

SonicWALL® Email Security

User Guide

Version 4.6



SonicWALL, Inc. reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme file and the Getting Started Guide.

Trademarks: SonicWALL, the SonicWALL logo, SonicWALL Email Security, SonicWALL Self Monitoring Active Response Team (SMART) Network, MailFrontier, the MailFrontier logo, and MailFrontier Gateway, MailFrontier Gateway Server™, Enterprise Edition, and MailFrontier Self Monitoring Active Response Team (SMART) Network are trademarks or registered trademarks of SonicWALL, Inc. All other product or company names may be trademarks or registered trademarks of their owners.

Release date: Tuesday, April 18, 2006

Version: 4.6

Copyright © 2005-2006 SonicWALL, Inc.

SonicWALL, Inc.
1143 Borregas Ave.
Sunnyvale, CA 94089
Phone: +1.408.745.9600
Fax: +1.408.745.9300
<http://www.sonicwall.com>

Preface

SonicWALL Email Security guards the perimeter of the organization against the costly, dangerous, and growing threats to corporate email. Threats are stopped before they infiltrate corporate mail servers and employee inboxes. SonicWALL Email Security secures email connections and blocks unwanted email while ensuring timely delivery of all legitimate email. SonicWALL Email Security provides the most comprehensive and effective spam blocking available. The solution filters email uniquely for each user, taking into accounts the varying preferences and patterns of each user.

SonicWALL's solution is dynamic, self-learning, and self-running. SonicWALL Email Security provides protection against all forms of email threats from entering your Inbox.

NOTE: SonicWALL Email Security might display the following branding in screen images: SonicWALL Gateway Server™, Enterprise Edition, SonicWALL Gateway Server™, Small Business Edition, SonicWALL Appliance, SonicWALL Gateway Server™, Enterprise Edition, SonicWALL Gateway Server™, Small Business Edition, and SonicWALL Appliance. The spam-preventing functionality is identical in all of the above product names.

Documentation Overview

SonicWALL provides documents to install, administer, and use its products to protect email users from phishing, spam, viruses; and manage your security policies for your organization.

Who Should Read this?	Document Name	Where to Find Information
Users, Administrators, and Product Evaluators	FAQ	http://www.mailfrontier.com/support_asg_faq.html
	White papers	http://www.mailfrontier.com/press_resources.html
Network and System Administrators	<i>SonicWALL Email Security Administrator Guide</i>	http://www.mailfrontier.com/support_overview.jsp
Email Users	<i>SonicWALL Email Security User Guide</i> <i>Two-page User's Quick Start Pamphlet</i>	http://www.mailfrontier.com/support_overview.jsp User_Quick_Start.

Note: To download SonicWALL's manuals, you must have a MailFrontier user ID and password.

Documentation Conventions

Font	Meaning
Bold	Terms you see in a SonicWALL Email Security window
<i>Italic</i>	Variable names
Courier	Text on a command line
Bold Courier	Text that you type in a command line

Finding Online Help



Clicking the **Help** button describes how to use the contents of the window.

IMPORTANT: Configure your web browser's pop-up blockers to allow pop-ups from your organization's SonicWALL Email Security server before using SonicWALL Email Security, because many of the windows are pop-up windows.

Table of Contents

Documentation Overview	iv
Documentation Conventions	iv
Finding Online Help.....	iv
ABOUT MAILFRONTIER GATEWAY	1
Types of Email Protection	2
Categories of Email	2
When A Message is Flagged as Junk	3
Deleting Spam.....	3
LOGGING IN TO YOUR JUNK BOX	4
Searching in Your Junk Box	6
Detailed Search Mode	7
Deleting Messages.....	8
Unjunking Messages	8
Viewing Message Content.....	8
Ending Your Junk Box Session	9
ANTI-SPAM TECHNIQUES	10
MANAGING ALLOWED AND BLOCKED LISTS	10
Adding People to the Allowed or Blocked Lists.....	11
Deleting People from the Allowed or Blocked Lists	12
Adding Companies or Domains to the Allowed or Blocked Lists	13
Adding a Company or Domain to the Allowed List	15
Deleting a Company or Domain.....	15
To delete a company or domain:	15
Adding Lists to the Allowed List.....	15
Screening Messages in Other Languages	17

Configuring Language Preferences for MailFrontier Gateway	18
Configuring Language Preferences for your Junk Box Summary	20
CONFIGURING RULES AND COLLABORATIVE SETTINGS.....	20
Configuring Collaborative Settings	21
Configuring Aggressiveness Settings	21
Determining Amounts and Flavors of Spam.....	22
SETTINGS.....	23
Spam Management.....	24
Assigning Delegates for the Junk Box	24
Removing a Delegate	25
Junk Box Summary	25
Send Simple (no graphics) Summary or Graphical Summary	27
REPORTS	29
Selecting Reports	29
Messages Processed.....	30
Methods of Identifying Email.....	31
INDEX	32

CHAPTER

1

About SonicWALL Email Security

SonicWALL Email Security™ manages email messages for the organization to ensure that each user gets the email they want (good mail) and do not receive spam and other unwanted email. SonicWALL Email Security is similar to a network security system in that it places multiple defenses in combination. SonicWALL Email Security resides on the outer edge of the organization network and processes email as it enters the organization mail infrastructure. Figure 1 illustrates how email enters the corporate network.

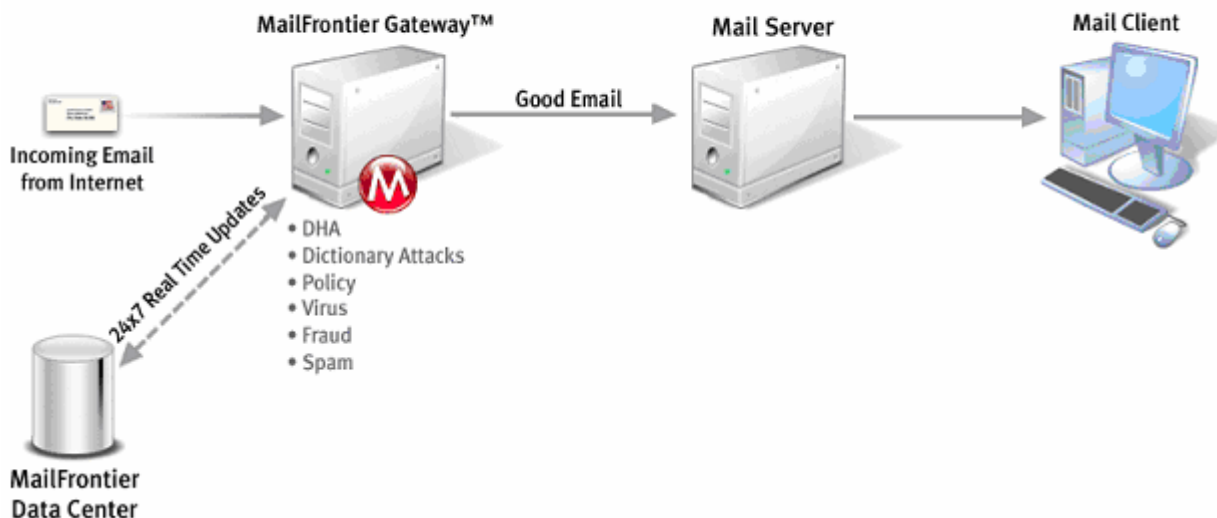


Figure 1 SonicWALL Email Security

SonicWALL Email Security uses multi-prong approaches to prevent junk email. As spammers become resilient to blocking methods, new technologies are required to defeat spam messengers. SonicWALL Email Security uses an adaptive plug-in architecture to easily support the addition of new junk-blocking technology.

SonicWALL Email Security uses several spam-blocking methodologies including:

- Dynamically created allowed lists
- Wide-ranging blocked lists
- Intelligent content filtering and rule checking
- Collaborative community blocking

Types of Email Protection

SonicWALL Email Security protects your organization against the following types of unwanted email:

- Spam and messages that likely contain spam
- Viruses and messages that likely contain viruses
- Phishing messages and messages that are likely to contain fraudulent content
- Policy Management¹
- Directory Harvest Attack (DHA), which is a technique spammers use to collect a list of all of the users in your organization's directory

Depending on how your network administrator configures your organization network, you might have one or more of these types of email protection. Your network administrator can explain what modules are in effect.

Categories of Email

Email can be classified into three categories. SonicWALL Email Security determines the destination for each category based on a proprietary content-filtering technology:

Sender Category	SonicWALL Email Security Action
Allowed	SonicWALL Email Security passes through email from senders whose addresses are on your Allowed list (sometimes known as <i>whitelists</i>) of people, companies, and lists, which are sent to you. Typically, people that you communicate with regularly and are in your address book are allow-listed. In addition to your own list of allowed senders, your IT department might also set up an organizational Allowed list.
Blocked	SonicWALL Email Security blocks email from individual email addresses and domains that are known to send junk email. These addresses are placed on a <i>blocked list</i> of perpetually blocked email addresses and domains. When you mark a message as junk, the sender is blocked from emailing you again.
Unknown	SonicWALL Email Security evaluates email from senders that are not on the list of either allowed or blocked emails. Messages from unknown senders evaluated using a variety of techniques for recognizing spam-like messages, including analysis of both the header (envelope) of the message as well as subject line and content.

¹ Policy Management manages incoming message content and headers for the organization. For example, some organizations might want to capture email with its trademarked product names for sales leads.

When A Message is Flagged as Junk

When SonicWALL Email Security determines a message is junk, it stores it in a Junk Box. Your network administrator determines whether users can access their Junk Boxes. If configured, the software periodically sends you email messages listing the messages flagged as junk email.

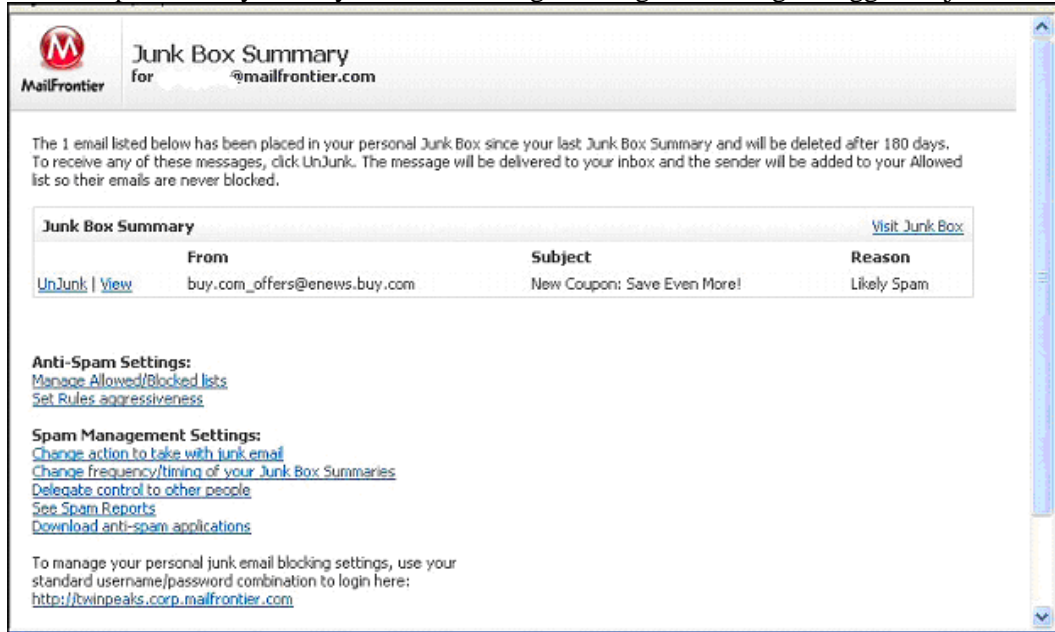


Figure 2 Junk Box Summary

You can scan these messages to see if there are any messages you want to receive, which were miscategorized as Junk. If you see a message you want to receive, click the **Unjunk** link next to it and the message is sent to your Inbox. The sender of any messages that you unjunk is added to your list of allowed senders and their messages are not marked as junk in the future.

Depending on the settings for your organization's installation of SonicWALL Email Security, you might also have a **View** link in the Junk Box summary message. Click the link to view the contents of the message to assist in determining whether it is spam.

Deleting Spam

If you do not care about the messages in the Junk Box, you can leave them there. They are automatically deleted later.

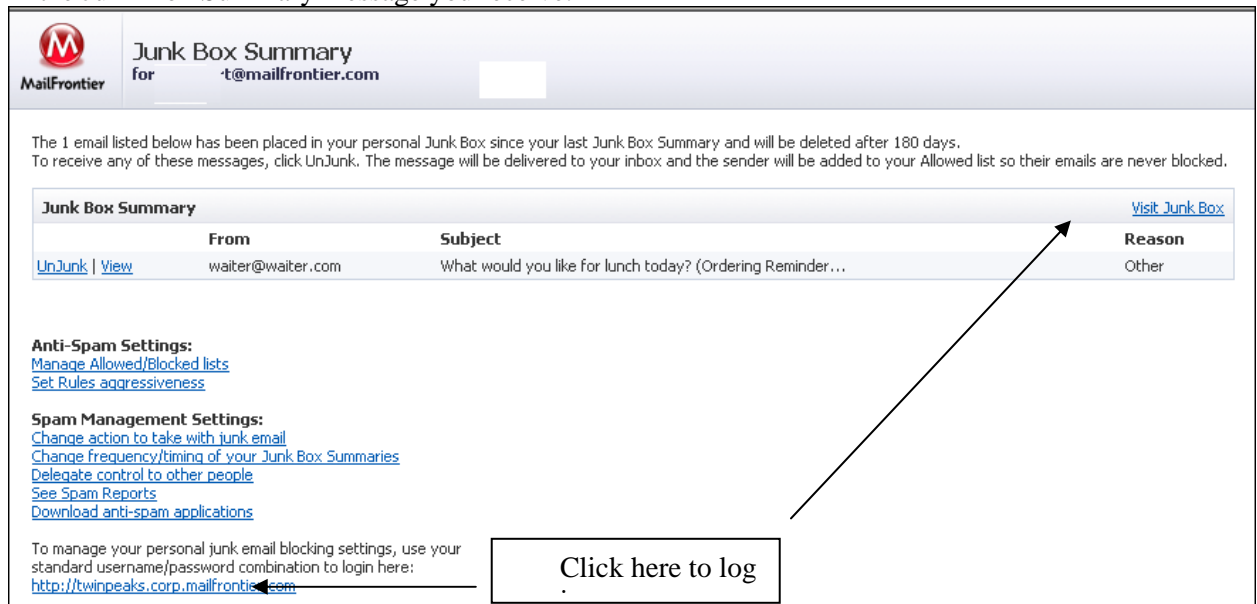
CHAPTER

2



Logging In to Your Junk Box

When SonicWALL Email Security determines that a message contains a threat or a likely threat, it stores the message in a Junk Box on the server and alerts you by email, as shown in Figure 3. You can log in to your Junk Box to view messages that were junked by SonicWALL Email Security. Log in to SonicWALL Email Security using the link that your IT administrator gave you or by clicking the link in the Junk Box Summary message you receive.

A screenshot of an email interface titled "Junk Box Summary" for "MailFrontier". The email body contains a table with one row of junked messages. A box labeled "Click here to log" has an arrow pointing to the "Visit Junk Box" link in the table's header row.

Junk Box Summary			Visit Junk Box
From	Subject		Reason
UnJunk View	waiter@waiter.com	What would you like for lunch today? (Ordering Reminder...	Other

Anti-Spam Settings:
[Manage Allowed/Blocked lists](#)
[Set Rules aggressiveness](#)

Spam Management Settings:
[Change action to take with junk email](#)
[Change frequency/timing of your Junk Box Summaries](#)
[Delegate control to other people](#)
[See Spam Reports](#)
[Download anti-spam applications](#)

To manage your personal junk email blocking settings, use your standard username/password combination to login here:
<http://twinpeaks.corp.mailfrontier.com>

Click here to log

Figure 3. Login Link

IMPORTANT: Configure your web browser's pop-up blockers to allow pop-ups from your organization's SonicWALL Email Security server before using SonicWALL Email Security, because many of the windows are pop-up windows.

To log in to your Junk Box:

1. Log in with your user name and password.
The Login Window is shown in Figure 4.



Figure 4 Login Window

2. Choose the appropriate domain from the list, if necessary.

Your personal Junk Box appears, with any messages that have been flagged as spam or other unwanted email, as shown in Figure 5.

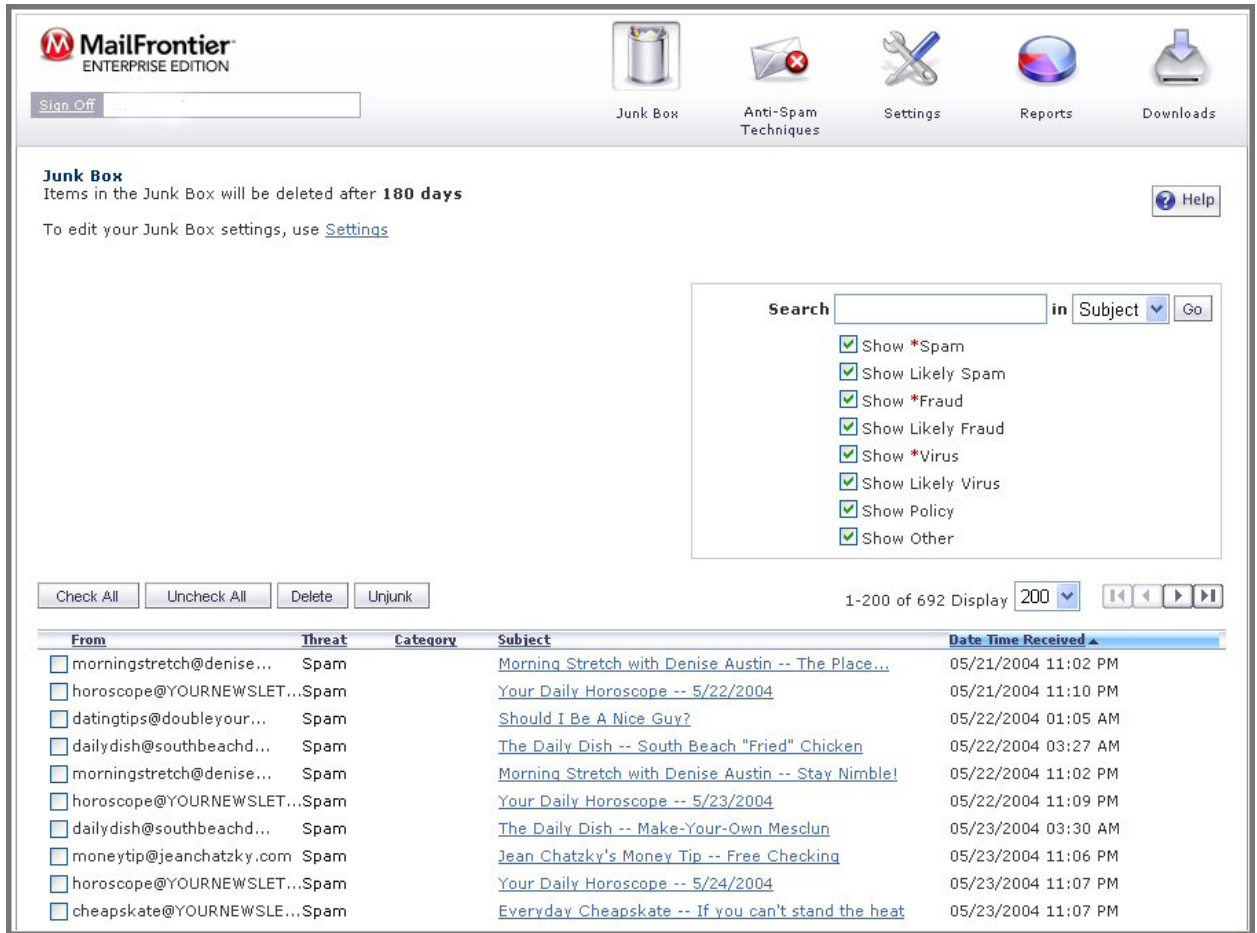
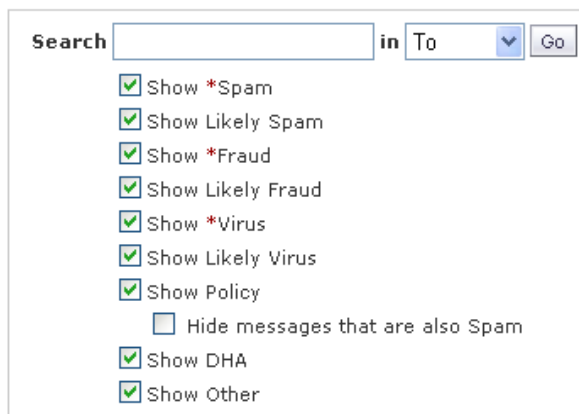


Figure 5 Junk Box window

You can display all junk mail, likely junk mail, or other unwanted email if your organization has configured SonicWALL Email Security to screen for viruses, phishing, or email that contains content you're your organization has chosen to manage through policies.



Searching in Your Junk Box

To search for email messages in your Junk Box:

1. Enter a word or partial word in the **Search** text box.
Note: Search is not case-sensitive.
2. Select the field you want to search in (Subject, From, or Date).
Date formats can be entered as MM/DD/YY or MM/DD/YYYY.
3. Click **Go**.

To search for specific email threats, check or deselect check boxes under the Search text box and click **Go**. As an example, suppose you wanted to see only messages that were Spam or Likely Spam. To do this, select the **Show *Spam** and **Show Likely Spam** check boxes, deselect all other check boxes and click **Go**.

Detailed Search Mode

When the Junk Box has more many messages than it can display, a **Detailed Search Mode** pane appears. It allows you to filter the messages by a date range or addresses and display a manageable subset.

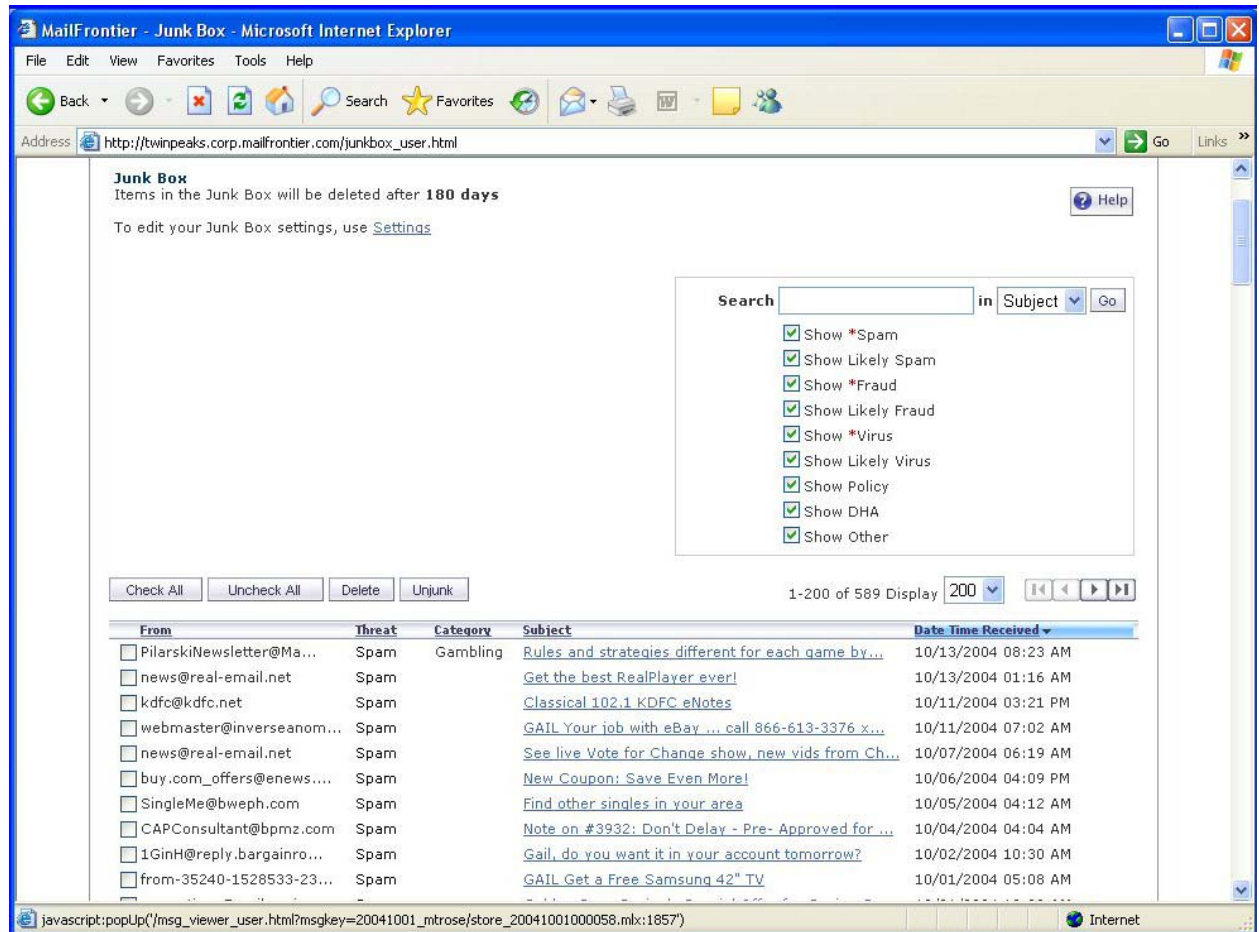


Figure 6. Detailed Search Mode

Deleting Messages

To delete individual messages:

1. Select a message.
2. Click **Delete**.

To delete all messages:

1. Click **Check All**.
2. Click **Delete**.

If you do nothing, these messages are automatically deleted after the number of days configured by the SonicWALL Email Security administrator.

Unjunking Messages

To unjunk a message:

Click the box to the left of the message to select the message you want to retrieve.

Click **Unjunk**.

The senders of any messages you unjunk are added to your list of allowed senders; future messages from these senders are delivered directly to your Inbox.

To unjunk all messages:

1. Click **Check All**.
2. Click **Unjunk**.

Viewing Message Content

Depending on your organization's configuration, you can view the message content by clicking the **View** link in the Junk Summary Message. For security reasons, SonicWALL Email Security displays only the text portions of the message and does not display graphical images.

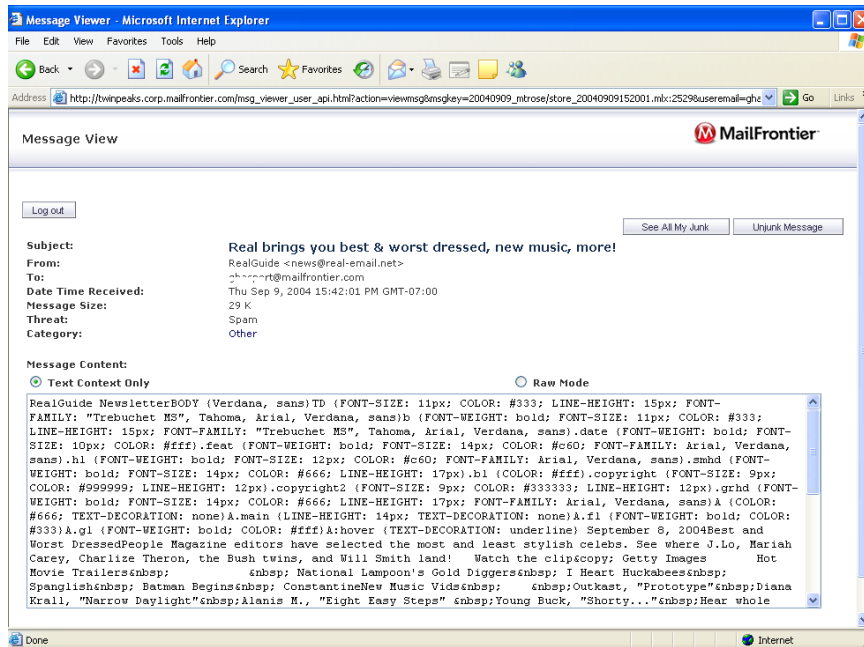


Figure 7. Viewing the Message

To view the header information, click the **Raw Mode** option.

Ending Your Junk Box Session

When you are done managing your Junk Box, click the **Sign Off** button in the upper left corner of the screen or close the browser window.



Figure 8 Signing Off

CHAPTER

3



Anti-Spam Techniques

This chapter provides information on the following topics:

[Managing Allowed and Blocked Lists](#)

[Configuring Rules and Collaborative Settings](#)

[Screening for Spam in Other Languages](#)

Managing Allowed and Blocked Lists

Use the Anti-Spam Techniques window to create your own lists of senders from whom you want to allow and block email. SonicWALL Email Security provides separate lists for people, companies (domains), and mailing lists. For each type of list, click the **Allowed** and **Blocked** tabs to see the different allowed and blocked lists.

You can search for allowed and blocked names, company, and lists in the Anti-Spam Techniques window. Click **Search** and type the name of the person, company, or list.

Note: An email address or domain cannot be simultaneously on the Allowed and Blocked lists. If you add an address in one list that already exists on the other, SonicWALL Email Security removes the address from the first list.

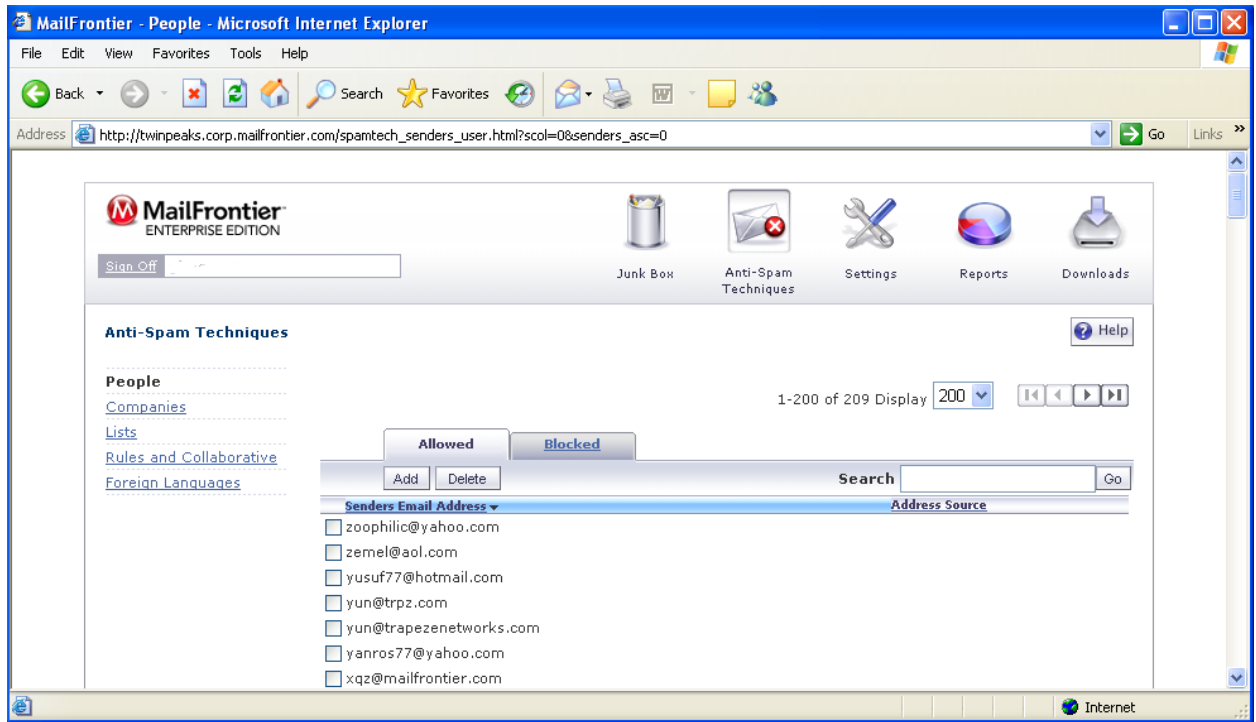


Figure 10 Anti-Spam Techniques

Adding People to the Allowed or Blocked Lists

To add people to **Allowed** or **Blocked** lists:

Click the **Anti-Spam Techniques** button. The window in Figure 10 appears.

1. Click **Allowed** to add people to the **Allowed** list.

2. Click **Add** to add a person.

The **Add People to Allowed List** dialog appears.

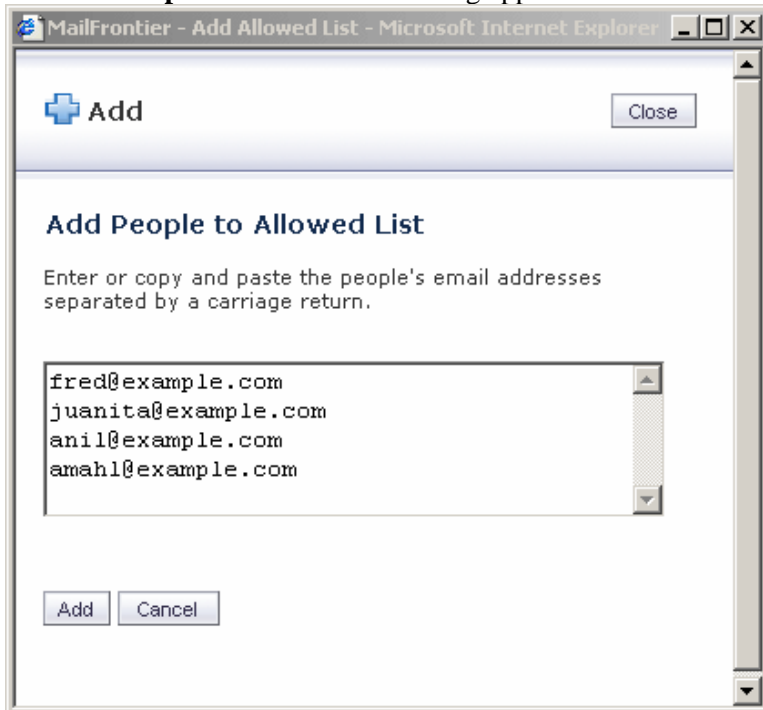


Figure 11 Add People to Allowed List

2. Enter the email address of the address you want to remove.
If you remove multiple people, press **Enter** after each one.
3. Click **Add**.

Deleting People from the Allowed or Blocked Lists

To delete people from **Allowed** or **Blocked** lists:

1. Click the **Anti-Spam Techniques** button.

The **Anti-Spam Techniques** window appears, as shown in Figure 12.

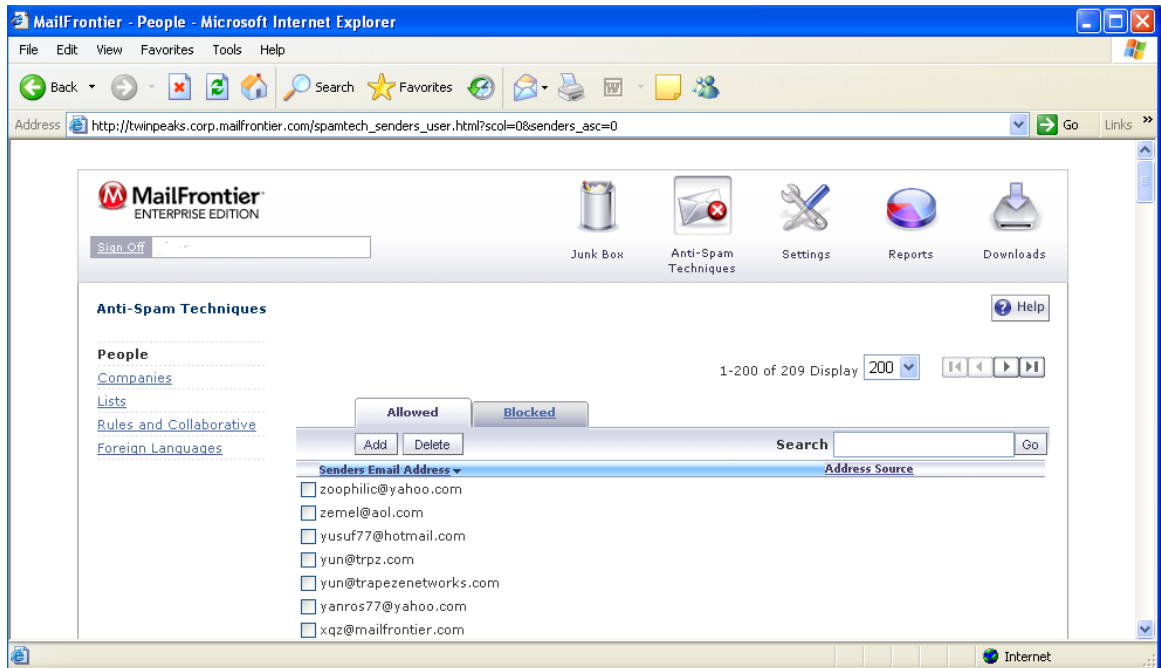


Figure 12 Deleting People from the Allowed List

2. Click the checkbox adjacent to the address to delete that address from the **Allowed** list.
3. Click **Delete**.

Adding Companies or Domains to the Allowed or Blocked Lists

To add companies or domains to **Allowed** or **Blocked** lists:

Click the **Anti-Spam Techniques** button.
The window in Figure 13 appears.

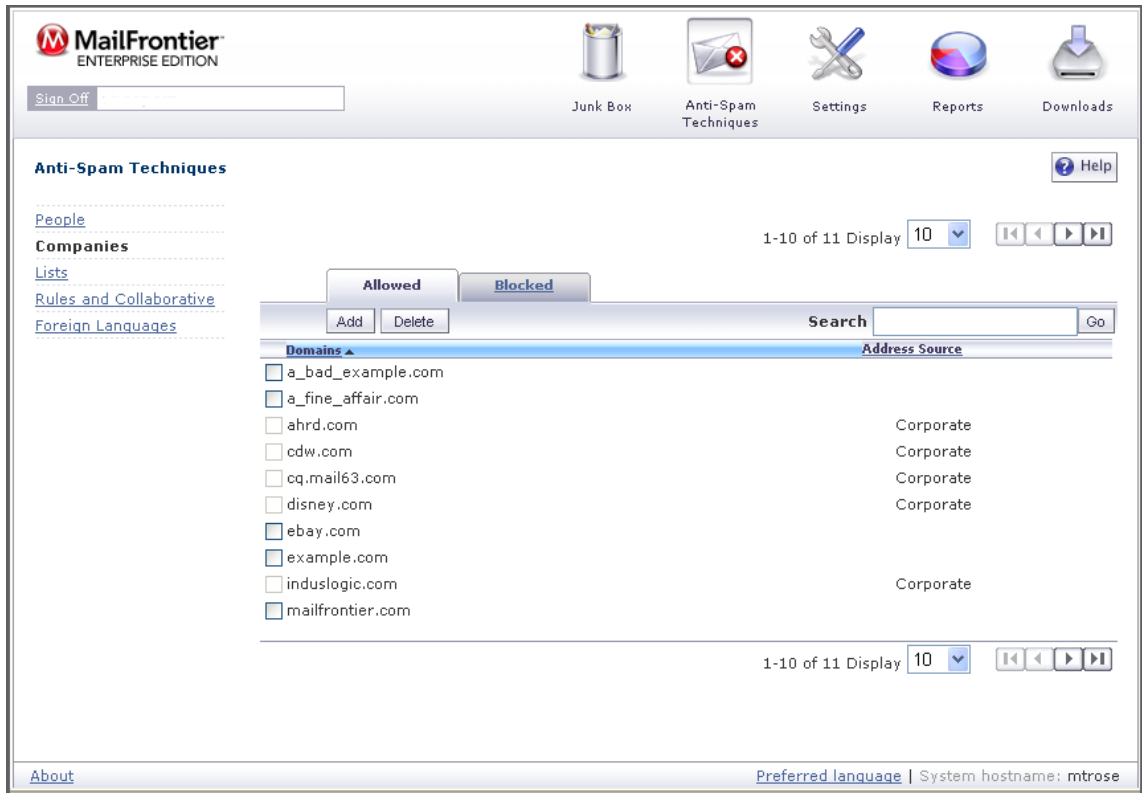


Figure 13 Allowing or Blocking Companies and Domains

Note: In Figure 13, some company addresses are adjacent to a dimmed checkbox. These addresses are on the organization Allowed list; users cannot delete these companies.

1. Click **Companies**.

A list of companies is displayed, as shown in Figure 14.



Figure 14 Add Companies to Allowed List

2. Click **Allowed** to view the companies and domains in the Allowed list.

Adding a Company or Domain to the Allowed List

1. Enter the name of the company or domain.

NOTE: Specify full domain names in this format: *example.com* or *example.gov*.
Domain names such as *.gov* or *.com*, are not valid entries.

2. Click **Add** to add a company or domain.

Deleting a Company or Domain

To delete a company or domain:

1. Check the check box adjacent to the name of the company or domain you want to delete.
2. Click the **Delete** button to delete that company from the Allowed list.
The Delete Domain window appears, as shown below.

Adding Lists to the Allowed List

Email messages from mailing-list servers do not always come from the same email address or FROM: field in the address. The email messages are from the person who posted the message to the list-server and the message is to (TO) the mailing list. The list sections looks at both the FROM: and TO: fields and allows only mailing-list mail.

Note: You can only add and delete Allowed lists.

To add lists to Allowed Lists:

1. Click the **Anti-Spam Techniques** button.
2. Click the **Lists** link.

The **Lists** window appears, as shown in Figure 15.

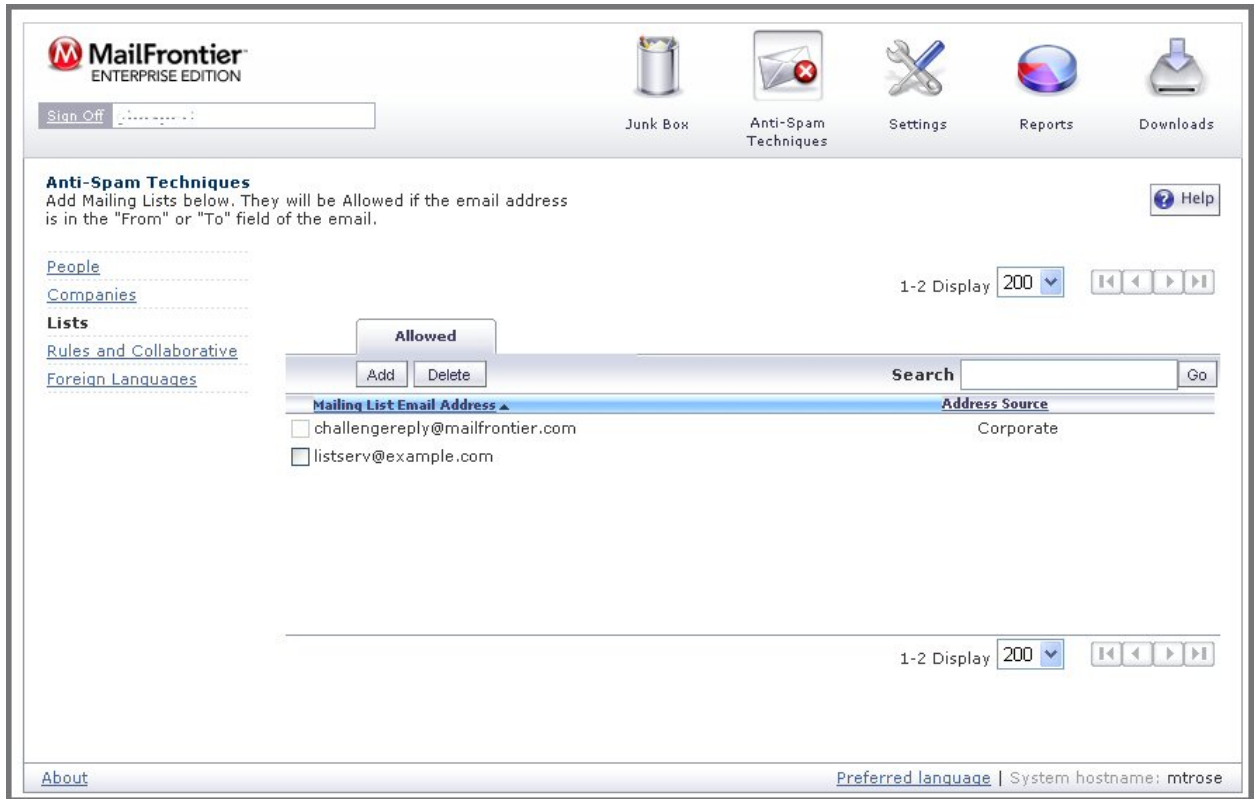


Figure 15 Allowed Lists

3. Click **Add** to add mailing lists to Allowed Lists. The **Add Lists** window appears, as shown in Figure 16.

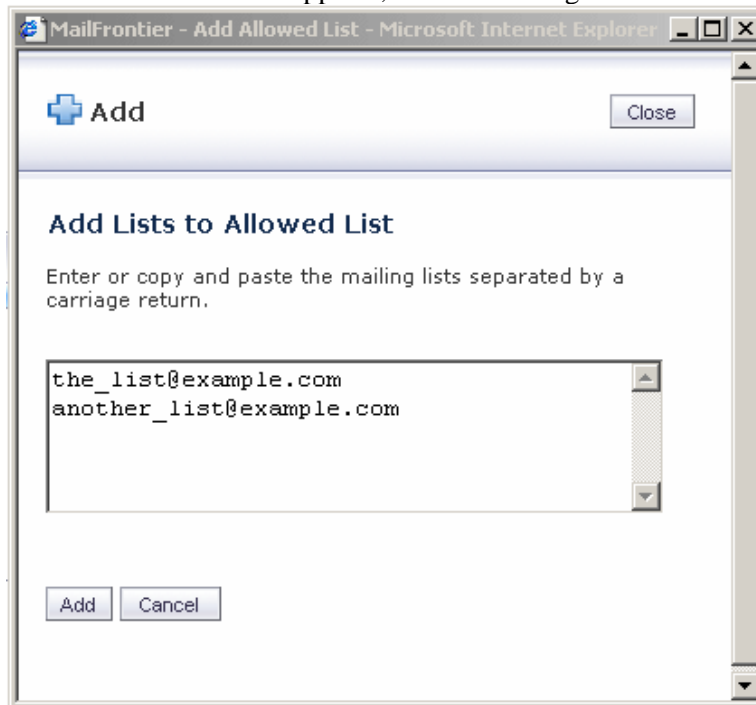


Figure 16 Add Lists to Allowed List

4. Enter the addresses of the lists.
5. Enter a carriage return between each list.
6. Click **Add**.

The updated Allowed Lists window appears, as shown in Figure 17.

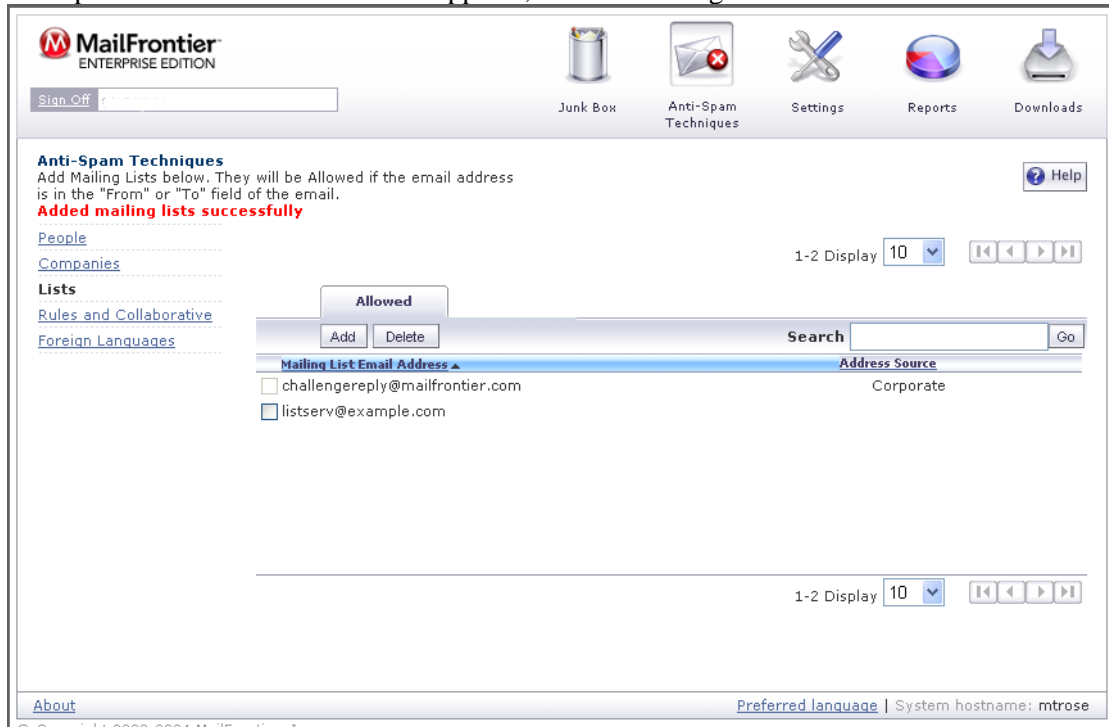


Figure 17 Updated Allowed Lists Window

Screening Messages in Other Languages

The Foreign Languages window allows you to use the language in which a message is written as a criteria for receiving the message.

For each language shown in Figure 18, you can choose allow, block, or have no opinion. For example, you might want to receive all messages in Baltic, but want to block messages in another language. You might also have no opinion about receiving messages in other languages.

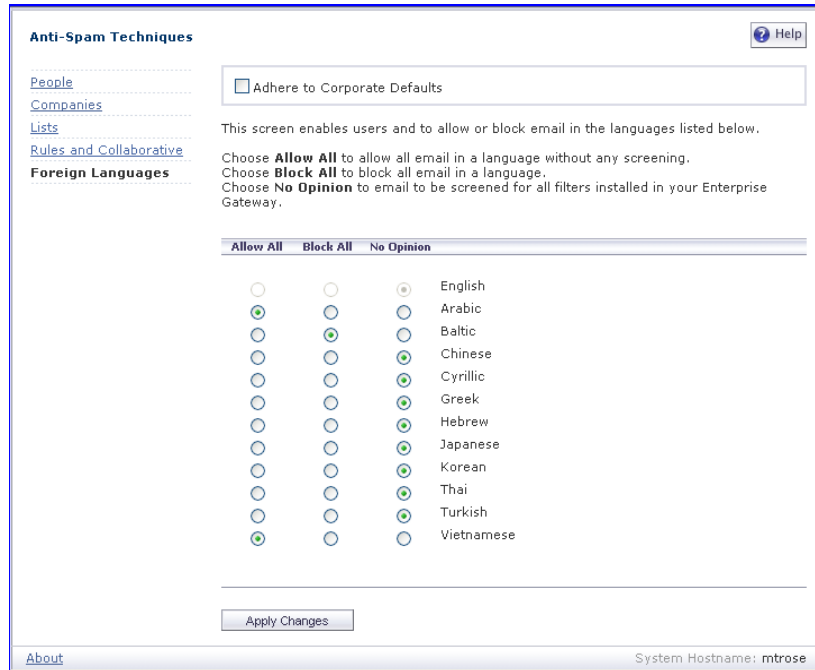


Figure 18 Foreign Language

For each language, decide if you want to receive or block messages in that language.

To receive all messages in a language, click the button under **Allow All** adjacent to the language.

To block all messages in a language, click the button under **Block All** adjacent to the language.

1. Click **No Opinion** for a language to receive messages in that language. All messages in languages for which you choose **No Opinion** are screened for spam and all other filters in SonicWALL Email Security.

Note: English is not included on the list of foreign languages because it is the default language for SonicWALL Email Security.

Configuring Language Preferences for SonicWALL Email Security

You can change the language in which the user interface for SonicWALL Email Security is displayed.

To change the language:

1. Click the **Preferred Language** link in the lower right frame of most user interface windows.



The Preferred Language window appears, as shown in Figure 19.

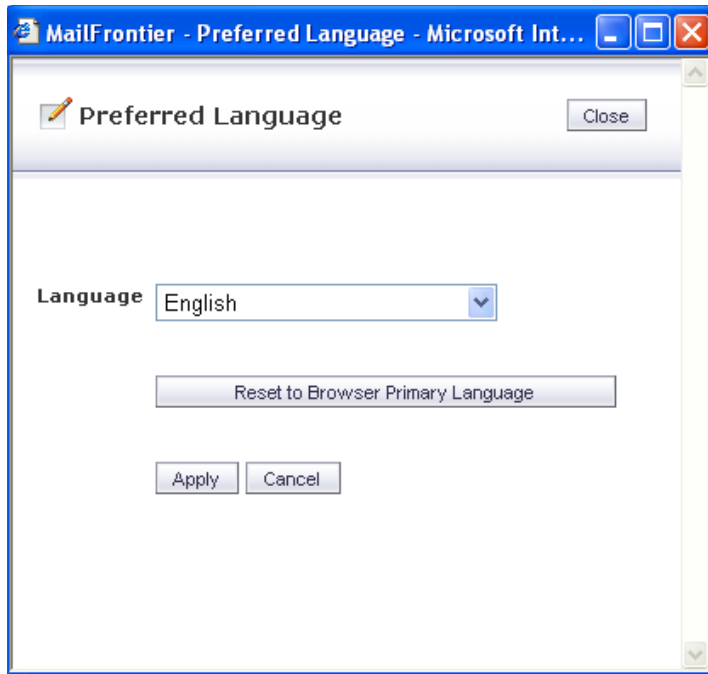


Figure 19 Preferred Language

1. Click the **Language** drop-down list.
2. Select any of the available languages.

NOTE: Your computer must support the language so that the language is displayed correctly.



Figure 20 Available Languages for SonicWALL Email Security

3. Click **Reset to Browser Primary Language** to return to the language your browser

usually runs.

Configuring Language Preferences for your Junk Box Summary

You can configure your Junk Box summary to appear in any of the languages shown in Figure 21, if your computer supports the language modules to display the character sets. To change the language for your Junk Box summary:

1. Log in to the SonicWALL Email Security server.
2. Click the **Visit Junk Box** link.
3. Click the **Settings** icon at the top of the window and select the **Junk Box Summary** link.
4. Select a language from the **Language to send Summary** drop-down list, as shown in Figure 21.

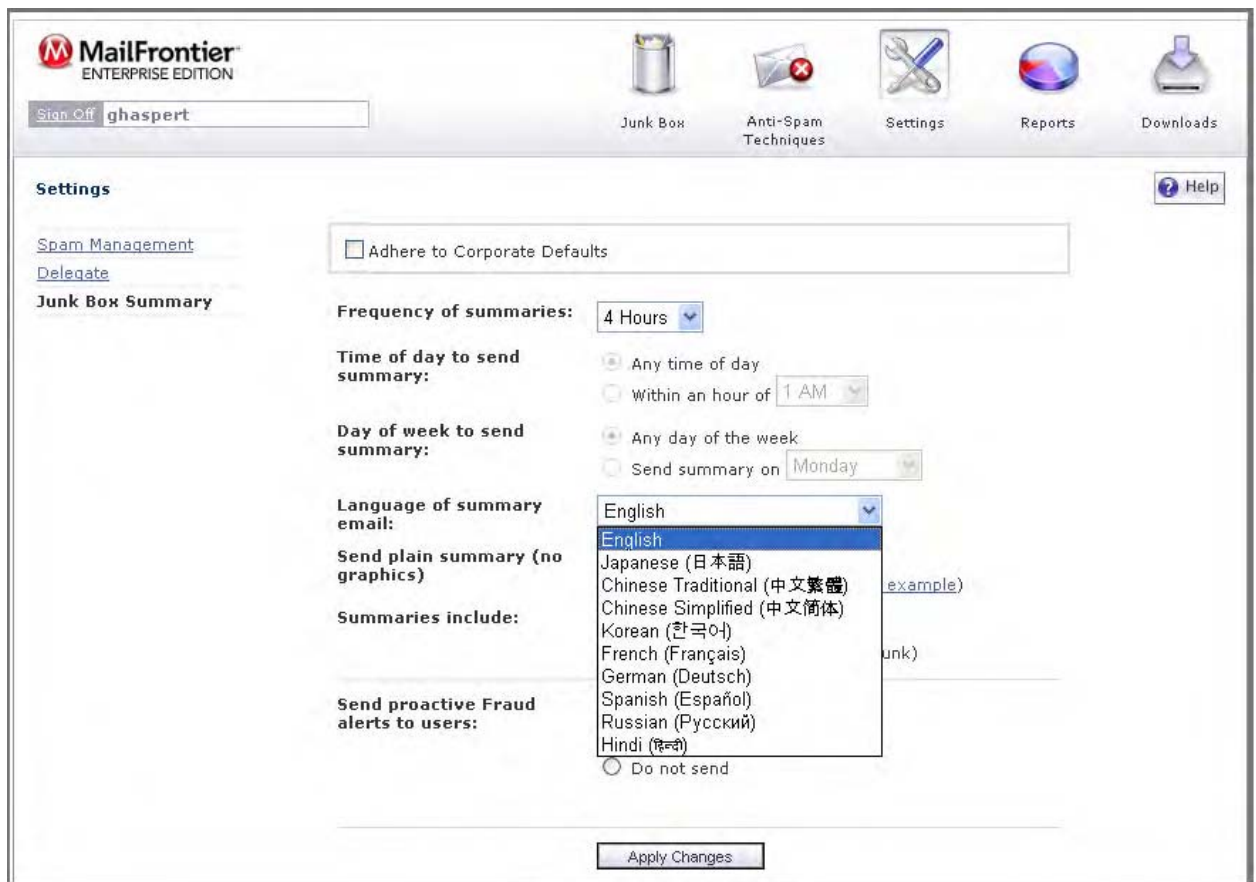


Figure 21 Languages for Junk Box Summaries

5. Click **Apply**.

Configuring Rules and Collaborative Settings

The Rules and Collaborative window allows you tailor SonicWALL Email Security to your preferences. This window is optional. MailFrontier recommends using the default setting of **Medium** or **3** unless you require different settings for specific types of spam blocking.

Note: The **Adhere to Corporate/Group Defaults** checkbox allows you to follow your IT department's recommendations. If your IT department enforces these settings, the checkbox is dimmed; you cannot change blocking levels.

Anti-Spam Techniques Help

[People](#)
[Companies](#)
[Lists](#)
Rules and Collaborative
[Foreign Languages](#)

Adhere to Corporate Defaults

Select the blocking level appropriate to you.

	Mild		Medium		Strong
	1	2	3	4	5
Selecting a stronger setting will make MailFrontier Gateway more responsive to other users who mark a message as spam.					
Collaborative	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Selecting a stronger setting will make MailFrontier Gateway more likely to mark a message as spam.					
Aggressiveness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Selecting a stronger setting will make the content below more likely to be marked as spam.					
Sexual Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Offensive Language	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Get Rich Quick	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gambling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Advertisements	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

[About](#) [Preferred language](#) | System hostname: mtrose

Figure 22 Rules and Collaborative Settings

Configuring Collaborative Settings

You can adjust collaborative settings to customize the level of influence community input has on organization spam blocking. Updates are provided to your gateway server at defined intervals.

To adjust your collaborative settings:

- Click one of the radio buttons from **Mild (1)** to **Strong (5)**.
 A setting of 5 means that you are comfortable with the collective experience of the SonicWALL user community. A setting of 1 or 2 indicates that you are skeptical of the collective experience and want to judge more email for yourself.

Configuring Aggressiveness Settings

The aggressiveness settings are a measurement of how much you want to trust the SonicWALL Email Security filters to screen unwanted email. These settings let you specify preferences in the continuum of choice and volume of email.

Use the **Aggressiveness** settings to specify how much spam and how much good email

being flagged as spam you can tolerate.

- If you choose **Mild** (checkbox **1**), you are likely to receive more questionable email in your mailbox and receive less email in your Junk Box. This can cause you to spend more time weeding unwanted email from your personal mailbox.
- If you choose **Medium** (checkbox **2, 3, or 4**), you accept the SonicWALL Email Security spam-blocking techniques.
- If you choose **Strong** (checkbox **5**), SonicWALL Email Security rules out greater amounts of spam for you. This can create a slightly higher probability of good email messages in your Junk Box.

Determining Amounts and Flavors of Spam

You can determine how aggressively to block particular types of spam, including sexual content, offensive language, get rich quick, gambling, and advertisements.

For each of the spam flavors:

- Choose **Mild** (checkbox **1**) to be able to view email that contains terms that relate to these topics.
- Choose **Medium** (checkbox **2 through 4**) to cause SonicWALL Email Security to tag this email as likely junk.
- Choose **Strong** (checkbox **5**) make it more likely that email with this content is junked.

CHAPTER

4



Settings

Settings

Settings allows you to set various options about what you want to do with messages that are spam, likely spam, phishing, viruses, or have content that is not allowed by your organization's policy.

Click the **Settings** button to view and change your Spam-filtering settings.

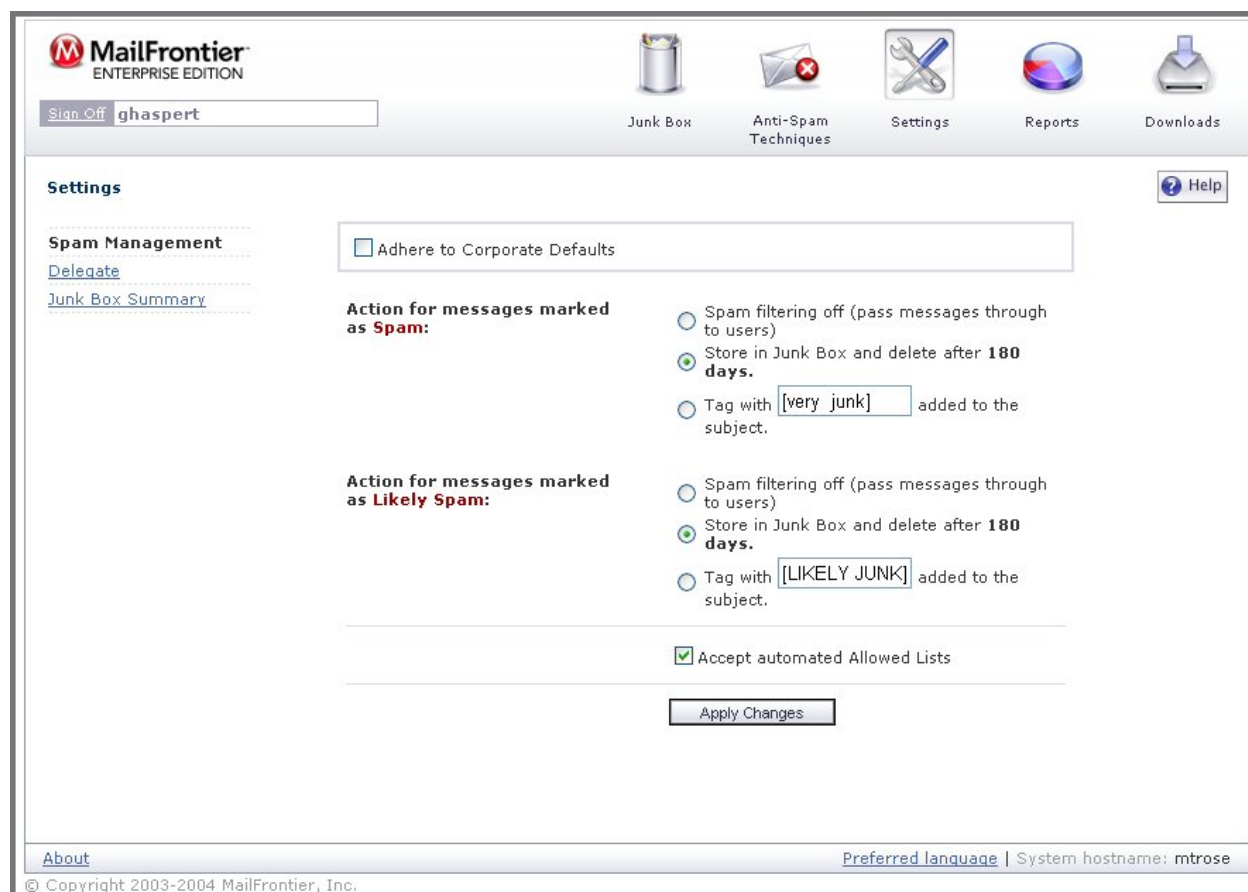


Figure 23 Settings window

Spam Management

You can determine what action to take with messages marked as Spam and Likely Spam. Check one of the following options:

Spam Filtering Off:

SonicWALL Email Security passes messages through to your Inbox

Store in Junk Box and delete after *number* of days:

SonicWALL Email Security stores all messages that it determines as spam for the number of days set by your SonicWALL Email Security administrator.

Tag with text: you can add words to mark messages that are spam or are likely spam.

Assigning Delegates for the Junk Box

The Delegate window allows you to authorize one or more users to monitor your Junk Box, as shown in Figure 24.

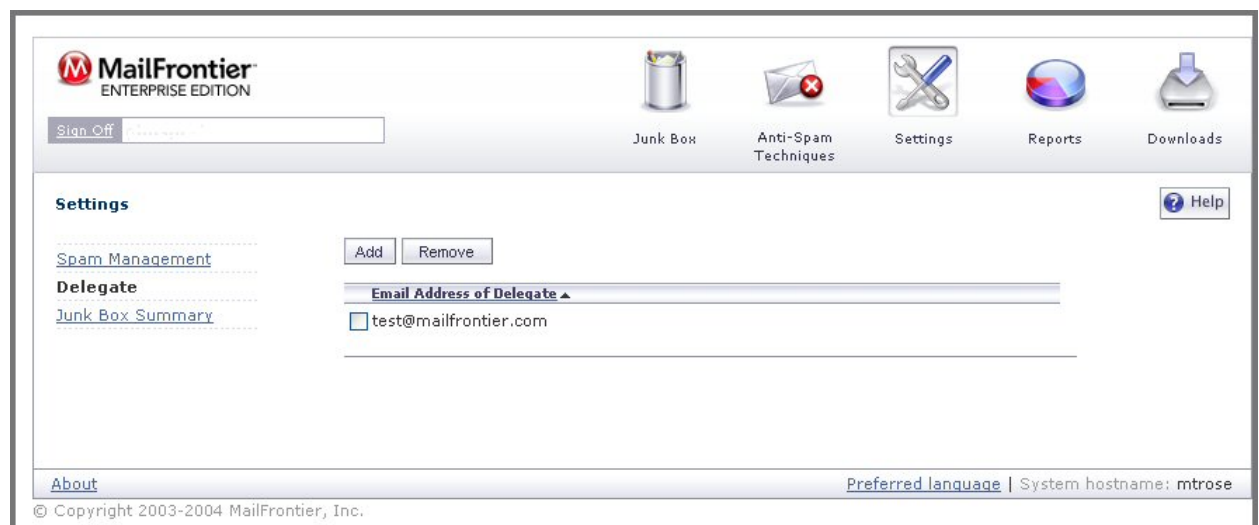


Figure 24 Delegate User

To add a delegate:

1. Click the **Add** button.
The **Add New Delegate** screen appears, as shown in Figure 25.
2. Select a delegate from the list.

If there are too many users to display, to search for the user, type the user's name in the text box and click **Go**.

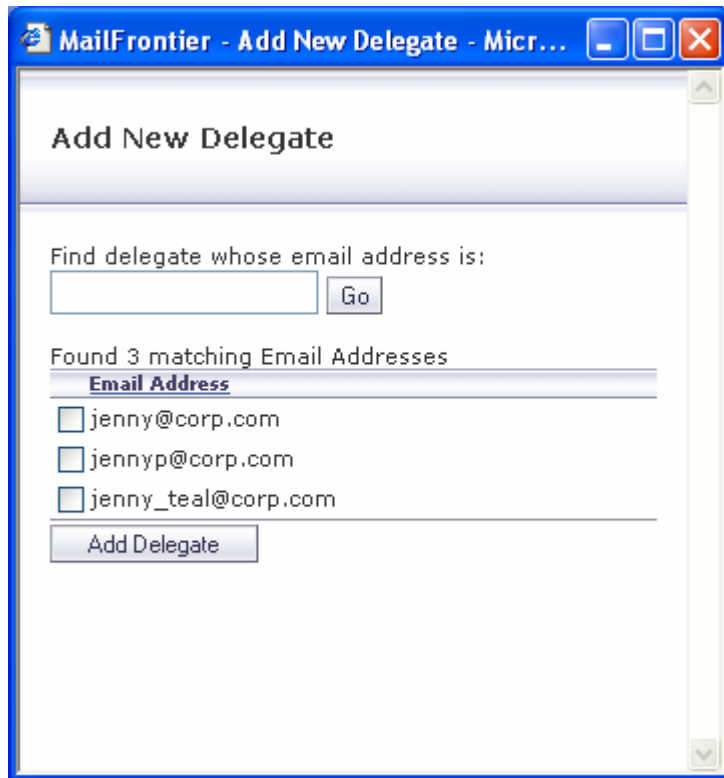


Figure 25 Add New Delegate

3. Enter the email address of the delegate in the textbox.
4. Click the checkbox adjacent to the preferred delegate.
5. Click **Add Delegate**.

Removing a Delegate

To remove a delegate:

1. Click the delegate that you want to remove.
2. Click the **Remove** button in the Delegate window.

Junk Box Summary

When SonicWALL Email Security moves junk and likely junk messages to your Junk Box, you can choose to be notified periodically by email.

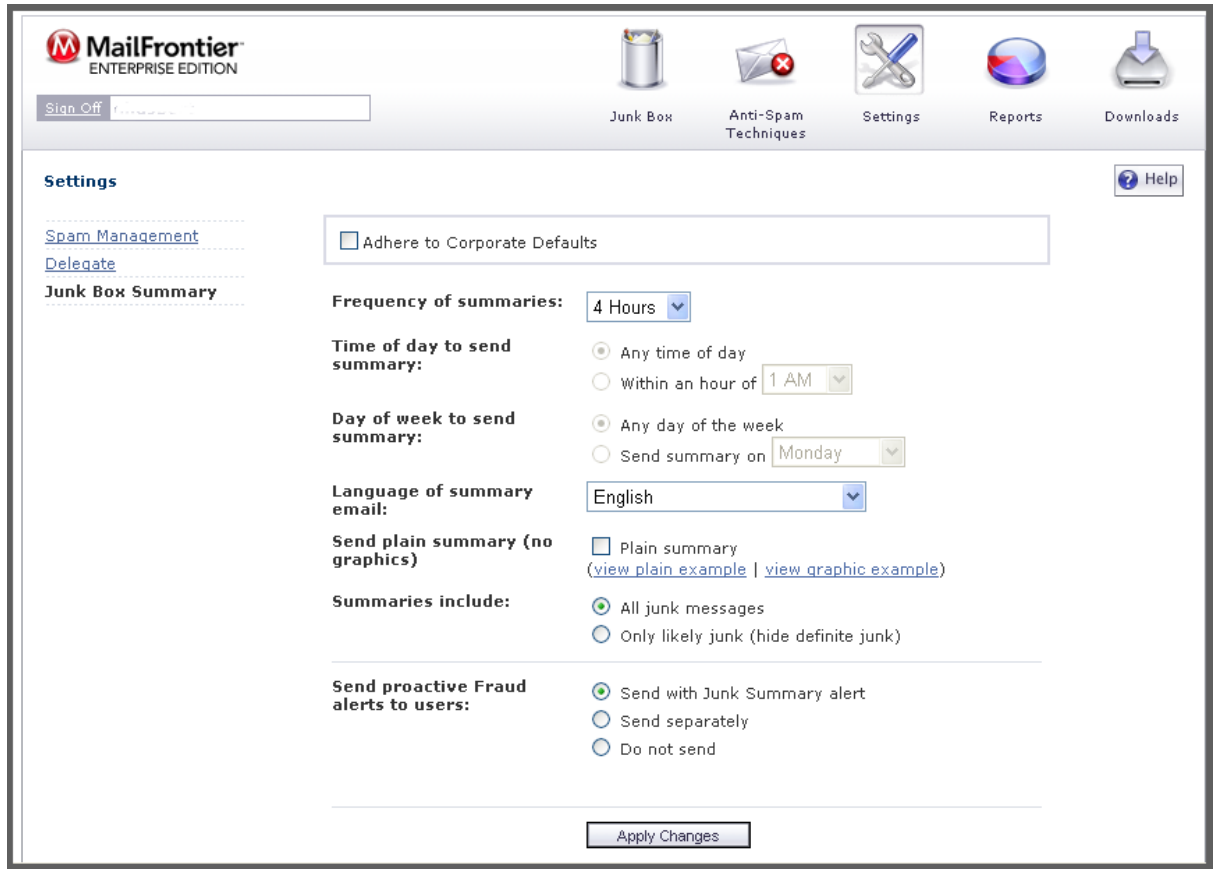


Figure 26 Junk Summary Settings

To manage your junk summary settings:

1. Choose the **default email frequency** for Junk summaries from the dropdown list. Your choices range from one hour to 14 days to never.
2. Choose the **Time of day** to receive the Junk summary.
3. Choose the **Day of the week** to receive the Junk summary.
4. Choose the **Language** in which to view your Junk summary. You can choose to view the your junk summaries in the following languages:

English
 Japanese
 Chinese Traditional
 Chinese Modern
 Korean
 Dutch
 French
 German
 Spanish
 Brazilian Portuguese
 Russian
 Hindi

NOTE: To correctly display the Junk Summary in a language other than English, you must install the appropriate language packs on your computer.

5. If you prefer, check the **Send Simple (no graphics) summary** checkbox.
6. Choose whether to **Include in Summary**:
 - All Junk Messages
 - Likely Junk Only (Hide Definite Junk)
7. For **Phishing Announcements**, choose one of the following options:
 - Include announcements in Junk summary
 - Send announcement via separate email
 - Do not send announcements
8. Click **Apply**.

Send Simple (no graphics) Summary or Graphical Summary

You can receive the Junk Box Summary as a simple list or in a more graphical format. Figure 27 shows a simple list; Figure 28 shows a more graphical presentation.

Junk Box Summary for: biz@mailfrontier.com
The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days.

To receive any of these messages, click UnJunk. The message will be delivered to your inbox and the sender will be added to your Allowed list so their emails are never blocked.

Junk Box Summary

[UnJunk] john@180solutions.com	Re: 180 Advertising
[UnJunk] dmcswwsain@hotmail.com	*- YES, Earn a Doctors income wi...
[UnJunk] support@ebay.com	Win Free Stuff
[UnJunk] spammer@corp.net	Take Some Viagra, its Cheap
[UnJunk] jlef@mb12.com	Enlarge another body part
[UnJunk] sally@getitup.com	Nigerian Prince wants your PIN number
[UnJunk] edd@aled.net	Mortgage rates that are just OK
[UnJunk] aber@is.i.ua	95% off of our Yahts
[UnJunk] save@real-profesions.com	Become a surgeon in only two weeks
[UnJunk] openit@daareyou.com	Open this attachment: crack.exe
[UnJunk] cus@find-family.com	Your long lost half cousin
[UnJunk] tic-tac@halatosis.com	Does your breath stink? Mine did
[UnJunk] smash-mouth@onthesun.com	New now, your an all-star, go play
[UnJunk] wow@cards-for-all.com	Playing cards of Canada's Most Wanted
[UnJunk] mr.tingles@petstylist.com	Pajamas for your Poodle
[UnJunk] info@paypal.com	Paypal lost your info. Please submit again
[UnJunk] strawberry@jam12.net	Platinum Membership to the Jam Club
[UnJunk] sir@mixalot.com	I like big butts and I can not lie
[UnJunk] hard-drive@yourpc.com	A Message From Your Computer: I need updates
[UnJunk] warning@alertsPC.com	*!Alert. Read this. Click on buttons or BOOM
[UnJunk] 31331@haxor.i.ua	133t H@x0r e2 nP10ts
[UnJunk] es@speller.com	Learn to read words like a Pro
[UnJunk] biggy@fat-guru.com	Secret strategies of staying unemployed and fat
[UnJunk] opportunity@yesyoucan.com	Crop dusting jobs for Arab Americans

Figure 27 Simple Junk Box Summary

MailFrontier **Junk Box Summary**
for biz@mailfrontier.com

The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days. To receive any of these messages, click UnJunk. The message will be delivered to your inbox and the sender will be added to your Allowed list so their emails are never blocked.

Junk Box Summary [Visit Junk Box](#)

	From	Subject	Reason
Unjunk View	support@ebay.com	Official notice to biz@mailfrontier.com from Ebay Inc.	Fraud
Unjunk View	dmcswzzain@hotmail.com	-*- YES, Earn a Doctors income wi...	Get Rich
Unjunk View	spammer@corp.net	Win Free Stuff	Gambling
Unjunk View	jlief@mb12.com	Take Some Viagra, its Cheap	Advert
Unjunk View	sally@getbitup.com	Enlarge another body part	Sexual
Unjunk View	edd@aled.net	Nigerian Prince wants your PIN number	Collab
Unjunk View	aber@ls.ua	Morgage rates that are really just ok	Get Rich
Unjunk View	savenow@yahts.com	95% off of our Yahts	Advert

Fraud Alert Notification

Do not respond to any the following emails if you receive one

	From	Subject
View	eBay Inc (support@ebay.com)	Official notice to [your email address] from Ebay Inc.
View	Citibank	Your Checking Account at Citibank
View	(support@ebay.com)	eBay Account Information
		Dear Pa...

Figure 28 Graphical Junk Box Summary

CHAPTER

5



Reports

The reports in this module show statistics for your corporation—not just your own spam. Click the **Reports** button to view them.

SonicWALL Email Security displays summary information about the emails processed, how many were spam, and why they were flagged as spam.

A screenshot of the MailFrontier Enterprise Edition web interface. The top navigation bar includes a "Sign Off" button, a "Junk Box" icon, an "Anti-Spam Techniques" icon, a "Settings" icon, a "Reports" icon (highlighted), and a "Downloads" icon. The main content area is titled "Reports" and contains a "Reports Overview" section. This section includes links for "Messages Processed", "Methods of Identifying Junk Email", and "Reports Overview Since: Nov 2003". The overview statistics are: Total email processed for organization: 4,081,537; Total junk email identified for organization: 1,545,548. A "Reasons" table lists: Allowed List (2,625,754), Blocked List (1,455,691), Rules (298,692), and Collaborative (606,016). The footer contains an "About" link, a "Preferred language" dropdown, and a "System hostname" field. Copyright information for 2003-2004 MailFrontier, Inc. is visible at the bottom left.

Figure 29 Reports

Selecting Reports

Select the report you want to view by clicking the appropriate link to the left. Each report allows you to select the time frame for which you want the report run: hourly, daily, or monthly.

Messages Processed

Click on the **Messages Processed** link to the left to see the statistics on messages that have been filtered by SonicWALL Email Security.

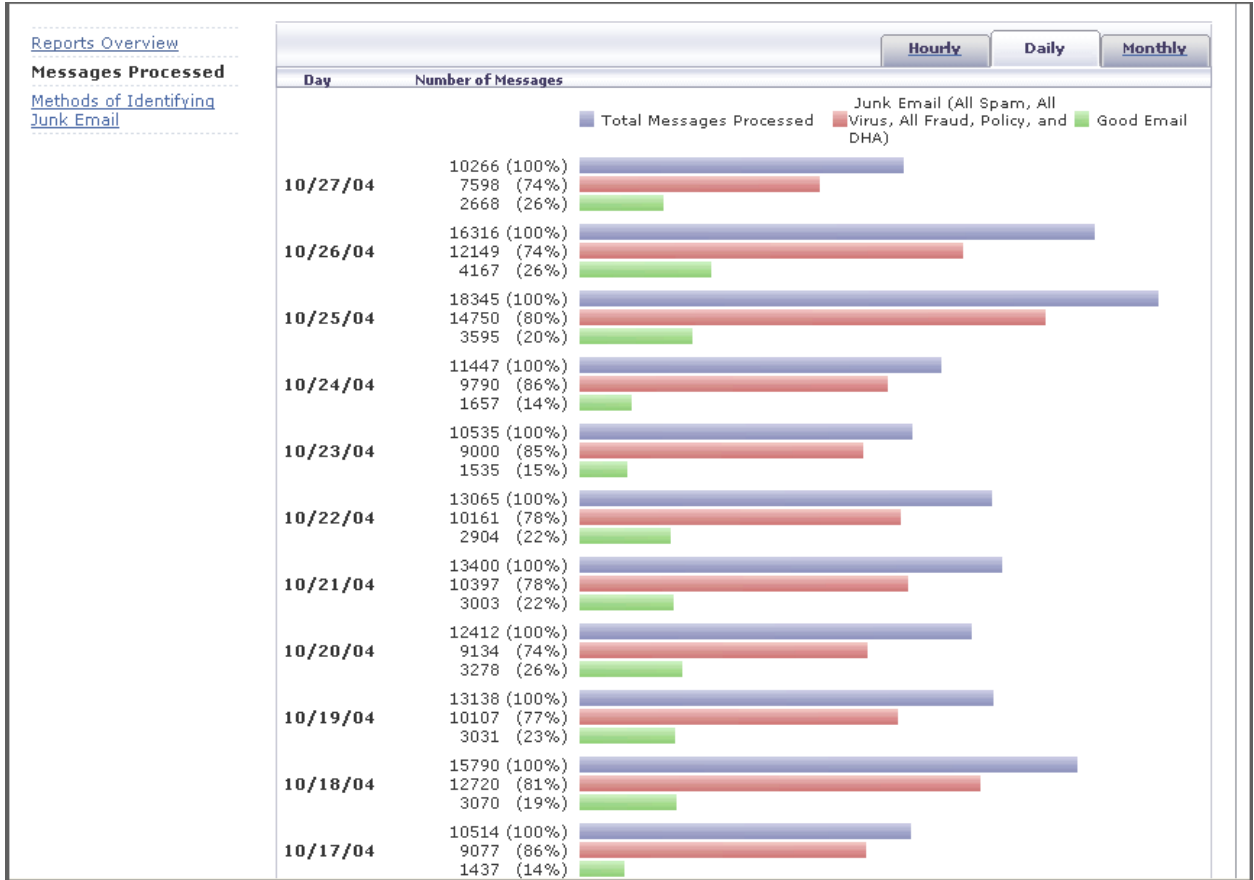


Figure 30 Messages Processed

Methods of Identifying Email

This report illustrates the types of messages received, and shows the comparative amounts of messages that were identified as messages with spam, likely spam, contained viruses, likely contained viruses, phishing, likely phishing, were identified by policy rules, and were considered Directory Harvest Attacks (DHA).

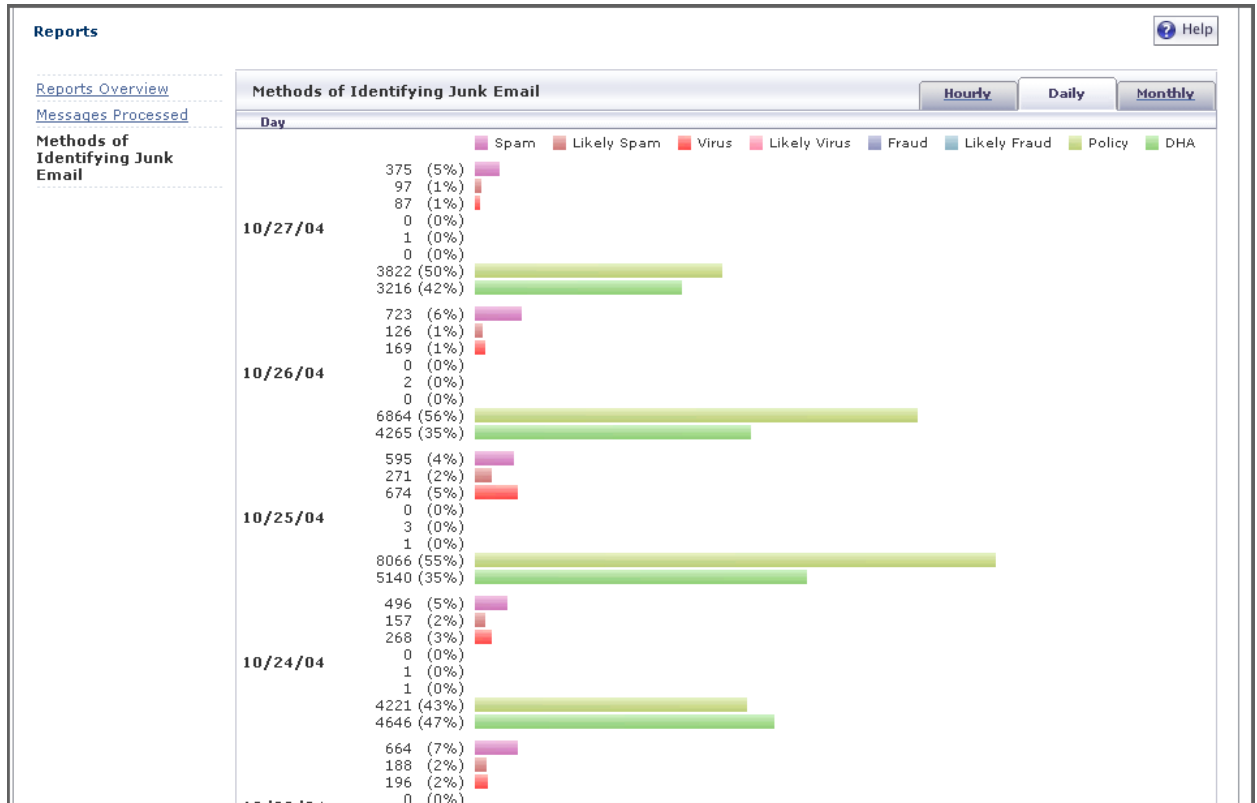


Figure 31 Methods of Identifying Email

Index

A		L	
address conflicts.....	10	logging in	4
allowed and blocked lists	10		
allowed senders.....	2		
B		M	
blocked lists	10	messages	
		processed	32
C		R	
categories of email	2	reports.....	31
		downloading	31
		time frame.....	31
D		S	
deleting		searching	
junk mail	8	corporate junk box	7
Directory Harvest Attacks (DHA).....	32, 33	signing off	9
downloading reports.....	31	statistics	32
J		U	
junk box	7	unjunking mail.....	8
		unknown senders	2