attachment Filter Rule .....	5-28
Attachment Extension Names .....	5-31

## Chapter 6: Monitoring and Tracking

Viewing Summary Information .....	6-2
Dashboard Data Explained .....	6-2
Using the Dashboard .....	6-3
Tracking Messages .....	6-4
Viewing Quarantined Messages .....	6-5

Using Reports .....	6-7
Report Types .....	6-7
Threat Summary .....	6-8
IP Blocking .....	6-9
Quarantine .....	6-10
Inbound Traffic .....	6-11
Viewing Reports .....	6-12

## **Chapter 7: End-User Quarantine**

Giving Users Access to Their Quarantined Messages .....	7-2
Using the End-User Quarantine .....	7-3
Browser Requirements .....	7-3
Handling Messages in the End-User Quarantine .....	7-3
Approving Senders in the End-User Quarantine .....	7-5
Modifying Your End-User Quarantine Password .....	7-6

## **Chapter 8: Troubleshooting and FAQs**

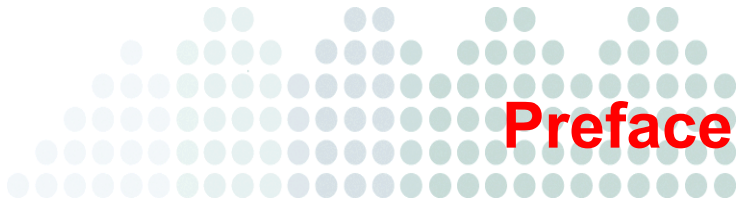
Troubleshooting .....	8-2
Frequently Asked Questions .....	8-3

## **Chapter 9: Technical Support**

Contacting Technical Support .....	9-2
Knowledge Base .....	9-2
TrendWatch .....	9-3
Submission Wizard .....	9-3
Free Scans with HouseCall .....	9-3

## **Index**





# Preface

Welcome to the *Trend Micro™ Secure Messaging Service Service Provider's Guide*. This section describes this document and other service documentation. It covers the following topics:

- *Content Summary* on page viii
- *Audience* on page ix
- *Document Conventions* on page ix
- *Where to Look for More Information* on page x

## Content Summary

The *Service Provider's Guide* serves as a comprehensive printable reference about Secure Messaging Service. To further understand how to use this document and where to find information, refer to the following table.

**TABLE P-1. Document Chapters**

GOAL	CHAPTER
Understanding the service and its features, as well as relevant concepts	<a href="#">Introducing Secure Messaging Service</a> starting on page 1-1
Getting started, including accessing the console and general setup instructions	<a href="#">Getting Started</a> starting on page 2-1
Managing your user profile and other accounts	<a href="#">Managing Accounts</a> starting on page 3-1
Understanding supported inbound and outbound filters	<a href="#">Understanding Mail Filters</a> starting on page 4-1
Managing filtering policies	<a href="#">Filtering Mail</a> starting on page 5-1
Tracking messages, viewing quarantined messages, and generating reports	<a href="#">Monitoring and Tracking</a> starting on page 6-1
Using the quarantine and the approved sender list for end users	<a href="#">End-User Quarantine</a> starting on page 7-1
Troubleshooting issues and getting answers to frequently asked questions	<a href="#">Troubleshooting and FAQs</a> starting on page 8-1
Contacting technical support	<a href="#">Technical Support</a> starting on page 9-1

## Audience

The *Service Provider's Guide* is designed for administrators who are responsible for connecting a subscriber mail system to Secure Messaging Service and ensuring that the subscriber fully benefits from the service.

## Required Knowledge

To effectively leverage the contents of this document and the service itself, readers are expected to have functional knowledge of the following:

- Mail routing concepts
- Subscriber mail infrastructure

## Additional Useful Knowledge

A good understanding of spam, phishing, malware, and other email security concepts may help you effectively perform tasks described in this document. Knowledge of Perl Compatible Regular Expressions (PCRE) will allow you to create advanced content filtering patterns.

## Document Conventions

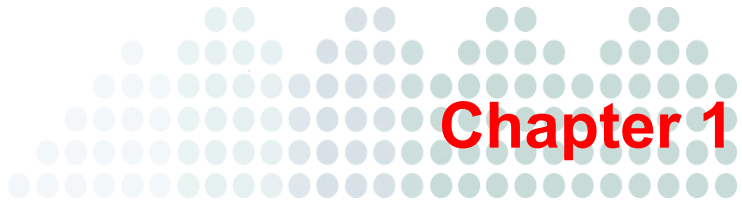
For the style conventions used in this document, refer to the following table.

**TABLE P-2. Document Conventions**

INFORMATION	CONVENTION
User interface items	<b>Bold</b>
Document and resource names; new, uncommon, and lengthy terms	<i>Italics</i>
URLs; strings to be typed as-is	Monospace

## Where to Look for More Information

Online Help pages are available on the Secure Messaging Service consoles for both administrators and end users. These pages provide information on console screens as well as related concepts and tasks. To open the Online Help, click **Help** or the contextual help icons from any screen on the consoles.



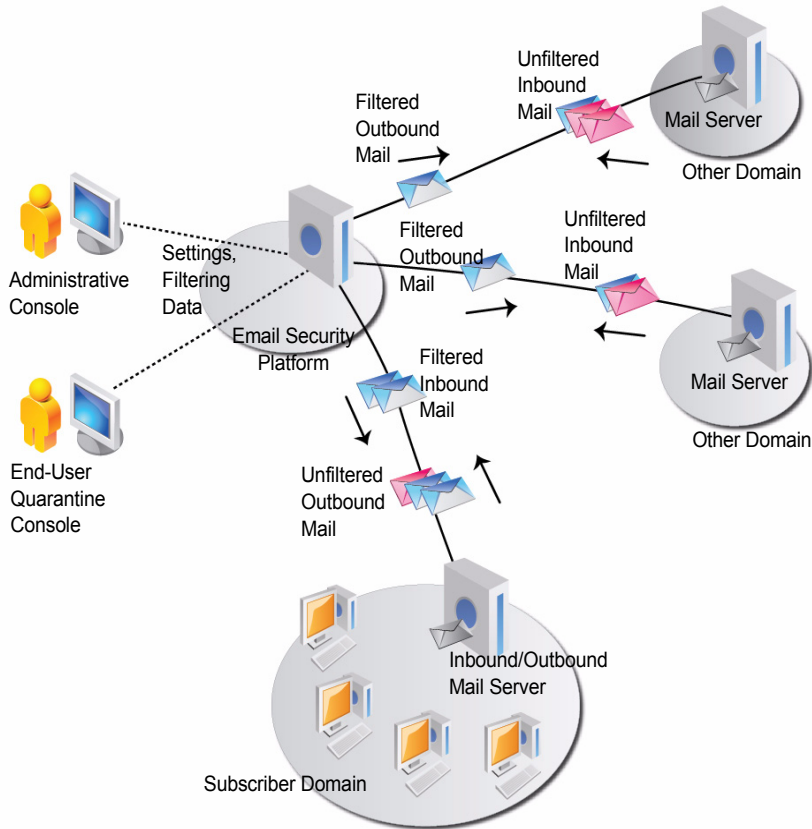
# Introducing Secure Messaging Service

This chapter introduces the service and concepts associated with the service. It covers the following topics:

- *Service Overview* on page 1-2
- *Features and Benefits* on page 1-3
- *What's New* on page 1-5
- *Glossary* on page 1-6

## Service Overview

Trend Micro™ Secure Messaging Service is a managed email security service powered by Trend Micro Email Security Platform for Service Providers. By routing inbound and outbound messages through the service, you can protect domains against spam, phishing, malware, and other messaging threats.



**FIGURE 1-1. Secure Messaging Service overview**

A Web-based administrative console allows administrators to configure and manage the service. Likewise, end users can access quarantined messages and configure individual lists of approved senders through the End-User Quarantine console.

## Features and Benefits

Secure Messaging Service offers multiple benefits.

### Recipient and Sender Filtering

When enabled, the *valid recipients* filter allows only messages sent to specified recipients. With this filter, Secure Messaging Service can prevent directory harvest attacks (DHAs) and other forms of spam that use randomly generated recipient addresses.

By approving senders, Secure Messaging Service subscribers automatically allow messages from trusted mail servers, domains, or email addresses. Messages from approved senders are *not* checked for spam or source reputation.

By blocking senders, subscribers automatically block messages from untrusted sources.

For more information, see:

- [Types of Configurable Filters](#) on page 4-3
- [Specifying Valid Recipients](#) on page 5-8
- [Specifying Approved and Blocked Senders](#) on page 5-10

### Reputation-Based Source Filtering

With Trend Micro Email Reputation Service, Secure Messaging Service verifies email sources against dynamic and self-updating reputation databases to block messages from the latest botnets and other IP addresses controlled by spammers, phishers, and malware distributors.

For more information, see:

- [Types of Configurable Filters](#) on page 4-3
- [Understanding Email Reputation Service](#) on page 4-6
- [Enabling Email Reputation Service](#) on page 5-12

## Malware Protection

With Trend Micro antivirus technology, Secure Messaging Service protects against infectious messages from mass-mailing worms or manually crafted messages that contain Trojans, spyware, or other malicious code.

For more information, see:

- [Types of Configurable Filters](#) on page 4-3
- [Understanding Malware, Spam, and Phishing](#) on page 4-7
- [Configuring the Antivirus Filter](#) on page 5-13

## Spam and Phishing Filtering

Secure Messaging Service checks messages for spam and phishing characteristics to effectively reduce the volume of unsolicited messages and prevent fraud.

For more information, see:

- [Types of Configurable Filters](#) on page 4-3
- [Understanding Malware, Spam, and Phishing](#) on page 4-7
- [Configuring the Anti-spam Filter](#) on page 5-15

## Attachment Control

With the attachment filter, Secure Messaging Service regulates the type, size, and number of attachments that messages can contain.

For more information, see:

- [Types of Configurable Filters](#) on page 4-3
- [Configuring the Attachment Filter](#) on page 5-27

## Content Filtering

Secure Messaging Service can filter email messages with unwanted text in their subjects and message bodies. With Perl Compatible Regular Expressions (PCRE), you can filter for specific text and text patterns.



For more information, see:

- [Types of Configurable Filters](#) on page 4-3
- [Configuring the Content Filter](#) on page 5-20
- [Regular Expressions](#) on page 5-24

## Tracking and Reporting

Secure Messaging Service allows administrators to track messages sent to specific recipients and review quarantined messages. It provides multiple report types that cover message processing volume and filtering efficiency.

For more information, see:

- [Viewing Summary Information](#) on page 6-2
- [Tracking Messages](#) on page 6-4
- [Viewing Quarantined Messages](#) on page 6-5
- [Using Reports](#) on page 6-7
- [Giving Users Access to Their Quarantined Messages](#) on page 7-2

## What's New

The following table list the most recent features added to Secure Messaging Service.

**TABLE 1-1. New Features**

FEATURE	ADDED	DESCRIPTION	ADDITIONAL INFORMATION
Content filtering	July 2010	Filtering of messages with unwanted text in their subject or message body	<ul style="list-style-type: none"> <li>• <a href="#">Content Filtering</a> on page 1-4</li> <li>• <a href="#">Configuring the Content Filter</a> on page 5-20</li> </ul>
Antivirus notifications	August 2010	Sending of notifications whenever an infected message is detected and deleted	<ul style="list-style-type: none"> <li>• <a href="#">Sending Antivirus Notifications</a> on page 5-14</li> </ul>

## Glossary

The following table lists the concepts discussed in this document and other Secure Messaging Service documents.

**TABLE 1-2. Glossary**

<b>CONCEPT</b>	<b>DEFINITION</b>
Account type	Secure Messaging Service regulates access to all tasks in the administrative console, such as policy creation or filter configuration, using account types. Each account has a specified type that determines whether the account user can perform certain tasks.
Administrative console	The Web-based management console used by administrators of all levels to configure and manage the service. The administrative console also provides access to logs, quarantined messages, and reports.
Approved sender	The address of a sender whose messages are not checked by the anti-spam or the Email Reputation Service filters.
Blocked sender	The address of a sender address whose messages are automatically blocked.
Catch rate	A "catch rate" refers to the degree of sensitivity by which messages are detected as spam or phishing. The most aggressive catch rate has the highest chance of catching all spam or phishing messages, but also has the highest chance of falsely detecting normal messages. The most conservative settings yield the least number of detections but have very few false detections.
Content filtering	Content filtering involves checking mail for unwanted text strings. Secure Messaging Service supports content filtering with regular expression patterns.

**TABLE 1-2. Glossary (Continued)**

<b>CONCEPT</b>	<b>DEFINITION</b>
Destination servers	"Destination servers" refer to the set of mail servers that are used by a domain to receive inbound mail. Secure Messaging Service relays processed mail to these servers.
Domain	A subscriber network or, more specifically, a set of email addresses with the same domain name. A Secure Messaging Service policy applies to a single domain. For clarity, a domain may be referred to as a "subscriber domain" or a "policy domain".
Email Reputation Service	A cloud-based Trend Micro reputation service that checks the IP addresses of mail servers to block email messages from untrustworthy sources.
End user	Distinguished from administrators and other users of the Secure Messaging Service, end users are the owners of individual mailboxes in subscriber domains.
End-User Quarantine console	Also called "EUQ", the End-User Quarantine console is a Web-based console that allows end users to review quarantined messages and specify their own list of approved senders.
Filter	Each Secure Messaging Service filter corresponds to a specific method or capability to prevent unwanted email messages from reaching subscriber domains. Each filter, designed to be configured individually, addresses a particular threat domain.
Filter action	A filter action is the action performed on a message as soon as it is caught by a filter. Some filters support multiple, configurable filter actions, such as <i>delete</i> , <i>quarantine</i> , <i>change recipient</i> , or <i>insert text</i> .

**TABLE 1-2. Glossary (Continued)**

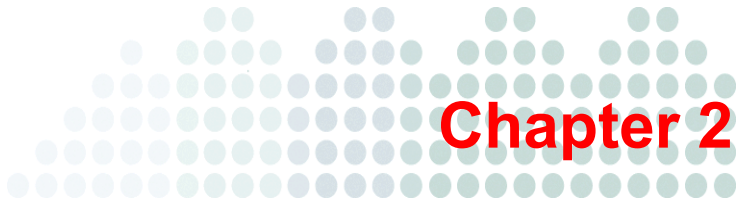
<b>CONCEPT</b>	<b>DEFINITION</b>
Filter criteria	Filter criteria are the bases by which messages are caught by the individual filters. When a message matches a criterion, Secure Messaging Service performs a corresponding filter action on the message.
Inbound	In Secure Messaging Service, "inbound messages" are messages sent from other domains to the subscriber domain. "Inbound" refers to the direction of traffic to the subscriber domain.
Local-part	The part of the email address that uniquely identifies a mailbox in a domain. In the email address <code>name@example.com</code> , the local-part is "name". When specifying email addresses from a known domain, Secure Messaging Service typically requires you to specify only the local-part.
Mail filtering	"Mail filtering" refers to the process of checking email messages for malware, spam, and other unwanted characteristics and then performing a corresponding action to protect or warn recipients of the unwanted content. This process is performed by multiple components—or filters—in Secure Messaging Service.
Malware	Malware programs are typically file-based threats, with some of the more common types being referred to as Trojans, viruses, and worms. Email users typically receive worms embedded as scripts in HTML email or as executable attachments.
Outbound	In Secure Messaging Service, "outbound messages" are messages sent from the subscriber domain to other domains. "Outbound" refers to the direction of traffic leaving the subscriber domain.

**TABLE 1-2. Glossary (Continued)**

<b>CONCEPT</b>	<b>DEFINITION</b>
Parent and child account	"Parent" and "child" are used to describe "creator-created" relationships between accounts. The parent account is the creator of the child account and can manage the child account.
Phishing	"Phishing" refers to the method of tricking users into submitting user names, passwords, credit card numbers, and other critical information to copycats that mimic trustworthy entities. Users are typically lured into phishing sites by fake email and instant messages.
Quarantine	"Quarantine" refers to a location where filtered messages are held. It can also refer to the act of moving messages to this location. Administrators and end users can review and choose to deliver quarantined messages.
Relay	"Relay" is used in Secure Messaging Service to refer to the process of sending messages from one MTA to another. For example, a subscriber's outbound messages are <i>relayed</i> to the service's outbound MTA for processing and eventual delivery.
Rule	In Secure Messaging Service, the anti-spam, attachment, and content filters support rules. Unlike other filters, which support only one combination of filter criteria and actions, rules allow these filters to support multiple combinations of filter criteria and actions.
Spam	"Spam" refers to unsolicited and unwanted electronic messages that are sent out indiscriminately and in bulk. The most widely recognized form of spam is email spam.
Sibling account	A "sibling" account is a Secure Messaging Service account with the same creator or parent. An account can be given privileges to manage sibling accounts.

**TABLE 1-2. Glossary (Continued)**

<b>CONCEPT</b>	<b>DEFINITION</b>
Subscriber	A customer of Secure Messaging Service; subscribers pay for the service and control the domains protected by the service.
Terminal action	A filter action is considered a "terminal action" if it causes Secure Messaging Service to stop processing a message. The <i>delete</i> , <i>quarantine</i> , and <i>change recipient</i> filter actions are considered terminal actions because no additional filtering can be performed on a message as soon as one of these actions is completed.
Valid recipient	With the <i>valid recipients</i> filter enabled, Secure Messaging Service blocks all messages sent to email addresses that are not in the <i>valid recipients</i> list. A "valid recipient" is considered a valid email address in the protected domain—an address that is allowed to receive messages from other domains.



## Getting Started

This chapter covers tasks that allow you to start leveraging the service and using the console. This chapter covers the following topics:

- *Preparing Required Information* on page 2-2
- *Logging On to the Console* on page 2-5
- *Setting Up Email Security* on page 2-7
- *General Console Tasks* on page 2-9

## Preparing Required Information

Before getting started with Secure Messaging Service, make sure you have the following general information about the service. You can obtain this information from your Trend Micro representative.

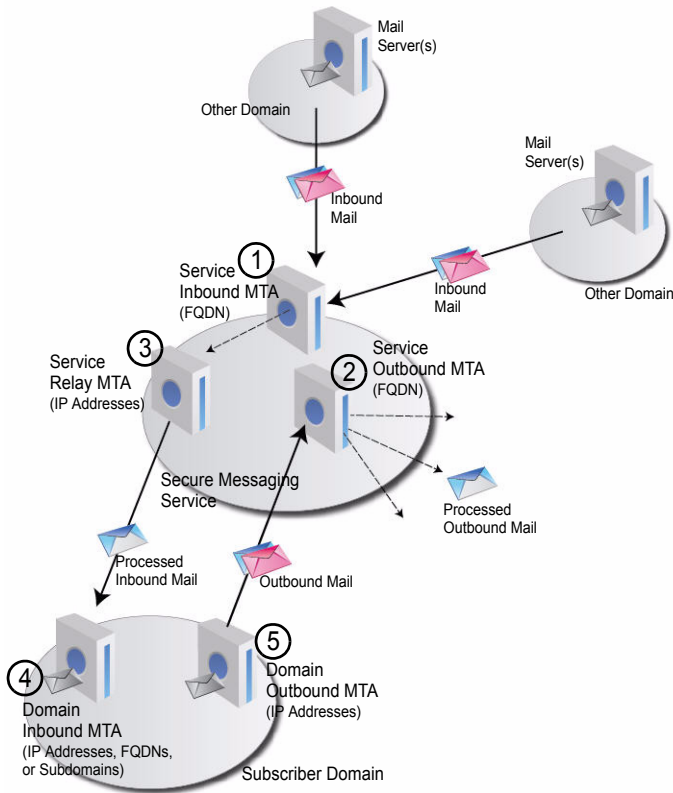
**TABLE 2-1. General Required Information**

<b>INFORMATION</b>	<b>DESCRIPTION</b>
Administrative console URL	URL of the logon page
End-User Quarantine console URL	URL of the console that email users need to access their quarantined messages
Account name	Name of the account you use to log on to the administrative console
Temporary password	Password that you use with the account name; change this password immediately after successfully logging on to the console
Domain name	Name of the domain that you plan to protect with Secure Messaging Service



## MTA Information

To get started with Secure Messaging Service, you need to properly configure routing between the domain's mail transfer agents (MTAs) and the MTAs used by the service. See the following diagram to understand how these MTAs interact.



**FIGURE 2-1. Domain and service MTAs**

You need to obtain the addresses used to identify these MTAs. These addresses can be IP addresses, FQDNs, or even subdomains, as described in the following table.

**TABLE 2-2. MTA Information**

#	MTA	SOURCE	ADDRESS TYPE	DESCRIPTION AND USAGE
1	Service inbound MTA	Trend Micro	FQDN	Identifies the service mail transfer agents (MTAs) that receive messages being sent to subscriber domains.  Point the domain's MX records to this FQDN.
2	Service outbound MTA	Trend Micro	FQDN	Identifies the MTAs that receive messages being sent from subscriber domains to other domains.  Configure the domain's outbound MTA to relay messages to this FQDN.
3	Service relay MTA	Trend Micro	IP addresses	Identifies the MTAs that relay processed messages to subscriber domains.  Configure the domain's firewall and inbound MTAs to allow transactions with these IP addresses.
4	Domain inbound MTA (destination servers)	Mail administrator	<ul style="list-style-type: none"> <li>• IP addresses</li> <li>• FQDNs</li> <li>• Subdomain name</li> </ul>	Also called <i>destination servers</i> , identifies the MTAs used by the subscriber domain to receive messages from other domains.  Configure Secure Messaging Service to relay processed messages to these addresses. See <a href="#">Specifying Destination Servers</a> on page 5-5.

**TABLE 2-2. MTA Information**

#	MTA	SOURCE	ADDRESS TYPE	DESCRIPTION AND USAGE
5	Domain outbound MTA	Mail administrator	IP addresses	Identifies MTAs used by the subscriber domain to send messages to other domains.  Configure Secure Messaging Service to accept outbound messages from these addresses. See <a href="#">Specifying Outbound Servers</a> on page 2-8.

## Logging On to the Console

The Secure Messaging Service administrative console is an easy-to-use Web-based interface for configuring email security settings for a domain. When logging on to the console, ensure that you have the correct console URL and use a supported Web browser.

## Browser Requirements

To properly display all the screens in the console, including the help pages, use one of the following Web browsers:

- Microsoft™ Internet Explorer™ 7 or 8
- Mozilla™ Firefox™ 3.0 or 3.5

## Display Issues on Internet Explorer

On certain Windows Server™ operating systems, including Windows Server 2003 and 2008, Internet Explorer Enhanced Security Configuration can prevent the console from displaying properly. To avoid display issues, try the following:

- Add the console domain to the Internet Explorer **Trusted sites** zone after enabling Enhanced Security Configuration.
- If adding the console domain does not correct display issues, disable Enhanced Security Configuration.

### **To disable Enhanced Security Configuration on Windows Server 2003:**

1. Open Windows Control Panel.
2. Open **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. Select **Internet Explorer Enhanced Security Configuration**, and then click **Details**.
5. Deselect the users or groups that you want to disable Enhanced Security Configuration for, and then click **OK**.
6. Click **Next**, and then click **Finish**.
7. Restart Internet Explorer to apply the changes.

---

**Note:** This procedure may vary on other Windows Server operating systems. Consult Windows Server help for more information. For more information on Enhanced Security Configuration, visit <http://support.microsoft.com/kb/815141>.

---

## **Resetting Forgotten Passwords**

If you have forgotten your password, you can reset it to access the console. This procedure applies to both the administrative console and the End-User Quarantine console.

### **Considerations:**

- You will need to activate your new password using the email address specified in your profile. If you have not specified an address or have given an invalid address, you will not be able to reset your password.
- The activation link for a new password expires after 48 hours. The original password remains in effect if you do not confirm the password change.

### **To reset your password:**

1. Click **Forgot your password?** on the logon page.
2. In the popup, supply your user name and your new password.
3. Click **Reset Password**. An activation link will be sent to your email address.
4. To log on the console using the new password, access your email account and click the activation link.

---

## Setting Up Email Security

Before a domain can start benefitting from the email filtering service, you need to ensure that the domain's inbound and outbound messages are properly routed through Secure Messaging Service servers and you have configured the service properly.

---

**Note:** For necessary information, such as service FQDNs and relay IP addresses, please contact your service provider. For more information, see [MTA Information](#) on page 2-3.

---

## Setting Up Inbound Filtering

**To begin protecting a domain from spam and other messaging threats:**

1. Create the policy for the domain. See [Creating Policies](#) on page 5-4.
2. During policy creation, specify the destination servers to ensure that Secure Messaging Service delivers messages bound for the domain after processing. See [Specifying Destination Servers](#) on page 5-5.
3. To ensure that Secure Messaging Service can relay processed messages to the domain, configure the domain's inbound mail servers to accept connections from the IP address range used by the service relay MTA.
4. Point the domain's MX records to the correct service *inbound* MTA FQDN.

---

**Note:** To help minimize having outdated DNS resolver cache entries that still point to the domain's MTA, temporarily lower the time-to-live (TTL) values for the resource records before pointing them to Secure Messaging Service servers.

---

## Setting Up Outbound Filtering

Secure Messaging Service accepts and processes outbound messages only if they are from the IP addresses you specified as outbound servers. The service permanently rejects (by returning error code 550) and prevents all other outbound messages from reaching their recipients.

**To help ensure that messages from a domain are free from spam and other messaging threats:**

1. Specify the IP addresses of the domain's outbound servers to ensure that Secure Messaging Service processes messages from these mail servers on their way to other domains. See *Specifying Outbound Servers* on page 2-8.
2. Configure the domain's mail servers to relay outgoing messages to the correct service *outbound* MTA FQDN.

## Specifying Outbound Servers

Secure Messaging Service processes and delivers outbound messages from specified outbound servers only. Specify the IP addresses of all the outbound servers of your domains to allow the service to process and deliver messages from these servers.

**Click path:** ... > **Outbound Servers**



**FIGURE 2-2.** Outbound Servers tab

---

**WARNING!** Ensure that your outbound server IP address list is complete before pointing traffic from the actual outbound servers to Secure Messaging Service.

---

**To add an outbound server:**

1. Click the **Outbound Servers** tab.
2. Type an IP address and click **Add**.

**To delete an outbound server:**

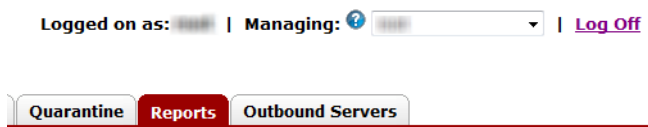
1. Click the **Outbound Servers** tab.
2. Select the IP address using the check box and click **Delete**.

## General Console Tasks

The following procedures describe how to perform tasks that can help you maximize efficiency while using the administrative console.

## Switching Accounts

Switching accounts lets you directly manage policies, accounts, and other resources that are managed by other accounts. By switching to an account, you choose to display only resources associated with that account. Switching accounts changes the policies, accounts, mail tracking entries, quarantine entries, dashboard statistics, and reports that are visible.



**FIGURE 2-3.** Managing drop-down list

**Considerations:**

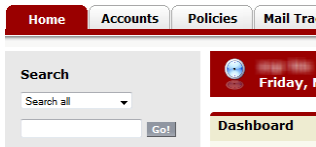
- You can switch only to an account that you manage.
- Switching to an account only changes the resources that are visible. Your permissions, including your ability to perform certain tasks, are retained.

**To switch accounts:**

Select the account from the **Managing** drop-down list.

## Using the Search Function

The search function lets you quickly locate information associated with certain accounts, policies, approved and blocked senders, and valid recipients.



**FIGURE 2-4. Search function**

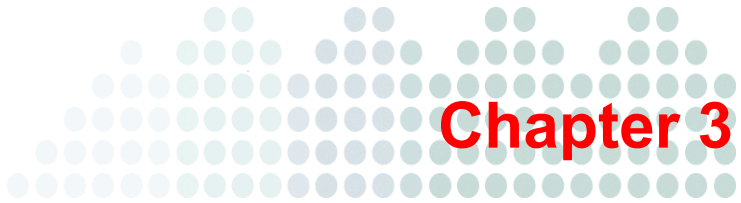
### **Considerations:**

- To return only exact matches, enclose your search string in double quotes ("").
- Narrow down your search terms to get results faster. The console may time out while retrieving the results of a very broad search.
- Performing other tasks, such as adding an account, while a search is running can result in errors.

### **To use the search function:**

1. In the left pane, select the type of information you want to locate and type your search term under **Search**.
2. Click **Go**.





## Managing Accounts

This chapter discusses tasks related to maintaining Trend Micro™ Secure Messaging Service accounts. It covers the following topics:

- *Modifying Your Account Profile* on page 3-2
- *Accounts Overview* on page 3-5
- *Creating or Modifying Accounts* on page 3-10

## Modifying Your Account Profile

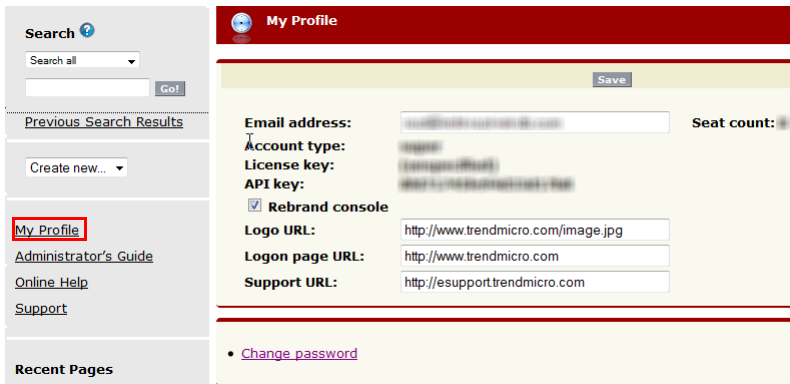
By modifying your account profile, you can change the following account settings:

- Email address
- Console rebranding settings
- Password

### Considerations:

- Contact your support provider to modify account settings that cannot be modified through your profile.
- The following information is also displayed when you view your profile:
  - **Account type**—determines the tasks that you are able to perform in Secure Messaging Service
  - **License key**—specified during account creation, the license key may be tied to your account through an external registration or licensing system
  - **API key**—used internally by the service infrastructure; you may need this key when contacting your support provider

**Click path:** ... > **My Profile**



**FIGURE 3-1.** My Profile link and page

## Changing Your Email Address

Specify the email address that Secure Messaging Service should use to contact you.

### **Considerations:**

Ensure that you provide the correct email address. When you attempt to reset a forgotten password, Secure Messaging Service sends an activation link to this address.

### **To change your email address:**

1. Click **My Profile** in the left pane.
2. Modify the email address and click **Save**.

## Configuring Console Rebranding

By default, console rebranding settings are inherited from the parent account. That is, if an account uses a rebranded console, any new account created by the account will use the same rebranded console. The child account, however, may be configured by the account creator or the account user to use different rebranding settings.

By rebranding the console, you can:

- Change the appearance of the console logo as shown below.



- You can also specify a Web page to replace the lower frame of the logon screen as shown below.



- You can specify the URL that opens when the **Support** link in the left pane of the console is clicked.

### Considerations:

- Logo file format and dimensions

You can use any image format that can be displayed by most browsers. Using an image that is close to the size of the default logo (120x54 pixels) can help prevent the console from displaying poorly.

- Accessing the rebranded logon page

To access the rebranded logon page, modify the default logon URL by inserting your account name at the beginning of the domain. For example, if your account name is "name", use the following URL to access the rebranded console:

`https://name.emailsecurity.trendmicro.com`

**To rebrand the console:**

1. Click **My Profile** in the left pane.
2. Specify the following:
  - **Logo URL**—the URL of the image file to use as the console logo
  - **Logon page URL**—the URL of the Web page to use in the service logon page
  - **Support URL**—the URL of the **Support** link in the left pane
3. Click **Save**.

## Changing Your Password

Change your password regularly to protect your account.

**Considerations:**

For strong passwords, use:

- More than eight characters
- Use both upper and lower case letters
- Numbers
- Non-alphanumeric characters

**To change your password:**

1. Click **My Profile** in the left pane.
2. Click **Change Password**.
3. Type your current and new passwords.
4. Click **Save**.

## Accounts Overview

Account users are typically able to manage only the domains and accounts that they create. However, you can also provide permissions so that they can manage sibling accounts and their domains.

---

**Note:** Account users can change their email address, console rebranding settings, and their password. For more information, see [Modifying Your Account Profile](#) on page 3-2.

---

The following options are available when you create or view an account.

**TABLE 3-1. Account Details**

SECTION	FIELD	DESCRIPTION
General	Enable account	Determines whether the account can be used to log on to the console.
	Account name	Logon name for accessing the console.
	Email address	Address to be used for service-related communication, including when resetting forgotten passwords; account users can modify their email addresses.  <b>Note:</b> Ensure that you provide the correct email address. When the account user attempts to reset his or her forgotten password, Secure Messaging Service sends an activation link to this address.
	Seat count	This field is for reference purposes only; you can use it to inform the account user about the maximum number of recipient email addresses whose messages can be processed by Secure Messaging Service.
	Password	Logon password for accessing the console.
	API key	This information displays only after an account is created. Secure Messaging Service uses the API key to regulate access to Web services. Your support provider may also use this key to troubleshoot console-related issues.

TABLE 3-1. Account Details (Continued)

SECTION	FIELD	DESCRIPTION
Permissions	Parent account	The account creator; the parent account has control over the account.
	Account type	<p>The account type determines the tasks that the account user can perform in the console.</p> <hr/> <p><b>Note:</b> The available account type options depend on your permissions. No account types will be listed if you do not have the necessary permissions to create accounts.</p> <hr/>
	Permitted tasks	<p>Displays the tasks that the account user can perform with the selected account type. Refer to this list to understand what types of tasks are available to the account.</p> <hr/> <p><b>Note:</b> This section displays only if you have the necessary permissions.</p> <hr/>
	Inherit ability to create the following account types	<p>Determines whether the account is given permission to create the same types of accounts as its parent account. Secure Messaging Service lists these account types in the information box.</p> <hr/> <p><b>Note:</b> Some account types are set as <i>not inheritable</i>. Child accounts cannot inherit the ability to create these types of accounts.</p> <hr/>
	Allow account to manage the following accounts and their domains	Determines whether the account can manage sibling accounts (accounts created by the same parent) and their domains.

**TABLE 3-1. Account Details (Continued)**

SECTION	FIELD	DESCRIPTION
Console Rebranding	Enable console rebranding	<p>Determines whether console rebranding settings are applied.</p> <hr/> <p><b>Note:</b> After an account is created, only the account user will be able to modify console rebranding settings. For details about console rebranding, see <a href="#">Configuring Console Rebranding</a> on page 3-3.</p> <hr/>
	Logo URL	URL of the image file used as the console banner.
	Logon page URL	URL of the Web page used as the lower frame of the logon page.
	Support URL	URL that opens when the account user clicks the <b>Support</b> link in the left pane of the console.
License	License key	The license key may be tied to your account through an external registration or licensing system.
	Expiration	When this date is reached, Secure Messaging Service stops checking both inbound and outbound messages. The account then starts running under a "grace period".
	Grace period	This field corresponds to the length of the grace period, which starts when the license expires, in days. During the grace period, Secure Messaging Service continues to deliver unprocessed messages. However, as soon as the grace period ends, the service starts to reject ( <i>response code 550</i> ) all inbound and outbound messages.



## Account Types

Account types define the types of tasks that account users can perform. Secure Messaging Service supports a wide variety of account types, including custom types that Trend Micro operators can create. The following table lists some of the standard account types in Secure Messaging Service.

**TABLE 3-2. Standard Account Types**

ACCOUNT TYPES	PERMISSIONS TO TASKS				
	CREATE ACCOUNTS	MANAGE POLICIES	TRACK MAIL	HANDLE QUARANTINED MESSAGES	VIEW REPORTS
xsp_reseller	Yes	Yes	Yes	Yes	Yes
xsp_standard	No	Yes	Yes	Yes	Yes
xsp_anti_spam	No	Yes (no anti-virus, attachment, and content filters)	Yes	Yes	Yes
xsp_mailtracking	No	No	Yes	No	No
xsp_view_policy	No	View only	No	No	No
xsp_support	No	View only	Yes	View only	Yes

---

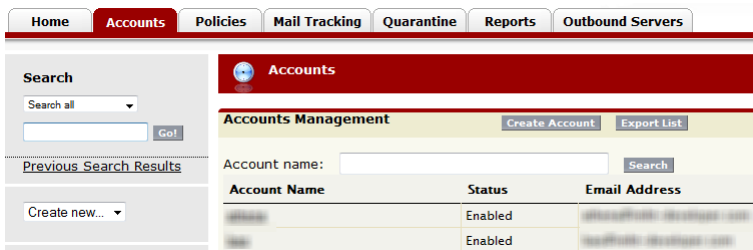
**Note:** Account types may vary. Also, an account type is visible during account creation *only* if you have the necessary permissions to create such an account. Contact your support provider for information on creating additional account types.

---

## Creating or Modifying Accounts

Create an account to allow other users to access the console. An account is typically able to access only the accounts and domains that it creates. It is able to perform only tasks associated with its account type. However, an account may be configured so that it has permissions to certain tasks and data that are accessible to its parent account.

**Click path:** ... > **Accounts**



**FIGURE 3-2. Accounts tab**

### Considerations:

- To understand the account options, see [Accounts Overview](#) on page 3-5.
- No account types will be listed if you do not have the necessary permissions to create accounts.
- Users can customize their accounts by changing their email address, console rebranding settings, and their passwords.
- Specify a valid email address.

### To create an account:

1. Click the **Accounts** tab.
2. Click **Create Account**.
3. Specify the details of the account. Items with asterisks (\*) are required.
4. Click **Save**.

**To modify an existing account:**

1. Click the **Accounts** tab.
2. Manually locate the account on the list or search for it by specifying the name.
3. Click the name of the account to open it.
4. Modify the details of the account and click **Save** or **Delete** the account.

## Exporting the Account List

Export the account list to obtain a local CSV copy of the list of accounts that you manage.

**Click path:** ... > **Accounts**

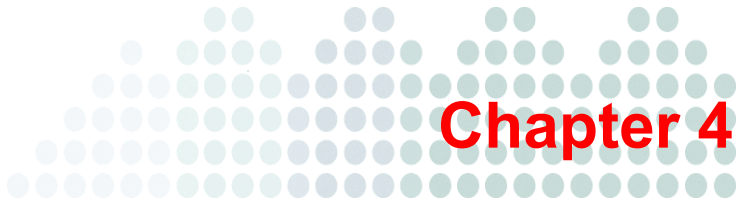
**Considerations:**

- The exported CSV file covers only the accounts that are managed by the currently active account. For information about switching accounts, see [Switching Accounts](#) on page 2-9.
- For each account, the CSV file includes the account name, status, email address, and license key.

**To export the account list:**

1. Click the **Accounts** tab.
2. Click **Export List**.
3. Save the file. If necessary, specify a path and name for the file.





## Understanding Mail Filters

Trend Micro™ Secure Messaging Service sets limits and supports configurable filters for inbound messages. This chapter provides an overview of the inbound filtering capabilities of Secure Messaging Service in the following topics:

- *System Limits* on page 4-2
- *Types of Configurable Filters* on page 4-3
- *Filtering Flow* on page 4-11
- *Filter Actions* on page 4-9

## System Limits

To protect the service infrastructure and ensure availability, Secure Messaging Service enforces the following limits on incoming messages.

**TABLE 4-1. System-wide Message Limits**

<b>CRITERIA</b>	<b>MAXIMUM</b>	<b>WHEN THIS LIMIT IS EXCEEDED...</b>
Message size including all attachments	50MB	Message is rejected (response code 550) before any policy is applied
Number of recipients	1000 recipients	Message is rejected (response code 550) before any policy is applied
Layers of compression for attachments	19 layers	Particular attachment is not checked for malware
Number of files in compressed attachments	300 files	Particular attachment is not checked for malware

## Types of Configurable Filters

Secure Messaging Service uses multiple filters to provide email security. When creating a policy, you can enable specific filters and configure filter options.

**TABLE 4-2. Filter Types**

FILTER TYPE	PRIORITY	DESCRIPTION	RULE SUPPORT
Valid recipients	1	Blocks inbound messages being sent to addresses that are not in a user-specified list	No
Approved senders	2	Allows all inbound messages from addresses in a user-specified list to bypass blocked sender checking and the ERS and anti-spam filters; messages are still checked by the antivirus and attachment filters. For more information, see <a href="#">Filtering Flow</a> on page 4-11.	No
Blocked senders	3	Blocks all inbound messages from addresses in a user-specified list	No
Email Reputation Service (ERS)	4	Blocks messages coming from domains or IP addresses with poor reputation; provides two levels of filtering: <ul style="list-style-type: none"> <li>• Standard—queries the standard reputation database to determine whether the message source is associated with spam</li> <li>• Advanced—queries a dynamic database that intelligently reassesses and adjusts reputation ratings</li> </ul>	No
Anti-spam	5	Performs user-specified filter actions on messages detected as one or both of the following: <ul style="list-style-type: none"> <li>• Spam</li> <li>• Phishing</li> </ul>	Yes

**TABLE 4-2. Filter Types (Continued)**

<b>FILTER TYPE</b>	<b>PRIORITY</b>	<b>DESCRIPTION</b>	<b>RULE SUPPORT</b>
Antivirus	6	Scans both inbound and outbound messages for malware code, deleting messages with malware	No
Attachment	7	Performs user-specified filter actions on messages containing attachments that match at least one of the following criteria: <ul style="list-style-type: none"> <li>• Extension name—user-specified list of unwanted file extension names</li> <li>• Individual size—maximum file size in KB</li> <li>• Total size—maximum total size of all files in KB</li> <li>• Count—maximum number of files</li> </ul>	Yes
Content	8	Checks the subjects or bodies of messages against user-defined regular expression patterns and performs the specified filter actions.	Yes

## Filter Criteria

Filter criteria are the standards used by Secure Messaging Service filters to determine whether or not to apply filter actions to a message. Each filter supports at least one criterion.



The anti-spam, attachment, and content filters support multiple criteria as shown in the table below.

**TABLE 4-3. Filter Criteria**

<b>FILTERS WITH MULTIPLE CRITERIA</b>	<b>FILTER CRITERION</b>	<b>DESCRIPTION</b>	<b>HOW TO CONFIGURE</b>
Anti-spam filter	Spam	When enabled, the filter checks messages for spam-like characteristics. In general, spam messages are sent in bulk and contain unsolicited and unwanted content.	Select catch rate.
	Phishing	When enabled, the filter checks messages for phishing characteristics. Phishing messages often contain links to fake Web sites designed to steal user information.	Select catch rate.
Content filter	Subject	When enabled, the filter checks the message subject for text that matches the specified regular expression pattern.	Specify the regular expression pattern.
	Message body	When enabled, the filter checks the message body for text that matches the specified regular expression pattern.	Specify the regular expression pattern.

**TABLE 4-3. Filter Criteria (Continued)**

<b>FILTERS WITH MULTIPLE CRITERIA</b>	<b>FILTER CRITERION</b>	<b>DESCRIPTION</b>	<b>HOW TO CONFIGURE</b>
Attachment filter	Extension name	When enabled, the filter checks attachment extension names.	Select extension names; attachments with these extension names are filtered.
	Individual size	When enabled, the filter checks individual attachments against a size limit.	Specify the maximum size for individual attachments in KB.
	Total size	When enabled, the filter checks the total size of all attachments in each message against a limit.	Specify the maximum total size of all attachments in KB.
	Count	When enabled, the filter checks the total number of attachments in each message against a limit.	Specify the maximum number of attachments.

## Understanding Email Reputation Service

Email Reputation Service identifies and blocks spam by verifying email source addresses against extensive reputation databases. Email Reputation Service is provided in two versions: standard and advanced.

## Email Reputation Service Standard

The standard service helps block spam by validating sender IP addresses against a relatively static reputation database of established spam sources. This database includes IP addresses of hosts that are typically leveraged to send or relay spam, including public proxy servers.

## Email Reputation Service Advanced

Email Reputation Service advanced uses a dynamic reputation database containing IP addresses that are constantly monitored for spam activity. Trend Micro continuously monitors network and traffic patterns and immediately updates the dynamic reputation database as new spam sources emerge, often within minutes of the first sign of spam. As evidence of spam activity ceases, the dynamic reputation database is updated accordingly.

The dynamic reputation database uses automated, large-scale correlation mechanisms that process large amounts of data to effectively track dynamic spam sources. These dynamic sources are typically infected computers that form botnets.

## Understanding Malware, Spam, and Phishing

Malware, spam, and phishing constitute the most common email messaging threats.

### Malware

Malware programs are typically file-based threats, with some of the more common types being referred to as Trojans, viruses, and worms. Worms—malware programs that can propagate from one system to another—in particular, have been known to successfully spread through email.

Worms spread through email by taking advantage of vulnerabilities in email clients and address books and the lack of security measures in the messaging protocols themselves. Email users typically receive worms embedded as scripts in HTML email or as executable attachments.

Secure Messaging Service uses award-winning Trend Micro antivirus technologies to detect malware in email messages. These technologies incorporate both signature and heuristic identification methods that can detect both known and unknown malware.

## Spam

Spam refers to unsolicited and unwanted electronic messages that are sent out indiscriminately and in bulk. The most widely recognized form of spam is email spam.

Secure Messaging Service protects email users from spam by filtering email messages for recognizable spam content. With Email Reputation Service, Secure Messaging Service can also filter email messages coming from IP addresses associated with spammers.

---

**Note:** The detection of spam messages is influenced by the selected catch rate. For more information, see [Spam and Phishing Catch Rates](#) on page 5-18.

---

## Phishing

Phishing refers to the method of tricking users into submitting user names, passwords, credit card numbers, and other critical information to copycats that mimic trustworthy entities. A sizable number of phishing attacks occur when users submit information to Web pages that mimic banking sites and online payment facilities.

Users are typically lured into phishing sites by fake email and instant messages.

Secure Messaging Service protects email users from phishing by filtering email messages for known phishing content and links. Filtering settings for phishing can be configured as part of the anti-spam filter settings.

---

**Note:** The detection of phishing messages is influenced by the selected catch rate. For more information, see [Spam and Phishing Catch Rates](#) on page 5-18.

---

## Understanding Rules

The anti-spam, attachment, and content filters support rules. With rules, you can create multiple combinations of filter criteria and filter actions. Rules also support rule-specific exceptions based on the recipient address.

Rules are defined during policy creation.









## Filter Actions

With the antivirus, anti-spam, attachment, and content filters, you can select the action to perform on screened messages. Secure Messaging Service can perform multiple actions on the same message. As soon as a match is made to a filter or a filtering criterion, applicable filter actions are performed based on a fixed order. However, if a terminal action is performed, no other subsequent action will be performed.

**TABLE 4-4. Filter Actions**

FILTER ACTION	DESCRIPTION	ORDER	TERMINAL?	FILTER SUPPORT			
				ANTIVIRUS	ANTI-SPAM	ATTACHMENT	CONTENT
Delete message	Deletes the entire message without quarantining it	1	Yes	✓	✓	✓	✓
Quarantine	Saves a copy of the entire message in quarantine; administrators and end users can later delete or deliver the message	2	Yes	✗	✓	✗	✓

TABLE 4-4. Filter Actions (Continued)

FILTER ACTION	DESCRIPTION	ORDER	TERMINAL?	FILTER SUPPORT			
				ANTIVIRUS	ANTI-SPAM	ATTACHMENT	CONTENT
Change recipient	<p>Modifies the message to change its recipient to a specified address</p> <hr/> <p><b>Note:</b> The recipient address should be an address in the domain covered by the policy.</p>	3	Yes				
Replace attachment with text	<p>Replaces the contents of attachments that match the filter criteria with specified text; when the total number of attachments exceeds the specified maximum, all the attachments are modified</p> <hr/> <p><b>Note:</b> This filter action does not modify the file name of attachments, only their contents. To inform email recipients that the contents of an attachment has been modified, use the <i>insert footer text</i> action.</p>	4	No				

**TABLE 4-4. Filter Actions (Continued)**

FILTER ACTION	DESCRIPTION	ORDER	TERMINAL?	FILTER SUPPORT			
				ANTIVIRUS	ANTI-SPAM	ATTACHMENT	CONTENT
Tag subject	Inserts specified text at the end of the subject	5	No	✗	✓	✓	✓
Insert footer text	Inserts specified text at the end of the message body	6	No	✗	✓	✓	✓

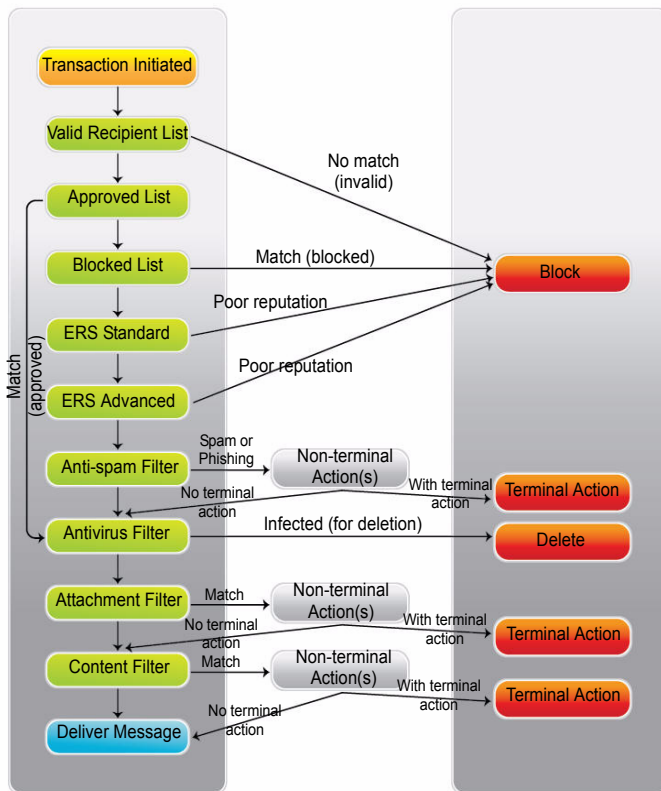
## Filtering Flow

Secure Messaging Service applies a different filtering process for:

- [Inbound Messages](#) on page 4-12
- [Outbound Messages](#) on page 4-14

## Inbound Messages

The following diagram shows the filtering flow for inbound messages. Non-terminal filter actions are actions that do *not* result in the stoppage of other applicable filter actions.



**FIGURE 4-1. Filtering flow of inbound messages**

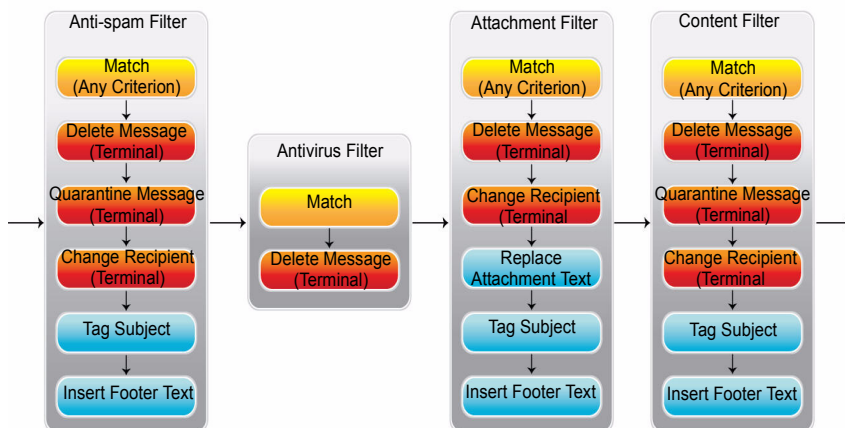
To block messages, Secure Messaging Service rejects transactions with response code 550.



## Multiple Criteria and Filter Actions

Whether you use one or many rules when configuring the anti-spam, the attachment, and content filters, you can have multiple filter criteria and multiple filter actions enabled at the same time. Below is information that can help you determine how messages are filtered in this scenario:

- The anti-spam filter checks messages before the antivirus, the attachment, and the content filters. Messages are assessed against all anti-spam filter criteria and corresponding actions are performed before they are assessed by other filters.
- The selected filter criteria or the listing of rules do not affect the order by which a message is processed by an individual filter. If a message matches one or more criteria, all applicable actions are performed on the message based on a fixed priority.
- If a terminal action (delete, quarantine, or change recipient) is performed, the filtering process ends, regardless if other filters have yet to assess the message.



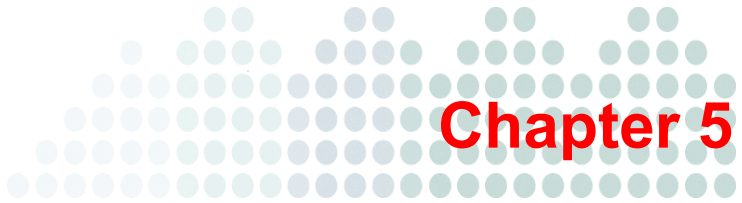
**FIGURE 4-2.** Filter actions and filtering flow

## Outbound Messages

Policy settings for a domain do not affect outbound filtering. To help ensure that email clients in the domain do not spread infected messages or send spam to other domains, a global policy applies the antivirus and anti-spam filters to all outbound messages. Secure Messaging Service then deletes all messages that are caught by these filters.

### **Considerations:**

- Mail tracking cannot be used to check the status of outbound messages.
- To ensure that only messages that are very likely to be spam are filtered, the catch rate for outbound messages is set to the lowest level. For information about catch rates, see [Spam and Phishing Catch Rates](#) on page 5-18.
- For information on how to set up outbound filtering, see [Setting Up Outbound Filtering](#) on page 2-7.



## Filtering Mail

Trend Micro™ Secure Messaging Service filtering settings are configured using policies. This chapter describes all tasks associated with the management of policies. It covers the following topics:

- *Policies Overview* on page 5-2
- *Searching for and Modifying Existing Policies* on page 5-3
- *Creating Policies* on page 5-4

## Policies Overview

Secure Messaging Service offers policy-based management of email security. Each policy applies to a domain and regulates how each filter is applied to messages sent to the domain.

The following table lists the information that defines each policy.

**TABLE 5-1. Policy Sections**

<b>SECTION</b>	<b>DESCRIPTION</b>
Domain	The domain that will be covered by the policy. With the correct routing settings, all email messages to this domain are protected by Secure Messaging Service.
Filter settings	These settings define the following Secure Messaging Service filtering options: <ul data-bbox="485 743 1009 889" style="list-style-type: none"><li>• Whether a filter is enabled or not</li><li>• For filters that support this option, how each filtering criterion is applied</li><li>• For filters that support this option, what filter actions to perform</li></ul>
Destination servers	The destination servers are the inbound mail servers for the domain. These servers receive messages bound for the domain after they are processed by Secure Messaging Service.

## Searching for and Modifying Existing Policies

Modify a policy to enable, disable, or configure the filters that apply to the domain.

**Click path:** ... > **Policies**

Action	Domain	Valid Recipients	Approved Senders	Blocked Senders	ERS Standard	ERS Advanced	Anti Virus	Anti Spam	Attachment
Edit   Del	example.com	⊖	⊕	⊖	⊕	⊕	⊖	⊖	⊖
Edit   Del	example.com	⊖	⊕	⊖	⊖	⊖	⊖	⊕	⊖
Edit   Del	example.com	⊖	⊕	⊖	⊖	⊖	⊖	⊕	⊖

**FIGURE 5-1.** Policies tab

### Considerations:

- Policies are defined by the domain, the filter settings, and the destination server settings.
- By default, a search returns both full and partial matches. To return only exact matches, enclose your search string in double quotes ("").

### To locate and modify a policy:

1. Click the **Policies** tab.
2. Click the name of the policy domain to select a policy. To search for a policy, type part of or the entire domain name under **Domain** and click **Search**.
3. Edit the policy. For details, see [Creating Policies](#) on page 5-4.
4. Click **Save**.

## Creating Policies

To allow Secure Messaging Service to provide email security services to a domain, create a policy for that domain.

### **Considerations:**

- Each policy applies to one domain only and only one policy can be created for a domain.
- A policy comprises a domain, filtering settings, and destination servers.
- Review each filter type and assess whether you want to apply it to the domain before saving the policy. Whether a filter is enabled by default depends on your account type.
- Trend Micro *strongly* recommends that you have the antivirus and anti-spam filters enabled and properly configured. Without these filters, the domain is highly vulnerable to large numbers of unwanted mail and infected messages.

### **To create a policy:**

1. Click the **Policies** tab.
2. Click **Create Policy**.
3. Type the domain.
4. Specify destination servers. See [Specifying Destination Servers](#) on page 5-5.
5. Configure the individual filters.
  - a. Specify valid recipients. See [Specifying Valid Recipients](#) on page 5-8.
  - b. Specify approved and blocked senders. See [Specifying Approved and Blocked Senders](#) on page 5-10.
  - c. Enable Email Reputation Service. See [Enabling Email Reputation Service](#) on page 5-12.
  - d. Configure the antivirus filter. See [Configuring the Antivirus Filter](#) on page 5-13.
  - e. Configure the anti-spam filter. See [Configuring the Anti-spam Filter](#) on page 5-15.
  - f. Configure the content filter. See [Configuring the Content Filter](#) on page 5-20.
  - g. Configure the attachment filter. See [Configuring the Attachment Filter](#) on page 5-27.
6. Click **Save**.

## Specifying Destination Servers

To ensure that inbound messages are checked, point the MX records for the domain to the Secure Messaging Service FQDN. During policy creation, specify the domain's actual destination servers to allow Secure Messaging Service to deliver messages to these servers after processing.

**Click path:** ... > **Policies** > **Create Policy** > **Destination Servers**

The screenshot shows the 'Policies' management interface. At the top, there is a search bar for domains. Below it, the 'Domain' is set to 'example.com'. The 'Destination Servers' tab is active, showing a table with the following data:

Type	Server	Port	Preference
<input checked="" type="checkbox"/> IP	172.16.254.1	25	10

**FIGURE 5-2.** Destination Servers tab

### Considerations:

- Secure Messaging Service supports different destination server options that let you point to A or MX records on your DNS or to IP addresses directly.
- Use the **Preference** option to specify routing priority for the destination servers. Secure Messaging Service will attempt to deliver messages to servers with lower preference values first. You can specify a value from 0 to 65535.

### To specify destination servers:

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Destination Servers** tab, specify the entry types, the servers (FQDN, IP address, or subdomain), their ports, and their routing priorities (preference). For more information, see [Destination Server Options](#) on page 5-6.
4. Click **Save**.

## Destination Server Options

After processing, Secure Messaging Service relays inbound messages to the domain's destination servers. To allow Secure Messaging Service to relay mail to the correct servers, specify destination servers during policy creation.

Secure Messaging Service supports several ways of specifying destination servers:

- [Pointing to A Records](#) on page 5-6
- [Pointing to MX Records](#) on page 5-7
- [Pointing to IP Addresses Directly](#) on page 5-8

### Pointing to A Records

Use this option to point to a corresponding mail server *A* record on the DNS. Secure Messaging Service will perform a DNS query to locate the particular server.

When using only this option, you need to specify an entry for each inbound mail server used by the domain. To control routing priority across multiple mail servers, specify preference values for each entry. Secure Messaging Service will attempt to send mail to servers with lower preference values first.

#### **Example:**

##### **DNS Records**

```
mail1.example.com A 192.168.1.1  
mail2.example.com A 192.168.1.2
```

##### **Destination Servers**

The following entries tell Secure Messaging Service to deliver mail to two mail servers identified by their *A* records on the DNS. Secure Messaging Service will prioritize the first mail server, which has a lower preference value.

TYPE	SERVER	PORT	PREFERENCE
A	mail1.example.com	25	1
A	mail2.example.com	25	2



## Pointing to MX Records

Use this option to point to MX records on the DNS. With this option, you can insert only one entry to cover all inbound mail servers used by the domain. To control routing priority, you need to set preference values on the MX records themselves.

To use this option, you need to define a subdomain and create corresponding MX records for that subdomain. Assuming that your mail servers already have corresponding A records, you then need to point the subdomain's MX records to the FQDNs of these mail servers. Once you have the subdomain's MX records in place, specify the subdomain as the destination server.

---

**Note:** Do *not* specify the policy domain itself as the destination server. MX records for this domain should point to Secure Messaging Service.

---

### Example:

#### DNS Records

```
example.com MX 1 filter.trendmicro.com
filter.example.com MX 1 mail1.example.com
filter.example.com MX 2 mail2.example.com
mail1.example.com A 192.168.1.1
mail2.example.com A 192.168.1.2
```

#### Destination Servers

The following entry tells Secure Messaging Service to deliver mail to mail servers identified by MX records for the subdomain `filter.example.com`. Routing priority is also determined by the MX records on the DNS.

TYPE	SERVER	PORT	PREFERENCE
MX	filter.example.com	25	1

## Pointing to IP Addresses Directly

Use this option to specify mail server IP addresses and allow Secure Messaging Service to locate the mail servers without performing a DNS query. To control routing priority across multiple mail servers, specify preference values for each entry in the list of destination servers.

### **Example:**

#### **DNS Records**

```
mail1.example.com A 192.168.1.1
```

```
mail2.example.com A 192.168.1.2
```

---

**Note:** Because this option allows Secure Messaging Service to connect to mail servers directly using IP addresses, DNS records have no effect on routing.

---

#### **Destination Servers**

The following entries tell Secure Messaging Service to deliver mail to two mail servers identified by their IP addresses. Secure Messaging Service prioritizes the first mail server because it has a lower preference value.

TYPE	SERVER	PORT	PREFERENCE
IP	192.168.1.1	25	1
IP	192.168.1.2	25	2

## Specifying Valid Recipients

During policy creation, you can enable filtering for valid recipients. By enabling this filter, you block all messages that are not destined for the specified recipients.

**Click path: ... > Policies > Create Policy > Valid Recipients**

The screenshot shows the 'Valid Recipients' tab in a web-based configuration interface. At the top, there is a 'Domain:' field with a search button. Below this, there are navigation tabs: 'Destination Servers', 'Valid Recipients' (which is selected and highlighted in red), 'Approved Senders', 'Blocked Senders', 'ERS', and 'Antivirus'. Under the 'Valid Recipients' tab, there is a checkbox labeled 'Allow only mail sent to valid recipients' which is checked. Below the checkbox, there is an 'Email address:' field containing 'local-part'. To the right of this field is a 'Valid recipients' list area with 'Add' and 'Remove' buttons.

**FIGURE 5-3. Valid Recipients tab**

**Considerations:**

- If you enable this filter but do not specify any valid recipients, all inbound messages will be blocked.
- When using the valid recipients list, ensure that you specify all the recipient addresses in the domain.
- Specify only the *local-part* (`local-part@example.com`) of the email address when adding an address to the valid recipients list.

**When importing recipient addresses:**

- You can import recipient addresses from text files in the following formats:
  - LDIF—the service imports all email addresses with matching domains using the "proxyaddresses" attributes.
  - CSV—use a single-column CSV with only one recipient address (local-part or full address) per line. For full addresses, only those with matching domains are imported.
- Ensure that you select the correct import mode. Selecting **Replace List** will delete *all* existing addresses from the list.
- Clicking **Commit** starts the import process, which you will not be able to cancel or undo.

**To specify valid recipients:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or **Create Policy**.
3. In the **Valid Recipients** tab, ensure that **Allow only mail sent to valid recipients** is selected.
4. Add email addresses to the list.
  - To add an email address, type its local-part under **Email address** and click **Add**.
  - Click **Import** to import multiple addresses from an LDIF or a CSV file.
5. Click **Save**.

## Specifying Approved and Blocked Senders

During policy creation, you can enable filtering of messages based on sender email or IP address. The service allows messages from approved senders to bypass the Email Reputation Service (ERS) and anti-spam filters, while rejecting messages from blocked senders.

**Click path:** ... > **Policies** > **Create Policy** > **Approved/Blocked Senders**

The screenshot shows the 'Policies' management interface. At the top, there is a red header with a 'Policies' tab and a search bar. Below this, a domain is selected, and there are 'Save', 'Cancel', and 'Create Policy' buttons. A navigation bar contains several tabs: 'Destination Servers', 'Valid Recipients', 'Approved Senders' (which is highlighted in red), 'Blocked Senders', 'ERS', and 'Antivirus'. Under the 'Approved Senders' tab, there is a checkbox labeled 'Enable the approved senders list' which is checked. Below the checkbox, there is a text input field for 'Email or IP address(es):' containing 'sender@example.com'. To the right of this field are two buttons: 'Add' and 'Remove'. Further to the right, there are two tabs: 'Email' (highlighted in red) and 'IP'. Below these tabs is a list area for approved senders.

**FIGURE 5-4.** Approved Senders tab

**Considerations:**

- The approved lists take precedence over the blocked list, the Email Reputation Service filter, and the anti-spam filter. All messages from addresses that match the addresses in the approved list are not processed by these filters. For more information, see *Filtering Flow* on page 4-11.
- The wildcard character \* may be used to specify any string in the *local-part* (local-part@example.com) of email addresses. Use wildcard characters with *caution* as they may allow or block messages from a large set of email addresses.
- Specifying an IP address will block or approve all messages from that IP address.
- When importing sender addresses:
  - Use a single-column CSV file with only one full email or IP address per row. The import function does *not* support wildcards.
  - Ensure that you select the correct import mode. Selecting **Replace List** will delete *all* existing email and IP addresses from the list.
  - Clicking **Commit** starts the import process, which you will not be able to cancel or undo.

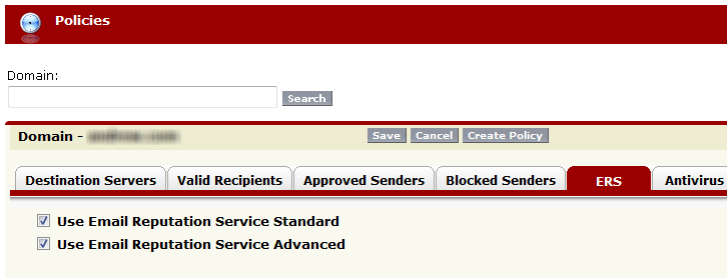
**To specify approved or blocked senders:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or **Create Policy**.
3. Ensure that the filter is enabled by selecting:
  - **Enable the approved senders list** in the **Approved Senders** tab
  - **Disallow all mail from blocked senders** in the **Blocked Senders** tab
4. Add email addresses to the list.
  - To add an email or IP address, type the address under **Email or IP address(es)** and click **Add**. To specify multiple email addresses, use the wildcard character \* in the local-part. For example, to allow or block all messages from domain.com, type \*@example.com and click **Add**.
  - Click **Import** to import multiple addresses from a CSV file.
5. Click **Save**.

## Enabling Email Reputation Service

By enabling Email Reputation Service (ERS), you take advantage of a dynamic and constantly updated email source rating system to block spam and other unwanted email messages. ERS blocks messages from source IP addresses whose current reputation ratings are poor.

**Click path:** ... > **Policies** > **Create Policy** > **ERS**



**FIGURE 5-5.** ERS tab

### **Considerations:**

You can enable the following service types:

- **Standard**—queries the standard reputation database to determine whether the message source is associated with spam
- **Advanced**—queries a dynamic database that is updated in real time

For more information about Email Reputation Service, see [Understanding Email Reputation Service](#) on page 4-6.

### **To enable Email Reputation Service:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or **Create Policy**.
3. In the **ERS** tab, select either or both of the following options:
  - **Use Email Reputation Service Standard**
  - **Use Email Reputation Service Advanced**
4. Click **Save**.

## Configuring the Antivirus Filter

When enabled, the antivirus filter can stop email messages containing known and unknown malware code, whether this code is contained in an attachment or embedded in the message body.

**Click path:** ... > **Policies** > **Create Policy** > **Antivirus**

The screenshot shows the 'Policies' configuration page. At the top, there is a 'Domain:' field with a 'Search' button. Below this is a 'Domain - outlook.com' header with 'Save', 'Cancel', and 'Create Policy' buttons. The 'Antivirus' tab is selected, showing a 'Check mail for malware' checkbox which is checked. Under 'Filter Criteria', it says 'If message contains malware'. Under 'Filter Actions', the 'Delete message' checkbox is checked.

**FIGURE 5-6.** Antivirus tab

### Considerations:

Email messages found to contain malware code are automatically deleted. To inform original recipients or other individuals, enable and configure antivirus notifications.

### To enable the antivirus filter:

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or **Create Policy**.
3. In the **Antivirus** tab, ensure that **Check mail for malware** is selected.
4. To send a notification to original recipients, select **Send notification using** and specify the details of the message. For details, see [Sending Antivirus Notifications](#) on page 5-14.
5. Click **Save**.

## Sending Antivirus Notifications

The antivirus filter automatically deletes messages that are found to contain malware code. Configure antivirus notifications to send a notification whenever the antivirus filter detects a message.

**Click path:** ... > **Policies** > **Create Policy** > **Antivirus**

### Considerations:

- When enabled, notifications are sent every time an infected message is detected and deleted.
- The default message is sent to the original recipients of the infected message.
- By default, notification messages are sent from the following email address:  
no-reply@emailsecurity.trendmicro.com

### When defining a custom notification message:

- Select **Send to original recipients** to send the notification to the original recipients of the infected message.
- The sender (from) and recipient (to) email addresses should be in one of the domains covered by your policies.
- When specifying multiple recipients, separate each address with a comma (,).
- You can use the following tokens when defining the body of the custom message.

**TABLE 5-2. Antivirus Notification Tokens**

TOKEN	DESCRIPTION
%SENDER%	Email address of the sender of the infected message
%DATE&TIME%	Date and time (in GMT) the infected message was sent
%SUBJECT%	Subject of the infected message



### To configure antivirus notifications:

1. While configuring the antivirus filter in the **Antivirus** tab, ensure that **Check mail for malware** and **Delete message** are selected.
2. Select **Send notification using** and choose whether to send a default message or to specify a custom message.
  - **Default message**—send a predefined message to the original recipients of the infected message
  - **Custom message**—specify the contents and the recipients of the message
3. Click **Save** when you are done configuring the antivirus filter.

## Configuring the Anti-spam Filter

When enabled, the anti-spam filter checks email messages for spam and phishing characteristics. The filter identifies messages as spam based on the selected catch rate.

**Click path:** ... > **Policies** > **Create Policy** > **Anti-spam**

Domain:

Domain - **contoso.com**

Enable the anti-spam filter

Rule	Type	Catch Rate	Action
<input type="checkbox"/>	Spam Phish	Spam : Highest Phish : Highest	Delete

**FIGURE 5-7.** Rule list in the Anti-spam tab

**Considerations:**

The anti-spam filter supports multiple rules, each containing complete filtering settings, including the filter criteria, the filter actions, and any exceptions to the rule.

**To configure the anti-spam filter:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Anti-spam** tab, ensure that **Enable the anti-spam filter** is selected.
4. Perform the following actions to configure the anti-spam filter:
  - To enable or disable a rule, click **Disabled** or **Enabled**. The label on the button reflects the current status of the rule.
  - To delete a rule, select the rule and then click **Delete**.
  - To edit a rule, click the name of the rule.
  - To create a new rule, click **Create Rule**. For instructions, see [Creating an Anti-spam Rule](#) on page 5-16.

## Creating an Anti-spam Rule

Create an anti-spam rule to define a set of filter criteria for spam and phishing messages and the actions to be performed on messages that match these criteria.

**Click path: ... > Policies > Create Policy > Anti-spam > Create Rule**

**Policies**

Domain:

Domain - **example.com**

**Destination Servers** **Valid Recipients** **Approved Senders** **Blocked Senders** **ERS** **Antivirus** **Anti-spam** **Attachment**

**Enable Rule**  
 Rule name

**Filter Criteria**

**Filter spam messages** **Baseline spam catch rate:**

**Filter phishing messages** **Baseline phishing catch rate:**

**Filter Actions**

**Delete message**

**Quarantine**

**Change recipient to**

**Tag subject**

**Insert stamp in footer Plain text:**

**Exceptions**

**Do not apply rule to mail for recipients in the exceptions list**

**Email address:**

**Exceptions**

**FIGURE 5-8. Anti-spam rule creation screen**

**Considerations:**

- You can choose to filter spam messages, phishing messages, or both.
- Creating separate rules for spam and phishing will let you apply different filter actions to spam and phishing messages.

- Consider the impact of the catch rate and the filter action on normal messages. For example, if you have selected a relatively high catch rate, consider quarantining messages instead of deleting them. You can create multiple rules to cover different catch rates. For more information about spam and catch rates, see [Spam and Phishing Catch Rates](#) on page 5-18.
- Each rule can have an exception list of recipient addresses such that the rule does not apply to messages sent to these addresses. Addresses in the exception list must be in the domain covered by the policy. Specify only the *local-part* (local-part@example.com) of these addresses.

#### **To create an anti-spam rule:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Anti-spam** tab, ensure that **Enable the anti-spam filter** is selected.
4. Click **Create Rule**.
5. Type a descriptive name for the rule.
6. Under **Filter Criteria**, select whether to filter for spam messages, phishing messages, or both and select a catch rate.
7. Under **Filter Actions**, select your preferred action.
8. Under Exceptions, select **Do not apply rule to mail for recipients in the exceptions list** so that messages sent to specified email addresses are *not* checked against the rule. Add addresses to the exception list by specifying one address at a time.
9. Click **Save**.

## **Spam and Phishing Catch Rates**

A catch rate refers to the degree of sensitivity by which messages are detected as spam or phishing. Spam and phishing detection involves analyzing message characteristics, including the sender address, source servers, strings, links, and images. A high or low catch rate increases or decreases the sensitivity of the detection mechanism to spam- or phishing-like message characteristics, thereby affecting the likelihood that spam or phishing messages are detected.

The most aggressive catch rates have the highest chance of catching all spam or phishing messages, but they also have the highest chance of falsely detecting normal messages. The most conservative settings yield the least number of detections, but have very few false detections.

### Spam Catch Rates

The available catch rate options are:

- Highest
- High
- Moderately High
- Moderately Low
- Low
- Lowest

### Phishing Catch Rates

Because phishing normally involves fake Web sites, phishing detection focuses on analyzing embedded links. Secure Messaging Service supports phishing catch rates that are closely tied to link safety information.

**TABLE 5-3. Phishing catch rates**

<b>CATCH RATE</b>	<b>DESCRIPTION</b>
High	Catches messages with links to: <ul style="list-style-type: none"><li>• Known phishing and malware sites</li><li>• Potentially malicious sites</li><li>• Sites associated with spam or possibly compromised</li></ul>
Medium	Catches messages with links to: <ul style="list-style-type: none"><li>• Known phishing and malware sites</li><li>• Potentially malicious sites</li></ul>
Low	Catches messages with links to: <ul style="list-style-type: none"><li>• Known phishing and malware sites</li></ul>

## Selecting a Catch Rate

By increasing the catch rate, you will catch more spam or phishing messages. This, however, can increase the likelihood of normal messages being detected.

Consider your anti-spam filter actions before selecting the catch rate. Selecting a high catch rate may be acceptable if you do *not* select "delete" as the filter action.

## Configuring the Content Filter

When enabled, the content filter can apply filter actions on email messages whose subjects or message bodies contain text that matches specified regular expression patterns.

**Click path: ... > Policies > Create Policy > Content**

The screenshot shows the 'Policies' management interface. At the top, there's a search bar for domains. Below that, a domain is selected, and several tabs are visible: Destination Servers, Valid Recipients, Approved Senders, Blocked Senders, ERS, Antivirus, Anti-spam, **Content**, and Attachment. The 'Content' tab is active, and the 'Enable content filter' checkbox is checked. Below this, there are 'Delete' and 'Create Rule' buttons. A table lists the configured rules:

	Rule	Type	Action	Modified	Status
<input type="checkbox"/>	Rule1	Subj	Delete	July 08, 2010 17:27	Enabled
<input type="checkbox"/>	Rule2	Subj Body	Quarantine	July 08, 2010 17:27	Enabled

**FIGURE 5-9. Rule list in the Content tab**

### Considerations:

The content filter supports multiple rules, each containing complete filtering settings, including the filter criteria, the filter actions, and any exceptions to the rule.

### To configure the content filter:

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Content** tab, ensure that **Enable content filter** is selected.

4. Perform the following actions to configure the content filter:
  - To enable or disable a rule, click **Disabled** or **Enabled**. The label on the button reflects the current status of the rule.
  - To delete a rule, select the rule and then click **Delete**.
  - To edit a rule, click the name of the rule.
  - To create a new rule, click **Create Rule**.

## Creating a Content Filter Rule

Create a content filter rule to specify the regular expression patterns that Secure Messaging Service matches to text in the subject and bodies of messages and the actions it performs on messages that contain matching text.

**Click path: ... > Policies > Create Policy > Content > Create Rule**

Destination Servers Valid Recipients Approved Senders Blocked Senders ERS Antivirus Anti-spam **Content** Attachment

**Enable rule** ?  
 Rule name:

**Filter Criteria**

Specify the text to filter. Note that the content filter supports [Perl Compatible Regular Expressions](#) and gives special meaning to certain characters ( \ ( ) { } [ ] . ^ \$ \* + ? ).

**Check message subject for the following content:**

**Check message body for the following content:**

**Filter Actions** ?

Delete message

Quarantine

Change recipient to:   
 Specify an email address in the domain covered by this policy.

Insert text

Tag subject:

Insert stamp in footer **Plain text:**

**Exceptions**

Do not apply rule to mail for recipients in the exceptions list

Email address:  **Exceptions**

**FIGURE 5-10. Content filter rule creation screen**

**Considerations:**

- Each rule can have an exception list of recipient addresses such that the rule does not apply to messages sent to these addresses. Addresses in the exception list must be in the domain covered by the policy. Specify only the *local-part* (local-part@example.com) of these addresses.



- When using non-alphanumeric characters to specify the text to filter, note that the content filter recognizes regular expression patterns. With regular expression, certain characters (\ | ( ) { } [ ] . ^ \$ \* + ?) have special meaning and are not matched literally. For more information, see [Regular Expressions](#) on page 5-24.
- Use only ASCII characters. The content filter cannot match double-byte characters, including East Asian characters.
- By default, regular expression matching is case sensitive. To invoke case-insensitive matching, use (?i) at the beginning of the pattern.

**To create an attachment filter rule:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Content** tab, ensure that **Enable content filter** is selected.
4. Click **Create Rule**.
5. Type a descriptive name for the rule.
6. Under **Filter Criteria**, enable and configure the following options as preferred.

**TABLE 5-4. Filter Criteria for Content**

OPTION	DESCRIPTION	CONFIGURATION PROCEDURE
<b>Check message subject for the following content</b>	Checks if the specified regular expression pattern matches text in the message subject	Select option to enable and type alphanumeric text or specify a regular expression pattern
<b>Check message body for the following content</b>	Checks if the specified regular expression pattern matches text in the message body	Select option to enable and type alphanumeric text or specify a regular expression pattern

7. Under **Filter Actions**, select your preferred action.
8. Under **Exceptions**, select **Do not apply rule to mail for recipients in the exceptions list** so that messages sent to specified email addresses are *not* checked against the rule. Add addresses to the exception list by specifying one address at a time.
9. Click **Save**.

## Regular Expressions

The content filter supports Perl Compatible Regular Expressions (PCRE). When matching simple strings with alphanumeric characters only, the content filter looks for exact and literal matches. For example, the string "spam" matches only strings with the same four letters in the same exact order. The content filter, however, recognizes regular expression patterns, which you can define using the following special characters:

() [] {} . \* + ? ^ \$ \

Within character sets defined by [], only the following special characters can be used:

[] \ - ^

## Special Characters

The following table describes the special characters and how they are used.

**TABLE 5-5. PCRE Special Characters**

CHARACTER	DESCRIPTION	EXAMPLES
\	Escapes (suppresses any special meaning given to) the succeeding special character; as a result, the special character is matched literally	\.exe suppresses the special meaning of "." and matches ".exe"
^	Indicates the start of a line  <b>Note:</b> Use \b to mark the start or the end of a string.	^s matches the "s" in "spam" but not in "message"

**TABLE 5-5. PCRE Special Characters (Continued)**

CHARACTER	DESCRIPTION	EXAMPLES
\$	Indicates the end of a line	m\$ matches the "m" in "spam" but not in "empty"
.	Matches any character except the <i>newline</i> character	s.am matches "spam", "scam", and "slam"
?	Matches 0 or 1 occurrence of the preceding character	sp?am matches "spam" and "sam"
*	Matches 0 or more occurrences of the preceding character	am* matches "a" in "spa", "am" in "spam", "amm" in "spammy"
+	Matches 1 or more occurrences of the preceding character	sp+am matches "spam" and "spppam", but not "sam"
	Matches either the preceding or the succeeding character	sp cam matches "spam" and "scam"
[]	Defines a character set; matches any one character in the set	s[pc]am matches "spam", "scam", and "slam", but not "sham"
[-]	Indicates a character range in a character set defined by []; matches any one character in the range	[a-z] matches any alphabetic character from a to z
[^]	Matches any character that is not in the set	s[^cl]am does not match "scam" and "slam", but matches "spam"

**TABLE 5-5. PCRE Special Characters (Continued)**

CHARACTER	DESCRIPTION	EXAMPLES
()	Defines a subpattern; matches to subpatterns can be referenced using \$1, \$2, ..., \$n	<ul style="list-style-type: none"> <li>• (s[pc]am) matches "spam" and "scam"</li> <li>• If "spam" and "scam" are respectively the first and second matches to the subpattern, then:               <ul style="list-style-type: none"> <li>• \$1my matches "spammy"</li> <li>• \$2mer matches "scammer"</li> </ul> </li> </ul>
{}	Defines the number of occurrences of the preceding character to match; you can specify: <ul style="list-style-type: none"> <li>• An exact number {number}</li> <li>• A range {minimum,maximum}</li> <li>• A minimum {minimum,}</li> <li>• A maximum {,maximum}</li> </ul>	<ul style="list-style-type: none"> <li>• sp{2}am matches "sppam" only</li> <li>• sp{2,3}am matches "sppam", and "sppppam", but not "spam" and "sppppam"</li> <li>• sp{1,}am matches "spam", "sppam", "sppppam", "sppppppam", and so on</li> <li>• sp{,3}am matches "sam", "spam" "sppam", and "sppppam", but not "sppppppam"</li> </ul>

### Syntax Notes

Before defining regular expression patterns, review the following notes:

- Use only ASCII characters. The content filter *cannot* match double-byte characters, including East Asian characters.
- By default, regular expression matching is case sensitive. To invoke case-insensitive matching, use (?i) at the beginning of the pattern.

- To support multi-line matching, use (?m) at the beginning of the pattern.
- To indicate the start or end of a string, use \b.
- For more information about PCRE syntax, visit <http://perldoc.perl.org/perlre.html>.

## Configuring the Attachment Filter

When enabled, the attachment filter can apply filter actions on email messages whose attachments match specified criteria.

**Click path:** ... > **Policies** > **Create Policy** > **Attachment**

The screenshot shows the 'Policies' configuration page. At the top, there is a search bar for domains. Below it, a 'Domain' dropdown is set to 'example.com'. A row of tabs includes 'Destination Servers', 'Valid Recipients', 'Approved Senders', 'Blocked Senders', 'ERS', 'Antivirus', 'Anti-spam', and 'Attachment'. The 'Attachment' tab is selected. Below the tabs, there is a checkbox labeled 'Enable attachment filter'. Underneath, there is a 'Delete' button and a 'Create Rule' button. A table lists the rules:

	Rule	Type	Action	Modified	Status
<input type="checkbox"/>	100-0000	Ext	Stamp		Enabled
<input type="checkbox"/>	100-0000	Size	Delete		Enabled
<input type="checkbox"/>	1000				Enabled

**FIGURE 5-11.** Rule list in the **Attachment** tab

### Considerations:

The attachment filter supports multiple rules, each containing complete filtering settings, including the filter criteria, the filter actions, and any exceptions to the rule.

### To configure the attachment filter:

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Attachment** tab, ensure that **Enable attachment filter** is selected.

4. Perform the following actions to configure the attachment filter:
  - To enable or disable a rule, click **Disabled** or **Enabled**. The label on the button reflects the current status of the rule.
  - To delete a rule, select the rule and then click **Delete**.
  - To edit a rule, click the name of the rule.
  - To create a new rule, click **Create Rule**.

## Creating an Attachment Filter Rule

Create an attachment filter rule to define a set of filter criteria for messages based on the characteristics of their attachments and the actions to be performed on messages that match these criteria.

**Click path:** ... > **Policies** > **Create Policy** > **Attachment** > **Create Rule**

The screenshot shows the 'Attachment' tab in a policy configuration interface. The 'Enable Rule' checkbox is checked, and the rule name is 'Large Attachments'. Under 'Filter Criteria', the 'Total file size is larger than' checkbox is checked with a value of 10000 KB. Under 'Filter Actions', the 'Insert footer text' and 'Replace attachment with text' checkboxes are checked. The footer text is: "The attachment(s) in this message have been modified by Trend Micro Secure Messaging Service because of a policy violation." The replacement text is: "File content removed." Under 'Exceptions', the 'Do not apply rule to mail for recipients in the exceptions list' checkbox is checked, and an email address 'support\_mailbox@example.com' is entered in the 'Email address' field.

**FIGURE 5-12.** Attachment filter rule creation screen

**Considerations:**

- Use filter actions such as "tag subject" and "insert footer text" to spread awareness about attachment restrictions in your organization. For more information, see *Filter Actions* on page 4-9.
- When using the filter action "replace attachment with text", use the action "insert footer text" to notify recipients that the contents of attachments have been replaced. For example, you can insert the following footer:  
  
*"The attachment(s) in this message have been modified by Trend Micro Secure Messaging Service because of a policy violation."*
- Secure Messaging Service is unable to detect .eml (Outlook™ Express email) attachments and treats such attachments as part of the body of the message. Any files that are attached to undetected .eml files are treated as attachments to the message itself.
- Each rule can have an exception list of recipient addresses such that the rule does not apply to messages sent to these addresses. Addresses in the exception list must be in the domain covered by the policy. Specify only the *local-part* (local-part@example.com) of these addresses.

**To create an attachment filter rule:**

1. Click the **Policies** tab.
2. Click the domain name of a listed policy or click **Create Policy**.
3. In the **Attachment** tab, ensure that **Enable attachment filter** is selected.
4. Click **Create Rule**.
5. Type a descriptive name for the rule.

- Under **Filter Criteria**, enable and configure the following options as preferred.

**TABLE 5-6. Filter Criteria for Attachments**

OPTION	DESCRIPTION	CONFIGURATION PROCEDURE
Extension name	Filters messages based on the extension names of attachments; for the list of supported extension names, see <a href="#">Attachment Extension Names</a> on page 5-31	Click <b>List</b> to specify extension names.
Individual file size is larger than	Filters messages with attachments larger than the specified size	Type the size in KB.
Total file size is larger than	Filters messages whose total attachment size is larger than the specified size	Type the size in KB.
Total number of files is more than	Filters messages with more attachments than the specified maximum	Type the maximum number of attachments

- Under **Filter Actions**, select your preferred action.
- Under **Exceptions**, select **Do not apply rule to mail for recipients in the exceptions list** so that messages sent to specified email addresses are *not* checked against the rule. Add addresses to the exception list by specifying one address at a time.
- Click **Save**.



## Attachment Extension Names

The attachment filter can check messages with attachments that match selected extension names. You can choose to filter for any or all of the following extension names.

**TABLE 5-7. Supported Extension Names for Attachment Filtering**

EXTENSION NAME	DESCRIPTION / COMMON ASSOCIATIONS
.386	Windows virtual device driver
.acm	Audio Compression Module add-on
.asp	Active Server Pages
.avb	AntiViral Toolkit Pro Bases
.bat	Batch file
.bin	Binary file; text mode memory dump
.cgi	Common Gateway Interface script
.chm	Compiled help file
.cla	Clarion source file
.class	Java class file
.cmd	Command Prompt batch file
.cnv	Microsoft Word import DLL
.com	DOS executable
.cs*	C# source file; cascading style sheet (.css); comma-separated values text file (.csv)
.dll	Dynamic-link library
.drv	Driver

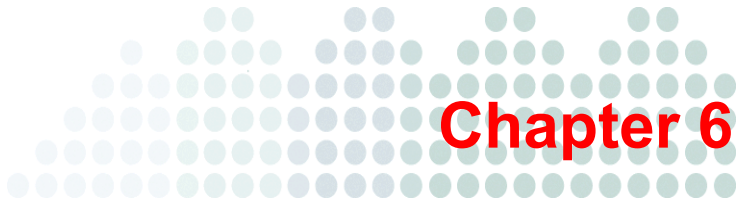
**TABLE 5-7. Supported Extension Names for Attachment Filtering (Continued)**

<b>EXTENSION NAME</b>	<b>DESCRIPTION / COMMON ASSOCIATIONS</b>
.exe	Self-contained executable
.gms	GhostMouse script
.hlp	Help file
.hta	HTML program
.htm*	Hypertext Markup Language file (.htm or .html)
.htt	Microsoft hypertext template
.inf	Information file
.ini	Initialization file
.js*	JScript source file (.js); Java Server Pages (.jsp)
.lnk	Windows shortcut
.mht*	Web archive file (*.mht)
.mpd	Device driver; Windows mini-port driver
.ocx	OLE custom control
.opo	Psion OPL object
.ovl	Overlay file
.php	PHP script file
.pif	Program information file
.pl	Perl source file

**TABLE 5-7. Supported Extension Names for Attachment Filtering (Continued)**

<b>EXTENSION NAME</b>	<b>DESCRIPTION / COMMON ASSOCIATIONS</b>
.prc	Rational Rose Processes; Corel Presentation file; Palm OS resource file
.reg	Windows registry file
.scr	Silverlight file; DOS debug input file; Windows screensaver file





## Monitoring and Tracking

Trend Micro™ Secure Messaging Service allows you to track specific messages, view quarantined messages, and generate reports. This chapter covers tasks associated with these features in the following topics:

- *Viewing Summary Information* on page 6-2
- *Tracking Messages* on page 6-4
- *Viewing Quarantined Messages* on page 6-5
- *Using Reports* on page 6-7

## Viewing Summary Information

Secure Messaging Service makes filtering data highly visible through the dashboard in the **Home** tab and several types of reports.

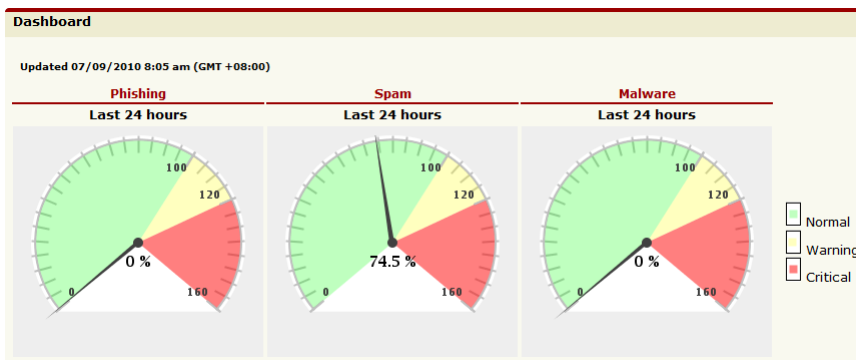


FIGURE 6-1. Dashboard

## Dashboard Data Explained

The dashboard displays relative filtering results for the following email threats:

- Phishing
- Spam
- Malware

The graphs on the dashboard compare the number of threat messages filtered in the past 24 hours against the daily average from the past 10 days. The values shown in the graphs are calculated using the following equation:

$$\text{Displayed value} = \frac{\text{(No. of messages filtered in the past 24 hours)}}{\text{(Average no. of messages filtered in the past 10 days)}}$$

The examples in the table below show how the values displayed in the graphs are calculated.

**TABLE 6-1. Calculation Examples for Dashboard Data**

	<b>DAILY AVERAGE FROM PAST 10 DAYS (BASELINE)</b>	<b>PAST 24 HOURS</b>	<b>CALCULATION</b>	<b>DISPLAYED VALUE</b>
Example 1	1000	1200	1200/1000	120%
Example 2	500	400	400/500	80%

### Calculating the 10-day average

When calculating the average number of messages filtered in the past 10 days, days with zero (0) or no messages filtered are not considered. For example, if no messages are filtered for 5 days in the past 10 days, the average is calculated as the total number of message filtered divided by 5.

The 10-day average is calculated using the following equation:

$$\begin{array}{l}
 \text{10-day average} = \frac{\text{(Total no. of messages filtered in the past 10 days)}}{\text{(No. of days in the past 10 days with at least 1 filtered message)}}
 \end{array}$$

## Using the Dashboard

The Home tab provides quick information through the following sections:

- Dashboard—current threat levels relative to the past 10 days
- News and Announcements—real-time service information
- System maintenance—maintenance schedules and reminders

**Considerations:**

The dashboard displays relative filtering results for the different email threats. For more information, see [Dashboard Data Explained](#) on page 6-2.

**To view the dashboard:**

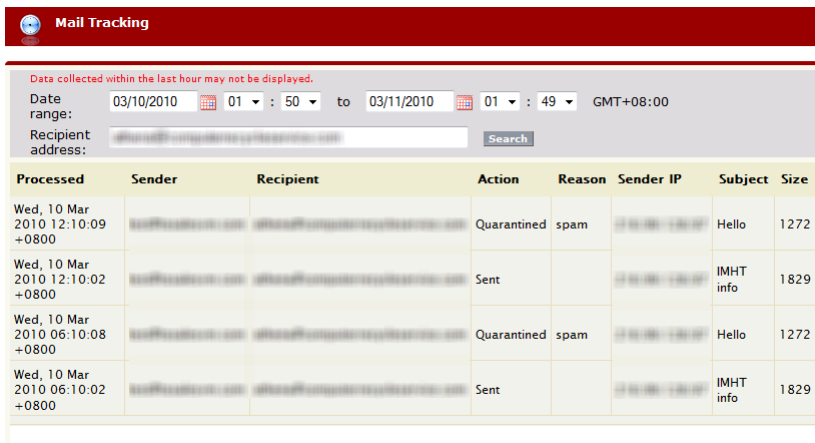
Click the **Home** tab to view summary information.

## Tracking Messages

Use mail tracking to determine the status of messages sent to particular recipients. Mail tracking displays the following information about the messages:

- Date and time the message was processed
- Sender email address and IP address of the source server
- Action performed on the message, if it has been quarantined, deleted, or delivered
- Reason why an action was performed on the message, which filters matched
- Subject and size of the message

**Click path:** ... > **Mail Tracking**



The screenshot shows the 'Mail Tracking' interface. At the top, there is a red header with the 'Mail Tracking' title. Below the header, a message reads 'Data collected within the last hour may not be displayed.' The date range is set to '03/10/2010 01:50 to 03/11/2010 01:49 GMT+08:00'. A search box for the recipient address is present. The main content is a table with the following data:

Processed	Sender	Recipient	Action	Reason	Sender IP	Subject	Size
Wed, 10 Mar 2010 12:10:09 +0800	[redacted]	[redacted]	Quarantined	spam	[redacted]	Hello	1272
Wed, 10 Mar 2010 12:10:02 +0800	[redacted]	[redacted]	Sent		[redacted]	IMHT info	1829
Wed, 10 Mar 2010 06:10:08 +0800	[redacted]	[redacted]	Quarantined	spam	[redacted]	Hello	1272
Wed, 10 Mar 2010 06:10:02 +0800	[redacted]	[redacted]	Sent		[redacted]	IMHT info	1829

**FIGURE 6-2.** Mail Tracking tab



**Considerations:**

- You can track only the messages sent to email addresses in the domains that you manage.
- Secure Messaging Service provides mail tracking information from 1 hour to 30 days ago. Message tracking information is discarded after 30 days.
- You can retrieve only up to 24 hours worth of tracked messages at a time. The specified date range cannot cover more than 24 hours.

**To track messages:**

1. Click the **Mail Tracking** tab.
2. Specify a date range.

---

**Note:** The date range cannot cover more than 24 hours.

---

3. Type a specific recipient email address.
4. Click **Search**.

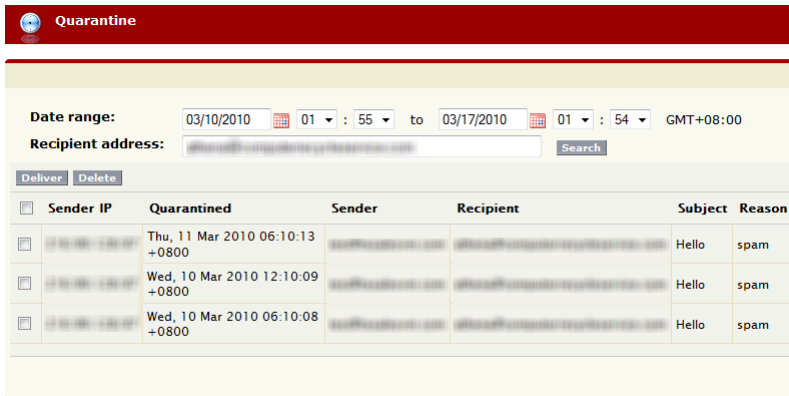
## Viewing Quarantined Messages

Review quarantined messages to understand the types of unwanted messages a domain receives and to assess filter settings. You can view the following information about quarantined messages:

- Date and time the message was processed
- Sender email address and IP address of the source server
- Recipient address
- Reason why the message was quarantined, which filters matched
- Subject and size of the message

You can choose to delete or deliver quarantined messages.

**Click path: ... > Quarantine**



**FIGURE 6-3. Quarantine tab**

**Considerations:**

- Use *caution* when delivering quarantined messages. Some of these messages may contain links to fraudulent Web sites and other undesirable content.
- The latest quarantine information that can be queried is from before the past hour.
- The oldest quarantine information that can be queried is from 30 days ago. Secure Messaging Service discards quarantined messages and corresponding information after 30 days.
- You can only retrieve up to 7 days worth of quarantine information at a time. The specified date range cannot cover more than 7 days.
- Users can access the End-User Quarantine console to view their quarantined messages. For more information, see [Using the End-User Quarantine](#) on page 7-3.

**To view quarantined messages:**

1. Click the **Quarantine** tab.
2. Specify a date range.

---

**Note:** The date range cannot cover more than 7 days.

---

3. Type a specific recipient email address.
4. Click **Search**.
5. Delete or deliver quarantined messages as necessary.

## Using Reports

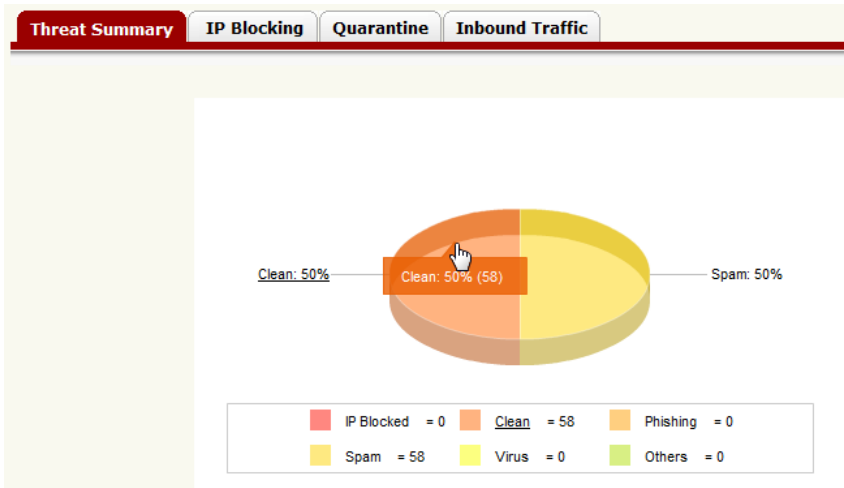
Secure Messaging Service supports multiple report types that can be viewed on the administrative console. These reports give an overview of the number of messages processed by the service and other filtering statistics.

### Report Types

Secure Messaging Service supports the following report types:

- *Threat Summary* on page 6-8
- *IP Blocking* on page 6-9
- *Quarantine* on page 6-10
- *Inbound Traffic* on page 6-11

## Threat Summary



**FIGURE 6-4.** Threat summary report

This chart shows the total number of messages processed and the number of messages that were caught by individual filters. The chart uses the labels below:

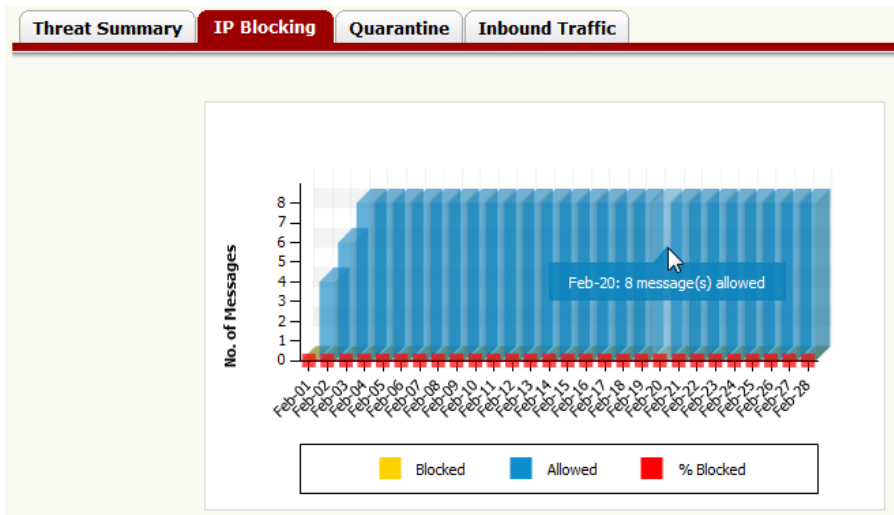
- IP Blocked—messages blocked by Email Reputation Service based on the reputation rating of their source IP address
- Clean—messages that did not match any filter criteria and are considered safe and normal
- Phish—phishing messages detected by the anti-spam filter
- Spam—spam messages detected by the anti-spam filter
- Virus—malware messages detected by the antivirus filter
- Others—messages that matched the attachment and the content filters, those that did *not* match the valid recipient list, and messages that exceeded the system-wide size limit (see *System Limits* on page 4-2)

---

**Note:** For more information on the individual filters, see *Types of Configurable Filters* on page 4-3.

---

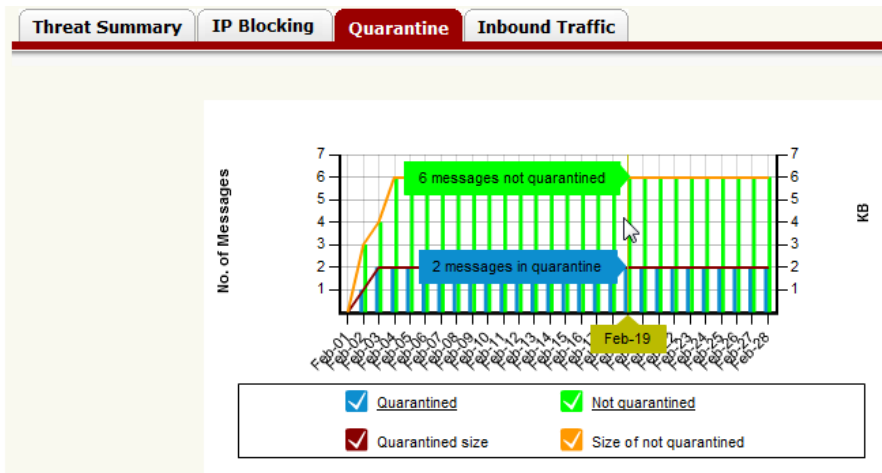
## IP Blocking



**FIGURE 6-5.** IP blocking report

This graph shows the total number of messages that have been blocked using Email Reputation Service and the total number of messages that have been allowed to pass. It also indicates what percentage of the total traffic has been blocked.

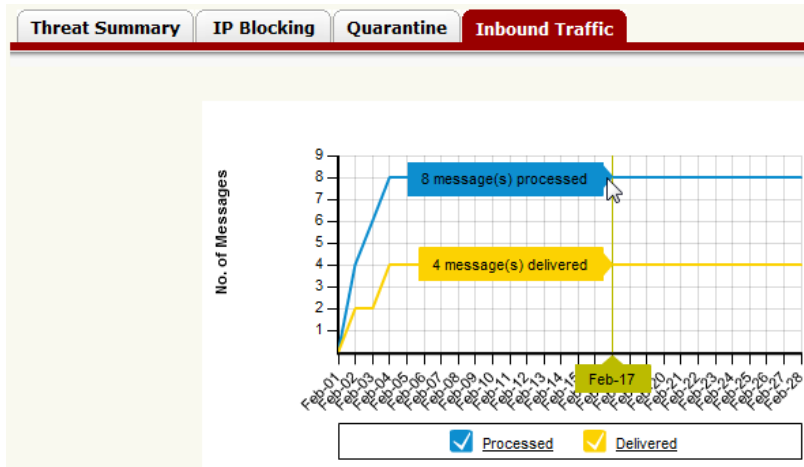
## Quarantine



**FIGURE 6-6. Quarantine report**

This graph shows the total number of messages that were quarantined and the total number of processed messages that were *not* quarantined during the specified period. It also shows the corresponding total size of quarantined messages and messages that were not quarantined.

## Inbound Traffic



**FIGURE 6-7.** Inbound traffic report

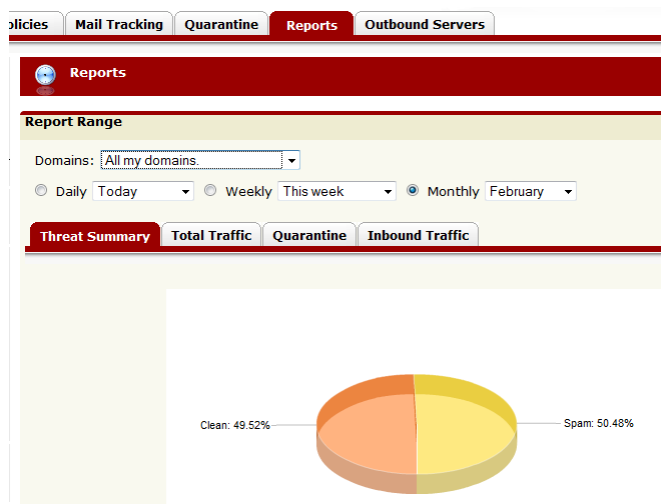
This graph shows the number of inbound messages (incoming messages from other domains) that have been processed and the number of processed messages that have been delivered to their respective recipients.

## Viewing Reports

Reports provide graphical summaries of the following information:

- Threat statistics
- Message blocking based on source IP addresses (Email Reputation Service)
- Quarantined messages
- Inbound traffic

**Click path:** ... > Reports



**FIGURE 6-8.** Reports tab

### Considerations:

- Reports either cover all the domains you manage or specific domains.
- For details about individual reports, see *Report Types* on page 6-7.
- All date and time values are in GMT.

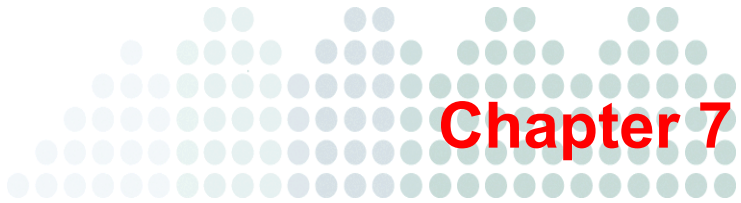
### To view reports:

1. Click the **Reports** tab.
2. Select the coverage of the report.



3. Keep the default selection **All my domains** to generate reports covering all the domains you manage.
4. Select a particular domain to generate reports for that domain.
5. Select the time range. You can choose from the following options:
  - **Daily**—display reports covering a specific day in the past week
  - **Weekly**—display reports covering a specific week in the past month
  - **Monthly**—display reports covering a specific month in the past six months
6. To select the report you want to view, click the corresponding tab.





## End-User Quarantine

The End-User Quarantine console allows email users to view their quarantined messages and configure their own approved list. This chapter describes tasks associated with the End-User Quarantine console in the following topics:

- *[Giving Users Access to Their Quarantined Messages](#)* on page 7-2
- *[Using the End-User Quarantine](#)* on page 7-3

## Giving Users Access to Their Quarantined Messages

Secure Messaging Service provides an End-User Quarantine console to allow email users to view a list of their incoming messages that have been quarantined. Users can do the following in the console:

- Delete or deliver quarantined messages
- Maintain a list of approved senders

### **Considerations:**

- The end-user approved lists take precedence over the blocked list, the Email Reputation Service filter, and the anti-spam filter. All messages from addresses that match the addresses in the approved list are not processed by these filters.
- Activation links for new accounts expire after 48 hours. Email users must sign up again if they are unable to activate within that period.

### **To give users access to the End-User Quarantine console:**

1. Contact your support provider for the correct URL to the console.
2. Provide the URL to the users.
3. Instruct the users to:
  - a. Create an account by clicking **Sign up for an account**.
  - b. During account creation, they need to specify their email account in the domain protected by Secure Messaging Service.
  - c. Wait for the confirmation message sent to their domain email account.
  - a. Click the link on the confirmation message. After they click the link, they are given access to the End-User Quarantine console.

## Using the End-User Quarantine

The End-User Quarantine for Secure Messaging Service provides email recipients:

- Access to quarantined messages and the ability to delete or deliver these messages
- Ability to specify a list of approved senders, whose messages are not checked for spam and phishing

---

**Note:** Messages in quarantine are automatically deleted after 30 days.

---

## Browser Requirements

To properly display all the pages in the End-User Quarantine console, including this help, use one of the following Web browsers:

- Microsoft™ Internet Explorer™ 7 or 8
- Mozilla™ Firefox™ 3.0 or 3.5

---

**Note:** On certain Windows Server™ operating systems, including Windows Server 2003 and 2008, Internet Explorer Enhanced Security Configuration can prevent the console from displaying properly. See [Display Issues on Internet Explorer](#) on page 2-5.

---

## Handling Messages in the End-User Quarantine

Review the quarantine to check whether it contains legitimate messages. The quarantine displays the following information about quarantined messages:

- IP Address—IP address of the mail server that sent the message
- Quarantined—time the message was quarantined
- Sender—email address of the message sender
- Subject—subject of the message
- Reason—why the message was quarantined

You can deliver or delete quarantined messages.

**Click path: ... > Quarantine**

The screenshot shows the 'Quarantine' tab selected. Below it, there are tabs for 'Approved Senders' and 'Profile'. A red banner at the top of the main content area says 'Quarantined Email'. Below this is a date range filter: 'Date range: 03/01/2010 02:25 to 03/08/2010 02:24 GMT+08:00' with a 'Search' button. Below the filter are three buttons: 'Deliver', 'Delete', and 'Approve Sender and Deliver'. A table follows with the following data:

<input type="checkbox"/>	Sender IP	Quarantined v	Sender	Subject	Reason
<input type="checkbox"/>	216.99.128.97	Sun, 07 Mar 2010 12:10:08 +0800	[redacted]	Hello	spam
<input type="checkbox"/>	216.99.128.97	Sun, 07 Mar 2010 06:10:09 +0800	[redacted]	Hello	spam
<input type="checkbox"/>	216.99.128.97	Sat, 06 Mar 2010 12:10:08 +0800	[redacted]	Hello	spam
<input type="checkbox"/>	216.99.128.97	Sat, 06 Mar 2010 06:10:10 +0800	[redacted]	Hello	spam
<input type="checkbox"/>	216.99.128.97	Fri, 05 Mar 2010 12:10:10 +0800	[redacted]	Hello	spam
<input type="checkbox"/>	216.99.128.97	Fri, 05 Mar 2010 06:10:07 +0800	[redacted]	Hello	spam
<input type="checkbox"/>	216.99.128.97	Thu, 04 Mar 2010 12:10:18 +0800	[redacted]	Hello	spam

**FIGURE 7-1. End-User Quarantine query results****Considerations:**

- Use *caution* when delivering quarantined messages. Some of these messages may contain links to fraudulent Web sites and other undesirable content.
- The latest quarantine information that can be queried is from before the past hour.
- The oldest quarantine information that can be queried is from 30 days ago. Messages in quarantine and corresponding information are automatically deleted after 30 days. To ensure that you do not lose any messages, check the quarantine regularly.
- You can only retrieve up to 7 days worth of quarantine information at a time. The specified date range cannot cover more than 7 days.

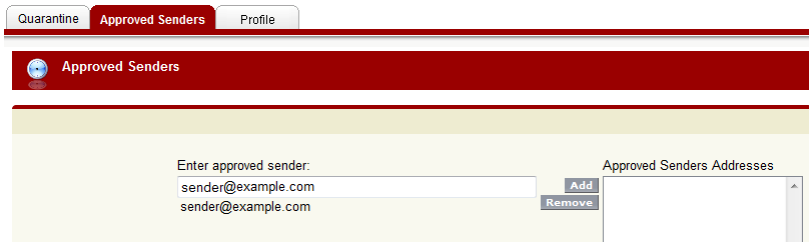
**To delete or deliver quarantined messages:**

1. Click the **Quarantine** tab.
2. Select the quarantined messages you want to delete or deliver.
3. Click **Delete** or **Deliver**. To deliver the messages and approve their senders at the same time, **click Approve Sender and Deliver**.

## Approving Senders in the End-User Quarantine

Secure Messaging Service uses a dynamic scoring mechanism that may tag normal messages with certain characteristics as spam. Use the approved senders list to ensure that messages from specific senders are not filtered as spam or phishing.

**Click path:** ... > **Approved Senders**



**FIGURE 7-2.** Approved Senders tab in the End-User Quarantine console

### **Considerations:**

All messages from addresses that match the addresses in your list will *not* be checked for spam and will bypass certain filters. Use *caution* when approving addresses.

### **To approve senders in the End-User Quarantine console:**

1. Click the **Approved Senders** tab.
2. Under **Email address**, type an email address.
3. Click **Add**.

---

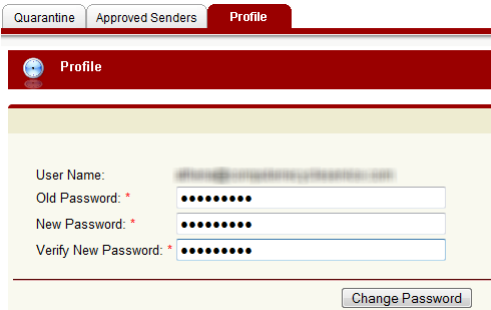
**Note:** To delete an address from the approved list, select the address and click **Remove**.

---

## Modifying Your End-User Quarantine Password

Secure your account by modifying your password regularly.

**Click path:** ... > **Profile**



The screenshot shows the 'Profile' tab in the End-User Quarantine console. The navigation bar at the top has three tabs: 'Quarantine', 'Approved Senders', and 'Profile'. Below the navigation bar is a red header with a profile icon and the word 'Profile'. The main content area is a light yellow box containing a form for changing the password. The form includes fields for 'User Name', 'Old Password', 'New Password', and 'Verify New Password', each with a red asterisk indicating a required field. The 'Old Password' field contains ten black dots. Below the form is a 'Change Password' button.

**FIGURE 7-3.** Profile tab in the End-User Quarantine console

### **Considerations:**

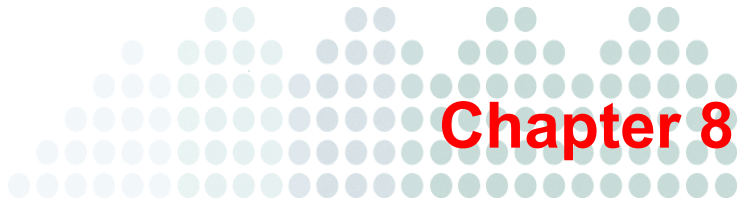
For strong passwords, use:

- More than eight characters
- Use both upper and lower case letters
- Numbers
- Non-alphanumeric characters

### **To modify your End-User Quarantine password:**

1. Click the **Profile** tab.
2. Type your current and your new password.
3. Click **Change Password**.





## Troubleshooting and FAQs

This section provides solutions to common issues and answers to common questions, in the following topics:

- *Troubleshooting* on page 8-2
- *Frequently Asked Questions* on page 8-3

## Troubleshooting

Refer to the following table for information on how to address common issues.

**TABLE 8-1. Common Issues and Solutions**

ISSUE	SOLUTION
Console does not display properly	Check your Web browser. For a list of supported browsers, see <a href="#">Browser Requirements</a> on page 2-5.
Missing messages	To determine the status of missing messages, use the mail tracking feature. See <a href="#">Tracking Messages</a> on page 6-4.
Unable to see messages in quarantine	Spam and phishing messages are quarantined only if you have selected quarantine as the filter action. Check your anti-spam filter settings. See <a href="#">Configuring the Anti-spam Filter</a> on page 5-15.
Unable to find messages in mail tracking	Mail tracking information is only kept for 30 days. Information on messages that are more than 30 days old is not shown in mail tracking. Also, information on messages blocked because they exceed the system-wide limits are not shown in mail tracking. For information on the limits, see <a href="#">System Limits</a> on page 4-2.
Unable to add accounts	You will be unable to create new accounts if you do not have the necessary permissions. Contact your support provider.
Unable to log on to the administrative or the End-User Quarantine console	If you have forgotten your password, use the password reset option. See <a href="#">Resetting Forgotten Passwords</a> on page 2-6.

**TABLE 8-1. Common Issues and Solutions (Continued)**

ISSUE	SOLUTION
Reports show no data	Check the selected domain and time range. See <a href="#">Viewing Reports</a> on page 6-12.
Unable to switch roles	You can only switch to accounts that you manage. You will not be able to switch roles if you do not manage any other accounts.

## Frequently Asked Questions

### What is Trend Micro Secure Messaging Service?

Secure Messaging Service is a managed email security service provided using Trend Micro Email Security Platform for Service Providers. By routing inbound and outbound messages through the service, you can protect domains against spam, phishing, malware, and other messaging threats.

### What are the advantages of a managed email security service?

As a hosted service, Secure Messaging Service allows subscribers to protect domains without having to purchase, install, and maintain an on-premise solution. Subscribers do not have to worry about hardware or software upgrades and maintenance.

### How is privacy protected?

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.

### Why should I trust Trend Micro with email security?

Trend Micro has been a recognized leader in threat management with years of experience in messaging and spam prevention and even longer experience providing leading antivirus solutions. Trend Micro has held considerable market

share as a provider of Internet gateway solutions and the mail server antivirus market.

### **What does one need in order to use this service?**

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

### **How does one begin using the service?**

A simple redirection of a domain's DNS resource records is all that is needed to start the service. The domain's email messages are processed by Secure Messaging Service to filter out spam, viruses, worms, Trojans, and phishing attacks; clean messages are then sent directly to the domain's mail server. For more information, see [Setting Up Email Security](#) on page 2-7.

### **How do I redirect a domain's MX records?**

If you manage the DNS records directly, manually redirect the MX records to point to Secure Messaging Service inbound MTAs. If the DNS records are managed by a third-party or an ISP, either they can do this for you or they may have a simple Web interface allowing you to make the change yourself. For more information, see [Setting Up Email Security](#) starting on page 2-7

### **Can I try the service on a limited number of users?**

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

### **Will messages be delayed as a result of this service?**

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

### **Does the service store or archive messages?**

Secure Messaging Service does not store or archive messages by default. All messages are processed and immediately relayed to your mail server. Messages are not spooled or stored in memory unless your mail server becomes unavailable. However, if you configure Secure Messaging Service to quarantine messages, it will store quarantined messages for up to 30 days.

**What do I do if I lose my password to the console?**

Click **Forgot your password?** on the logon screen to reset your password. After resetting your password, an activation link is sent to your email address. For more information, see [Resetting Forgotten Passwords](#) on page 2-6.

**What happens if the domain's mail server is unavailable?**

If the domain's mail server becomes unavailable, the message stream is automatically queued for up to five days or until such time that the server comes back online.

**Apart from the configurable filters, what other types of filtering are performed by Secure Messaging Service?**

Secure Messaging Service has system-wide filters and performs outbound filtering. See [Understanding Mail Filters](#) on page 4-1.

**Does Secure Messaging Service filter outbound messages?**

Yes. For more information on outbound filtering, see [Outbound Messages](#) on page 4-14.

**Can Secure Messaging Service work with a filtering solution installed inside a network?**

Yes, Secure Messaging Service is provided using Email Security Platform. This platform can serve as a pre-filter, significantly reducing the volume of messages that need to be scanned by an on-premise solution. Contact your support provider about using Email Security Platform as a part of a hybrid email security solution.

**How do I ensure that messages are properly routed and that there are no missing messages?**

Use mail tracking to check whether specific inbound messages have actually been processed. For filtering statistics, you can view reports. For more information, see [Tracking Messages](#) on page 6-4.

**How do I know how many messages are being processed by Secure Messaging Service?**

Secure Messaging Service supports several report types for viewing graphs of filtering statistics. See [Report Types](#) on page 6-7.

### **Can I export reports?**

Secure Messaging Service currently does not support exporting reports. You can view reports only from the console

### **What is the filtering priority? Which filters apply first?**

To understand the filtering order, see *Filtering Flow* on page 4-11.

### **Can multiple filter actions be applied to the same messages?**

Yes, unless a terminal action is encountered, any applicable action is performed. See *Filter Actions* on page 4-9.

### **Does the service check both the attachments and the email body for viruses and other malware?**

Yes, when the antivirus filter is enabled, both the body and attachments of messages are checked for malware code.

### **Can the antivirus filter check for viruses and other malware inside ZIP files or other compressed attachments?**

Yes, the antivirus filter can check inside files packed in common compression formats, including ZIP. It can decompress up to 19 layers of compression.

### **Does the attachment filter check the files inside ZIP files or other compressed attachments?**

No, the attachment filter cannot check files inside compressed attachments.

### **How do I prevent the filters from checking specific attachments?**

To prevent the service, particularly the antivirus filter, from checking specific attachments, compress these attachments, into a ZIP archive for example, and password-protect them. The antivirus filter cannot check password-protected files inside compressed archives. Note, however, that the archive file itself may be screened by the attachment filter.

### **Can I filter messages for particular content?**

The content filter can be used to check the subject and body of messages for unwanted text. With Perl Compatible Regular Expressions (PCRE), you can filter for text patterns. See *Configuring the Content Filter* on page 5-20.

**How does the catch rate work?**

The catch rate reflects sensitivity to spam- or phishing-like characteristics, such as certain phrases or links. A high catch rate has a higher chance of catching actual spam or phishing messages, but it also has a higher chance of filtering normal messages. For more information, see [Spam and Phishing Catch Rates](#) on page 5-18.

**Does the service check for malicious URLs in messages?**

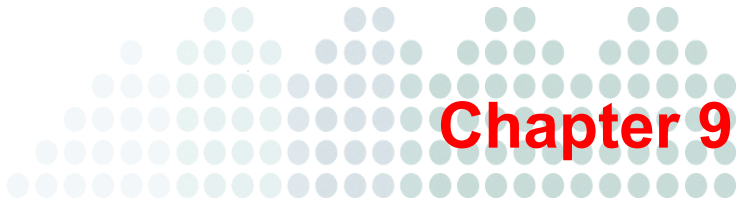
Yes, when you have the phishing option enabled in the anti-spam filter, the service checks messages for URLs associated with fraud and spam and those known to spread viruses and other malware.

**Can I access blocked outbound messages?**

No, blocked outbound messages are automatically deleted. For more information on outbound filtering, see [Outbound Messages](#) on page 4-14.







## Technical Support

This chapter provides information about getting technical support and about useful resources in the following topics:

- *Contacting Technical Support* on page 9-2
- *Knowledge Base* on page 9-2
- *TrendWatch* on page 9-3
- *Submission Wizard* on page 9-3
- *Free Scans with HouseCall* on page 9-3

## Contacting Technical Support

Contact your Trend Micro support representative for help. For contact information, click the support link on the administrative console or visit:

<http://esupport.trendmicro.com/enterprise/default.aspx>

## Knowledge Base

The Trend Micro Knowledge Base is an 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 lets you submit your question through email.

## TrendWatch

Comprehensive security information is available for free on the TrendWatch Web site:

<http://us.trendmicro.com/us/trendwatch/>

Visit TrendWatch to stay aware of threat activity, read security advisories and related news, and find free tools and other resources.

## Submission Wizard

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:

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

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

[virusresponse@trendmicro.com](mailto:virusresponse@trendmicro.com)

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

(877) TRENDAY, or 877-873-6328

## Free Scans with HouseCall

To quickly scan and clean your computer of viruses and other malware, use HouseCall™. Download it for free from:

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



# Index

## A

- Λ records 5-5—5-6
- account details 3-6
- account list, exporting 3-11
- account name 2-2, 3-6
- account types 3-2, 3-9—3-10
  - custom 3-9
  - inheriting 3-7
  - standard 3-9
- accounts 3-1, 3-3
  - creating or modifying 3-10
  - switching 2-9
- action 1-7
- activation link 2-6, 3-3
- adding accounts 8-2
- administrative console 1-3, 1-6
  - browser requirements 2-5
  - logging on 2-5
  - reset password 2-6
  - URL 2-2
- advantages 8-3
- aggressive catch rate 1-6
- alphanumeric characters 5-24
- alphanumeric text 5-23
- anti-spam filter 1-6, 1-9, 4-3, 4-5, 4-8—4-9, 4-13—4-14, 5-4, 5-10—5-11, 5-15—5-16, 5-18, 7-2
- anti-spam rules 5-16—5-17
- antivirus 1-4, 4-4

- antivirus filter 4-3, 4-13—4-14, 5-4, 5-13
  - notifications 5-14
- antivirus notifications 1-5, 5-13—5-14
  - custom message 5-14
  - default message 5-14
- API key 3-2, 3-6
- approved senders 1-3, 1-6, 2-10, 4-3, 5-4, 5-10—5-11
- ASCII characters 5-23, 5-26
- attachment count 4-4, 4-6, 5-30
- attachment filter 1-4, 1-9, 4-3—4-4, 4-6, 4-9, 4-13, 5-4, 5-27, 6-8
- attachment filter rule 5-28

## B

- banking sites 4-8
- benefits 1-3
- blocked list 7-2
- blocked senders 1-3, 1-6, 2-10, 4-3, 5-4, 5-10—5-11
- bulk mail 1-9

## C

- case sensitivity 5-23, 5-26
- catch rate 1-6, 4-5, 4-8, 4-14, 5-18, 8-7
  - selection 5-20
- change recipient 4-10, 4-13
- child account 1-9, 3-3
- clean 6-8
- compressed attachments 8-6
- compressed attachments, limits to 4-2
- compression layers, limits to 4-2

- configurable filters 4-1, 4-3, 8-5
- confirmation message 7-2
- content filter 1-9, 4-5, 4-9, 5-4, 5-20—5-21, 6-8
- content filter rules 5-22
- content filtering 1-4—1-6
- criteria 1-8
- CSV 3-11, 5-9—5-11
- custom account types 3-9

## D

- daily 6-13
- dashboard 6-2—6-4
- delete message 4-9, 4-13
- delete quarantined messages 7-3—7-4
- deliver quarantined messages 7-3—7-4
- destination servers 1-7, 2-4, 5-2, 5-4—5-5
- directory harvest attack (DHA) 1-3
- DNS 5-5—5-6
- DNS resolver cache 2-7
- DNS resource records 8-4
- document
  - audience ix
  - contents viii
  - conventions ix
- domain 2-4, 5-2—5-4
- domain name 2-2
- double-byte characters 5-23, 5-26
- dynamic reputation database 4-3, 4-7, 5-12

## E

- East Asian characters 5-23, 5-26
- email account 2-6
- email address 2-6, 3-2—3-3, 3-6, 3-10
- Email Reputation Service 1-3, 1-6—1-7, 4-3, 4-6, 5-4, 5-10—5-12, 6-8—6-9, 6-12, 7-2
  - advanced 4-3, 4-6—4-7, 5-12
  - standard 4-3, 4-6—4-7, 5-12
- Email Security Platform 1-2
- eml attachments 5-29

- enabled accounts 3-6
- end users 1-3
- end-user approved list 7-2, 7-5
- end-user approved senders 7-2—7-3
- End-User Quarantine (EUQ) 6-6, 7-2—7-3
  - browser requirements 7-3
  - console 1-3, 1-7, 2-2, 7-1
  - password 7-6
  - reset password 2-6
- Enhanced Security Configuration 2-6
- error code 550 2-7
- ERS 4-3, 5-10, 5-12
- exact matches 2-10
- exception list 5-18, 5-29
- exceptions 5-20, 5-22
- extension name 4-4, 4-6, 5-30—5-31

## F

- fake Web sites 5-19
- false spam/phishing detection 1-6, 5-19, 8-7
- FAQs 8-3, 9-2
- features 1-3
- filter 1-7
- filter actions 1-7, 1-9, 4-4, 4-9, 4-13, 5-16—5-18, 5-20, 5-27, 8-6
- filter criteria 1-8—1-9, 4-4, 5-16, 5-18, 5-20, 5-27—5-28
- filter rule 5-21, 5-28
- filter types 4-3
- filtering flow 4-11, 4-13
  - inbound messages 4-12
- filtering priority 8-6
- Firefox 2-5
- firewall 2-4
- footer 5-29
- forgotten passwords 8-2, 8-5
- FQDN 2-4, 2-7, 5-5
- fraud 8-7

fraud prevention 1-4  
frequently asked questions 8-3

## G

global policy 4-14  
glossary 1-6

## H

heuristic identification 4-7  
HouseCall 9-3  
hybrid email security 8-5

## I

import mode 5-11  
import recipient addresses 5-9  
import sender addresses 5-11  
inbound filtering 2-7  
inbound messages 1-8, 2-7, 4-1, 4-3–4-4, 8-5  
inbound MTA 2-4, 2-7  
inbound traffic 6-12  
inbound traffic report 6-11  
individual size 4-4, 4-6, 5-30  
infected messages 5-14  
    date and time sent 5-14  
    original recipients 5-14  
    senders 5-14  
    subject 5-14  
inherit 3-7  
insert footer text 4-11, 5-29  
Internet Explorer 2-5  
    display issues 2-5, 7-3  
    Enhanced Security Configuration 2-5–2-6, 7-3  
    Trusted sites zone 2-5  
IP address 2-4–2-5, 2-7, 6-8  
IP address blocking 6-9  
IP addresses 5-5, 5-8  
IP blocking 6-8, 6-12  
IP blocking report 6-9

## K

Knowledge Base 9-2

## L

LDIF 5-9–5-10  
license key 3-2, 3-8  
licensing 3-2, 3-8  
link safety 5-19  
local-part 1-8, 5-9, 5-11, 5-18, 5-22, 5-29  
logo 3-3–3-5  
login page 3-4–3-5

## M

Mail 1-8  
mail tracking 6-1, 6-4, 8-2  
mail tracking range 6-5  
mail transfer agent (MTA) 2-3  
malicious code 1-4  
malicious URLs 8-7  
malware 1-4, 1-8, 4-4, 4-7, 5-13, 6-2, 8-7  
malware sites 5-19  
managing another account 2-9  
message body 1-4, 4-5, 5-23  
message limits 4-1  
message size, limits to 4-2  
message storage 8-4  
missing messages 8-2  
monthly 6-13  
MTA 2-4–2-5, 8-4  
MX records 2-4, 2-7, 5-5, 5-7, 8-4

## N

new features 1-5  
news and announcements 6-3  
non-terminal actions 4-12  
notification tokens 5-14  
notifications 1-5

**O**

- online help x
- online payment facilities 4-8
- outbound 1-8
- outbound filtering 2-7, 4-14, 8-5, 8-7
- outbound messages 2-7, 4-4, 8-5, 8-7
- outbound MTA 2-4—2-5, 2-8
- outbound server IP address list 2-8
- outbound servers 2-7—2-8
- Outlook™ Express 5-29

**P**

- parent account 1-9, 3-3
- password 2-6, 3-2, 3-5—3-6, 3-10
- password-protected files 8-6
- Perl Compatible Regular Expressions (PCRE) 1-4, 5-24, 5-27
- permissions 3-9
- phish 6-8
- phishing 1-4, 1-9, 4-3, 4-5, 4-8, 5-16—5-18, 6-2, 7-3, 7-5, 8-2, 8-4, 8-7
  - catch rate 5-19
  - detection 5-19
  - sensitivity 1-6, 5-18
- phishing sites 5-19
- policies 2-7, 2-10, 5-1
  - creating 5-4
  - creation 5-4
  - overview 5-2
- potentially malicious sites 5-19
- preference 5-5
- pre-filter 8-5
- privacy 8-3
- profile 3-2, 3-5, 7-6
  - modifying 3-2
- public proxy servers 4-7

**Q**

- quarantine 1-9, 4-9, 4-13, 6-1, 6-5—6-6, 7-3, 8-2
  - approve a sender 7-4
  - date 7-3
  - deliver message 7-4
  - IP address 7-3
  - reason 7-3
  - sender 7-3
  - subject 7-3
- quarantine range 6-6
- quarantine report 6-10
- quarantined messages 1-3, 6-12

**R**

- rebranded URL 3-4
- rebranding 3-2—3-3, 3-10
- recipient count, limits to 4-2
- recipient filtering 1-3
- registration 3-2, 3-8
- regular expressions 1-6, 4-5, 5-21, 5-23—5-24
  - special characters 5-24
  - syntax 5-26
- relay MTA 2-4
- relay outgoing messages 2-8
- replace attachment with text 4-10, 5-29
- report types 6-7, 8-5
- reports 1-5, 6-1, 6-12, 8-3, 8-6
- reputation database 4-3, 4-7, 5-12
- required information 2-2
- required knowledge P-ix
- response code 4-2, 4-12
- roles 8-3
- rules 1-9, 4-9, 5-18, 5-20—5-21, 5-27—5-28

**S**

- search function 2-10
- search, timeouts during 2-10
- seat count 3-6



sender filtering 1-3  
service inbound MTA 2-7  
service outbound MTA 2-8  
service overview 1-2  
service relay MTA 2-7  
setting up 2-7  
sibling accounts 1-9, 3-5  
    managing 3-7  
signature identification 4-7  
source reputation 1-3  
spam 1-4, 1-9, 2-8, 4-3, 4-5, 4-7—4-8, 5-16—5-18,  
    6-2, 6-8, 7-2—7-3, 7-5, 8-2, 8-4, 8-7  
    catch rate 5-19  
    sensitivity 1-6, 5-18  
spam sites 5-19  
special characters 5-24  
spyware 1-4  
standard account types 3-9  
statistics 6-7  
strong passwords 7-6  
subdomain 2-4, 5-7  
subject 1-4, 4-5, 5-23  
Submission Wizard 9-3  
subscriber 1-10  
support link 3-4  
support URL 3-5  
switching accounts 2-9, 3-11  
switching roles 8-3  
system limits 4-2  
system maintenance 6-3  
system-wide limits 8-2

**T**

tag subject 4-11, 5-29  
technical support 9-1  
temporary password 2-2  
terminal action 1-10, 4-9, 4-13  
text patterns 1-4

threat statistics 6-12  
threat summary report 6-8  
time-to-live 2-7  
total size 4-4, 4-6, 5-30  
tracking 1-5  
TrendWatch 9-3  
Trojans 1-4, 1-8, 4-7, 8-4  
troubleshooting 8-2

## U

user name 2-6

## V

valid recipient list 6-8  
valid recipients 1-3, 1-10, 2-10, 4-3, 5-4, 5-8—5-10  
viruses 1-8, 4-7, 6-8, 8-4, 8-7  
volume 1-5  
vulnerabilities 4-7

## W

Web browser 2-5  
weekly reports 6-13  
wildcards 5-11  
Windows Server 2-5—2-6, 7-3  
worms 1-4, 1-8, 4-7, 8-4

## X

xsp\_anti\_spam 3-9  
xsp\_mailtracking 3-9  
xsp\_reseller 3-9  
xsp\_standard 3-9  
xsp\_support 3-9  
xsp\_view\_policy 3-9

## Y

your account 3-2

## Z

ZIP files 8-6

