



# Excalibur Technology Corp.

700 Fox Glen • Barrington • IL • 60010  
Ph: 847-842-9570 • Fx: 847-842-0190

support@excaltech.com  
www.excaltech.com



## Excalibur Technology SPAM & Virus Protection System<sup>©</sup>

### **How Does It Work?**

All e-mail messages sent to your e-mail address are analyzed by the Excalibur Technology SPAM & Virus Protection System before being delivered to your inbox. There are over eight levels of SPAM filtering performed on each message as well as three virus scans to help ensure that your messages are safe and trustworthy. There are also over 150 tests that a message must pass before it is approved for delivery to your inbox. In general terms, our system looks to see if the message is being sent from a known spammer, checks to see if it contains objectionable text, and looks at the content of the message for tag lines such as “limited time only” or “free offer” and many more.

Based on the number of tests that each message fails, it receives a SPAM score. The higher the score, the more likely the message is SPAM. We have set four threshold levels on our system that direct mail in various ways depending on the score received. We constantly develop new filtering techniques and will continue our vigilance to ensure that you always receive the highest quality of service and the least amount of junk e-mail.

### **Mail Delivery Score Thresholds**

*Low Score:* Messages that receive a low score are probably sent from reputable sources and are legitimate e-mails that you want. These messages will be delivered to your inbox as normal.

*Medium Score:* Messages that receive a medium score stand a good chance of being bulk mail, mass mail, or from an unreliable source. These messages will have their subject line modified to include [SPAM?] first in the subject, and will then be delivered to you. Our system does this to ensure that you are not going to miss legitimate e-mail, yet lets you know that this message probably is not worth reading.

*High Score:* Messages that receive a high score are almost always SPAM and to be disregarded. However, just incase the scanning process detected a wanted email, these messages will be held in “Quarantine” on our servers for you to review and release if you desire. If you have any messages that are quarantined, our system will notify you via email.

*Critical Score:* Messages that receive a critical score are more than likely blatant SPAM messages, virus infected or dangerous to your system and are discarded by the SPAM firewall. These messages are unrecoverable.

## How will you know the system is working? What else do you need to know?

The first day you have quarantined messages, you will receive a message from “Excalibur Spam Firewall” entitled “User Quarantine Account Information.” Open this mail message to receive your username and password to our SPAM server. You may click the link in that email to immediately logon to your personal Quarantine Inbox. Once you logon to the server, you will see a list of quarantined messages. You may choose to delete the messages, deliver the messages or whitelist the messages, meaning that all future messages from that sender will pass through the SPAM filter and receive a Low Score.

## Getting Started

Each user of the Excalibur SPAM Firewall is provided a personal SPAM Quarantine Inbox and custom user preferences to help efficiently manage SPAM. The SPAM Firewall interface is web based and can be accessed by using a standards based web browser such as Microsoft Internet Explorer or Mozilla Firefox. Users of protected mailboxes will receive an e-mail message from “Excalibur Spam Firewall” entitled “User Quarantine Account Information” upon the receipt of their first quarantined e-mail message. This message contains a username and password to login to their personal Quarantine Inbox as well as a hyperlink to immediately access it.

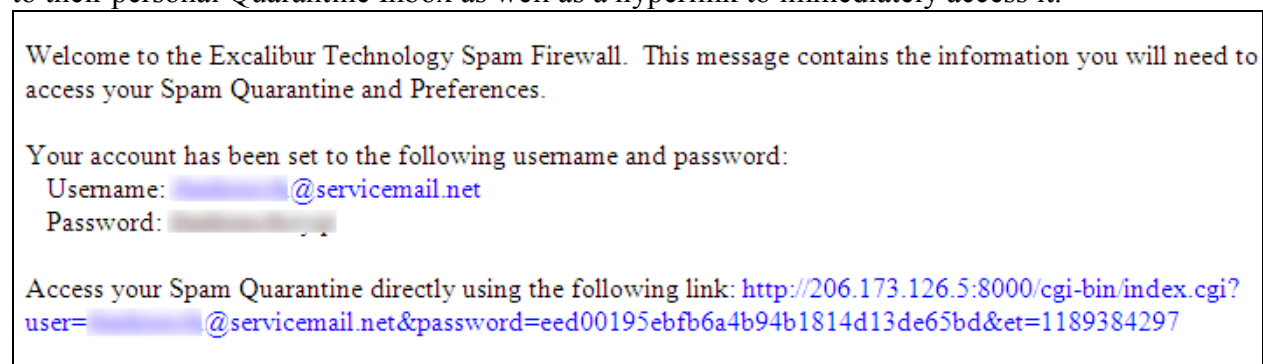


Figure 1 - Sample "User Quarantine Account Information" E-Mail

By default, users receive a summary message from the Excalibur SPAM Firewall each day. This message includes general statistics of the users Quarantine Inbox and displays the most recent quarantined messages in the Quarantine Inbox at the time it was delivered. Three actions can be performed on quarantined messages directly from the e-mail message by clicking on the action hotlinks listed to the right of each message. These actions, which are described in each summary e-mail received, are Deliver, Whitelist and Delete. Further actions and the ability to perform actions in bulk against many quarantined messages are available in the full web based SPAM Quarantine interface. This interface can be accessed by clicking the ‘click here’ hyperlink at the bottom of the most recently received ‘SPAM Quarantine Summary’ e-mail. Be aware that this link will expire after 48 hours, delivering you to the logon screen of the SPAM Firewall instead of directly into your Quarantine Inbox.



# Excalibur Technology Corp.

## SPAM QUARANTINE SUMMARY

Account: [redacted]@servicemail.net

This is your quarantine summary from the Excalibur Technology Spam Firewall.

You have **54** messages in your spam quarantine inbox. The most recent [redacted] of which are displayed below.

- Click on the **Deliver** link to have a message delivered to your mailbox.
- Click on the **Whitelist** link to have a message delivered to your mailbox and whitelist the sender so that his/her messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine.

Time Received From	Subject	Actions
09/04/07 04:55:31 "Daryl K. Lynch" <Daryl@raidersfan.net>	When I tried to [redacted] Please help!	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
09/04/07 04:14:28 "Mauricio G. Pruitt" <Mauricio@bellamyflaw.com>	My [redacted] mouth.	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
09/04/07 00:31:35 FootSmart <[redacted]@email.campaign.footsmart.com>	NEW Fall Shoe Arrivals - Now in Stock	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
09/03/07 22:26:02 "Rob Ivey" <agham@karen-mok.com>	ADOBE Pro retail price - US \$ 449.00 Our price: \$79.95 save \$369.05	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
09/03/07 13:02:39 "zhixin Pierson" <Pierson@bilknet.de>	ahctook	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
09/02/07 00:16:50 FootSmart <[redacted]@email.campaign.footsmart.com>	48 hours left to save 15%	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
09/01/07 11:05:01 <j.sundelin@garlandisd.net>	Day Trader, Weekend Report	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
08/31/07 18:15:41 "Plow&Hearth" <[redacted]@news.plowhearth.com>	Save Big At Our End-Of-Summer Clearance!	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
08/31/07 11:45:37 <Richard8@my-account-bankofamerica.com>	IMPORTANT :Update Your Bank of America Account	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
08/30/07 07:56:53 "Jeffrey Garland" <gtranm@gtran.com>	Software taking a bite out of your budget? Try OEM.	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
08/30/07 06:10:03 "Hillary" <onthelambzaug@online.kz>	Prepare yourself for this	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>

To view your entire quarantine inbox or manage your preferences, [click here](#).

Figure 2 - Sample "SPAM Quarantine Summary" E-Mail

Users may also log in to their personal SPAM Quarantine Inbox by browsing to <http://206.173.126.5:8000> in a standards based web browser such as Microsoft Internet Explorer or Mozilla Firefox. Users can enter the credentials they received in their original welcome message on this webpage. If a user does not know their credentials to login they may enter their full e-mail address in the 'username' field and click on the 'Create New Password' button. This will immediately deliver a "User Quarantine Account Information" e-mail message to the e-mail address entered. This message is identical in content to the message sent upon initial account creation as shown above in Figure 1.



## Excalibur Technology SPAM FIREWALL

### Excalibur Technology Spam Firewall

#### Login

Please type your email address and password below. If you are the firewall administrator, type your administrative credentials.

Language: English [v]

Username: [input field]

Password: [input field]

Login

**Note:** If you forget your password or do not have a password, type your email address in the **Username** box. Then, click **Create New Password**. A new password will be sent to you.

Create New Password

Figure 3 - Excalibur Technology SPAM Firewall Login WebPage

## Managing Your Quarantine Inbox

The screenshot displays the 'Quarantine Inbox' interface. At the top left is the Excalibur Technology logo with 'SPAM FIREWALL' below it. To the right are navigation tabs for 'QUARANTINE INBOX' and 'PREFERENCES', along with a 'Log Off' button and the user email '@servicemail.net'. A language dropdown is set to 'English'. Below the navigation is a 'Quarantine Usage' bar showing '1% of 5120 KB' and a note that 'Messages older than 15 days will be removed'. A 'Current Message Log Count: 10' is also shown. A row of buttons includes 'Deliver', 'Whitelist', 'Whitelist/Not Spam', 'Delete', 'Classify as Spam', and 'Classify as Not Spam'. The main area is a table with columns: 'Time Received', 'From', 'Subject', and 'Actions'. Each row has a checkbox on the left and links for 'Deliver', 'Whitelist', and 'Delete' in the 'Actions' column.

<input type="checkbox"/>	Time Received	From	Subject	Actions
<input type="checkbox"/>	09/04/07 04:55:31	"Daryl K. Lynch" <Daryl@raidersfan	When	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	09/04/07 04:14:28	"Mauricio G. Pruitt" <Mauricio@bell	My mouth.	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	09/04/07 00:31:35	FootSmart <@email.camp:	NEW Fall Shoe Arrivals - Now in Stock	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	09/03/07 22:26:02	"Rob Ivey" <agham@karen-mok.cor	ADOBE Pro retail price - US \$ 449.00 Our price: \$79.95 s	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	09/03/07 13:02:39	"zhiwin Pierson" <Pierson@bilknet.d	ahctook	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	09/02/07 00:16:50	FootSmart <@email.camp:	48 hours left to save 15%	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	09/01/07 11:05:01	<j.sundelin@garlandisd.net>	Day Trader, Weekend Report	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	08/31/07 18:15:41	"Plow&Hearth" <@news.plowhe	Save Big At Our End-Of-Summer Clearance!	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	08/31/07 11:45:37	<Richard8@my-account-bankofame	IMPORTANT :Update Your Bank of America Account	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	08/30/07 07:56:53	"Jeffrey Garland" <gtranm@gtran.co	Software taking a bite out of your budget? Try OEM.	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>

Figure 4 - SPAM Quarantine Inbox

After logging into the quarantine interface, select the 'Quarantine Inbox' tab to view a list of your quarantined messages. When you first start using the quarantine interface, you should view this list on a daily basis and classify as many messages as you can. The Excalibur Technology Spam Firewall has a learning engine that learns how to deal with future messages based on the ones you classify as spam and not spam. The learning engine becomes more effective over time as you teach the system how to classify messages and as you set up rules using the whitelist and blacklist. Clicking on the title of an email displays the message. Clicking on an action name will perform that action on the corresponding message immediately. The following describes the actions you can perform from this page.

**Deliver:** Delivers the selected message to your standard email inbox. Note: If you want to classify a message or add it to your whitelist, make sure to do so before delivering the message to your inbox. Once the Excalibur Technology Spam Firewall delivers a message, it is removed from your quarantine list.

**Whitelist:** Adds the selected message to your whitelist so all future emails from this sender are not quarantined *unless* the message contains a virus or banned attachment type. The Excalibur Technology Spam Firewall adds the sending email address, exactly as it appears in the message, to your personal whitelist.

**Delete:** Deletes the selected message from your quarantine list. This aides you in keeping track of which quarantine messages you have reviewed. You cannot recover messages you have deleted. The server will automatically delete messages older than 15 days without user intervention.

## Applying Bulk Actions to Messages

All actions listed above can be performed against a single message or multiple messages simultaneously. To prepare multiple messages to have a single action applied, such as deleting several messages from the quarantine inbox, click on the checkbox to the right of each message you wish to process with the action. Once this has been completed, simply click on the desired action among the buttons above the quarantined message list. To process all messages displayed on the page, click on the checkbox that appears in the title bar above the first message and then select the desired action.

The actions available for bulk application contain the three actions described above (Deliver, Whitelist and Delete) as well as the following:

**Classify as Spam:** Classifies the selected message(s) as spam in your personal learning database and then deletes it. Consistent use of this feature will aid the system in reducing the amount of SPAM you receive based on your personal preferences and standards.

**Classify as Not Spam:** Classifies the selected message(s) as not being spam in your personal learning database and delivers it to your e-mail inbox. Consistent use of this feature will aid the system in delivering desired mail to you based on your personal preferences and standards.

Note: Some bulk commercial email may be considered useful by some users and spam by others. Instead of classifying bulk commercial email, it may be more effective to add it to your whitelist (if you wish to receive such messages) or blacklist (if you prefer not to receive them). Directions for how to accomplish this appear below.

**Whitelist/Not Spam:** Performs the same actions described above for the 'Classify as Not Spam' action as well as those described for the 'Whitelist' action. Effectively, this classifies the message(s) as not being spam in your personal learning database, adds the sender to your personal whitelist and then delivers the message to your e-mail inbox.

## Changing your User Preferences

After logging into your quarantine interface, you can select the 'Preferences' tab to change your account password, modify your quarantine and spam settings, and manage your personal whitelist and blacklist.

## Changing Your Whitelist/Blacklist Settings

The following describes the options available within the 'Whitelist/Blacklist' configuration page within the 'Preferences' tab.

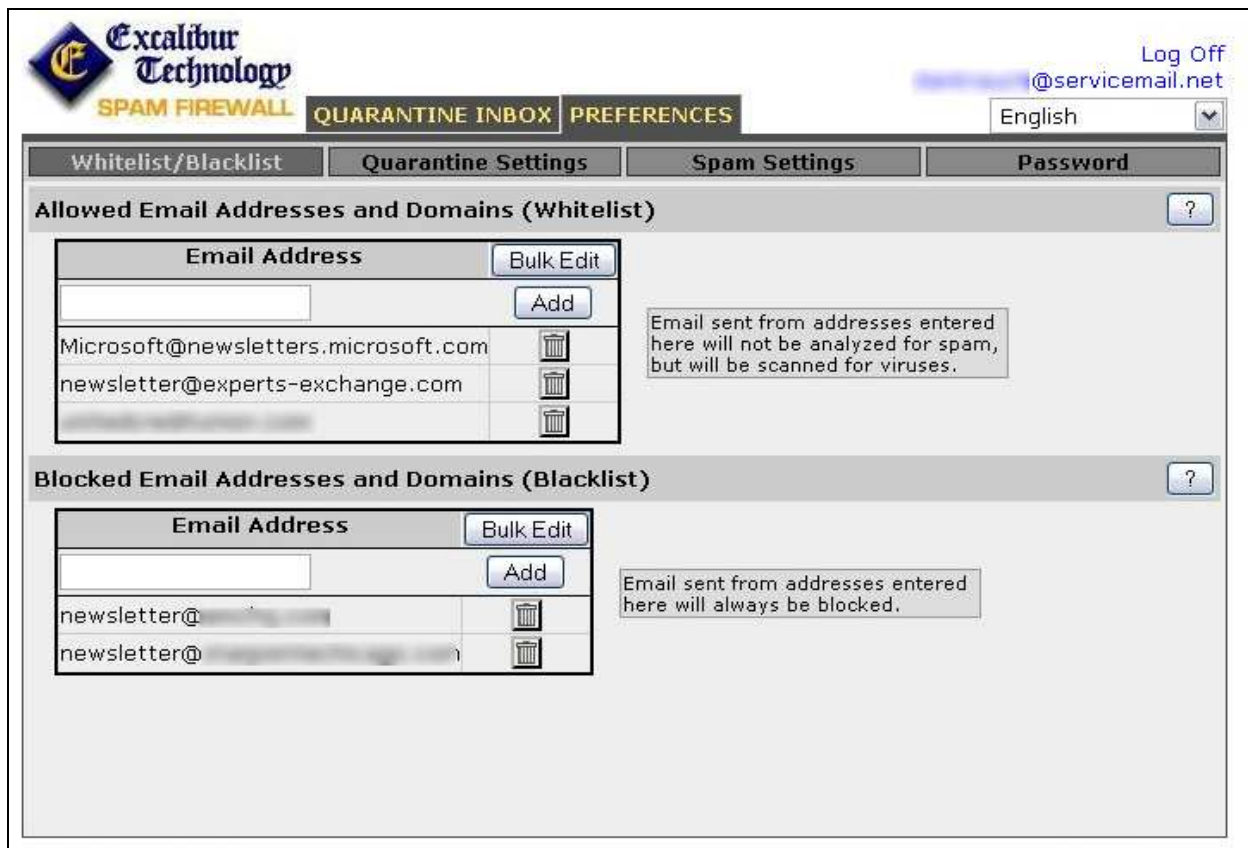


Figure 5 - Whitelist/Blacklist Dialog

**Allowed Email Addresses and Domains (Whitelist):** This section displays, and allows you to define, e-mail addresses and domains from which messages will be delivered to you without Spam scoring or being quarantined, regardless of content. The only exceptions to this rule are messages containing a virus or disallowed attachment type. The source addresses of messages that have had the 'Whitelist' action applied from the Quarantine Inbox or Quarantine Notification message will appear in this list. To manually add an address to this list, enter it into the box that appears at the top of the 'Email Address' table and click on the 'Add' button. You can also enter a domain, the part of an e-mail address that appears AFTER the @, to ensure mail sent from ALL addresses at that domain are delivered to your e-mail inbox. If you define a domain all sub domains are also included. As an example, if you entered ExcaliburTechnology.com, e-mail from sub domains support.ExcaliburTechnology.com and web.ExcaliburTechnology.com would also be accepted. To remove entries from the Whitelist table click on the 'Trash Can' icon displayed to the right of the entry. This action will be applied immediately without confirmation. Advanced users may wish to use the 'Bulk Edit' button which allows editing the list as a single text document to increase the speed of making many additions/removals.

**Blocked Email Addresses and Domains (Blacklist):** This section displays, and allows you to define, e-mail addresses and domains from which messages will be discarded regardless of content. To add an address to this list, enter it into the box that appears at the top of the 'Email Address' table and click on the 'Add' button. You can also enter a domain, the part of an e-mail address that appears AFTER the @, to ensure mail sent from ALL addresses at that domain are discarded. If you define a domain all sub domains are also included. As an example, if you entered ExcaliburTechnology.com, e-mail from sub domains support.ExcaliburTechnology.com and web.ExcaliburTechnology.com would also be discarded. To remove entries from the Blacklist table click on the 'Trash Can' icon displayed to the right of the entry. This action will

be applied immediately without confirmation. Advanced users may wish to use the ‘Bulk Edit’ button which allows editing the list as a single text document to increase the speed of making many additions/removals.

**A Note Regarding Mass Mailings:** Mass mailings often come from domains that do not resemble the organizations website name. For example, you may want to receive mailings from historybookclub.com, but you will find that this site sends out its mailing from the domain hbcfyi.com. Examine the “From:” address of an actual message that you are trying to whitelist or blacklist to determine what to enter.

## Changing Your Quarantine Settings

The following describes the options available within the ‘Quarantine Settings’ configuration page within the ‘Preferences’ tab.

The screenshot shows the 'Excalibur Technology SPAM FIREWALL' interface. The 'PREFERENCES' tab is selected, and the 'Quarantine Settings' sub-tab is active. The 'Quarantine Enable/Disable' section has 'Enable Quarantine' set to 'Yes' (radio button selected) and a 'Save Changes' button. A tooltip explains that if 'No', messages are delivered with '[QUAR]' in the subject line, and the recommended setting is 'Yes'. The 'Quarantine Notification' section has 'Notification Interval' set to 'Daily' (radio button selected), a 'Notification Address' text box, and a 'Save Changes' button. A tooltip explains that this determines how often you receive an email summary of quarantined messages, with a recommended setting of 'Daily'. The 'Default Language' section has 'Default Language' set to 'English (iso-8859-1)' (dropdown menu) and a 'Save Changes' button. A tooltip explains that this sets the default quarantine message language and encoding, and notes that all email notifications from Barracuda will be in UTF8 encoding.

Figure 6 - Quarantine Settings Dialog

**Quarantine Enable/Disable:** This setting determines whether the Excalibur Technology Spam Firewall quarantines your messages. If set to ‘Yes’, the Excalibur Technology Spam Firewall does not deliver messages scored for high enough to quarantine to your general email inbox, but you can view these messages from the quarantine interface and quarantine summary reports as described earlier in this document. If set to ‘No’, all messages that would have been quarantined for you are delivered to your general email inbox with the subject line prefixed with ‘[QUAR]:.’ Select the desired behavior and click on the ‘Save Changes’ button in the section title bar to change these settings.

**Quarantine Notification:** The 'Notification Interval' sets the frequency with which Excalibur Technology Spam Firewall sends you quarantine summary reports. [See Figure 2 above for a sample Quarantine Summary Report.] The default setting is daily. Please note that *the Excalibur Technology Spam Firewall only sends a daily quarantine summary report when one or more of your emails have been quarantined on that day.* If you select Never, you can still view your quarantined messages from the quarantine interface, but you will not receive quarantine summary reports in your e-mail inbox.

**Notification Address** The email address the Excalibur Technology Spam Firewall should use to deliver your quarantine summary report.

Select the desired options and click on the 'Save Changes' button in the section title bar to change these settings.

**Default Language:** This setting defines the language in which you want to receive your quarantine notifications. This setting also sets the default encoding for handling unknown character sets during filtering. All email notifications from the Excalibur Technology Spam Firewall are in UTF8 encoding.

## Changing Your Spam Settings

The following describes the options available within the 'Spam Settings' configuration page within the 'Preferences' tab.

The screenshot shows the 'Spam Settings' configuration page. At the top left is the Excalibur Technology logo and 'SPAM FIREWALL'. Navigation tabs include 'QUARANTINE INBOX' and 'PREFERENCES'. The user is logged in as '@servicemail.net' with a 'Log Off' link and a language dropdown set to 'English'. The 'Spam Settings' tab is active, showing sections for 'Spam Filter Enable/Disable', 'Spam Scoring', 'Bayesian Learning', and 'Bayesian Database Backup'. Each section has a 'Save Changes' button and a help icon (?).

Section	Option	Value	Recommendation/Note
Spam Filter Enable/Disable	Enable Spam Filtering:	<input checked="" type="radio"/> Yes <input type="radio"/> No	If No, all messages will be delivered without being scanned for spam. <b>Recommended: Yes</b>
	Spam Scoring	Use System Defaults:	<input checked="" type="radio"/> Yes <input type="radio"/> No If No, you must specify the scoring levels that you would like to use below. <b>Recommended: Yes</b>
Spam Scoring	Tag:	3	Score at which subject line is modified. <b>Recommended: 3.5</b>
	Quarantine:	3.5	Set to 10 to disable quarantine. <b>Recommended: 10</b>
	Block:	5	Set to 10 to disable blocking. <b>Recommended: 7</b>
Bayesian Learning	Messages classified as "Spam":	491	
	Messages classified as "Not Spam":	50	
	Reset Bayes Database:	<input type="button" value="Reset"/> <input type="button" value="Expert Only"/>	
Bayesian Database Backup	Backup Bayesian Database:	<input type="button" value="Backup"/>	<input type="button" value="Save file to local system"/>
	Restore Database:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload Now"/>	<input type="button" value="Upload file from local system"/>

Figure 7 - Spam Settings Dialog

**Spam Filter Enable/Disable:** - This setting determines whether the Excalibur Technology Spam Firewall scans your messages for Spam. If set to 'Yes', the Excalibur Technology Spam Firewall will scan your messages for Spam, applying scoring and taking action as defined in the 'Spam Scoring' section of this screen. If set to 'No', all messages sent to your e-mail address will be forwarded to your e-mail inbox without being scanned for spam. Select the desired options and click on the 'Save Changes' button in the section title bar to change these settings.

**Spam Scoring:** From this page you can also change the default spam scoring levels that determine when your emails are tagged, quarantined or blocked. When the Excalibur Technology Spam Firewall receives an email for you, it scores the message for its spam probability. This score ranges from 0 (definitely not spam) to 10 or higher (definitely spam). Based on this score, the Excalibur Technology Spam Firewall either allows, quarantines, or blocks the message. *A setting of 10 for any setting disables that option.*

The 'Use System Defaults' option defines if you wish to use the Excalibur Technology selected default scoring defaults against inbound messages. These have been selected to attempt to provide the greatest effective reduction of spam while keeping false positives to an absolute minimum. Select 'Yes' to use the default scoring levels. To configure the scoring levels yourself, select 'No' and make the desired changes in the Spam Scoring Levels section described below by typing the desired value into each scoring threshold box. Once the desired options have been selected click on the 'Save Changes' button in the section title bar to apply the settings.

The first scoring threshold is 'Tag' and it carries a default value of 3. Messages with a score equal to or above this threshold, but below the defined 'Quarantine' threshold, are delivered to you with the word [SPAM] inserted into the beginning of the subject line. Any message with a score below this setting is delivered to your e-mail inbox immediately with no other actions taken. The second scoring threshold is 'Quarantine' and it carries a default value of 3.5. Messages with a score equal to or above this threshold, but below the defined 'Block' threshold, are delivered to your 'Quarantine Inbox' to allow you to take further action as described in the 'Managing Your Quarantine Inbox' section above. The third scoring threshold is 'Block' and it carries a default value of 5. Messages with a score equal to or above this threshold are discarded and are unable to be retrieved. They are neither delivered to your Spam Quarantine or your e-mail inbox.

**Bayesian Learning:** This section displays statistics of your personal Bayesian Learning database. This is a database that aides in classifying messages as being spam based on your personal preferences. It is populated when you classify messages as Spam, or Not Spam, as described in the 'Applying Bulk Actions to Messages' section above. This section also reminds you that the database will not be used to aide in Spam detection if either category has less than 200 messages defined.

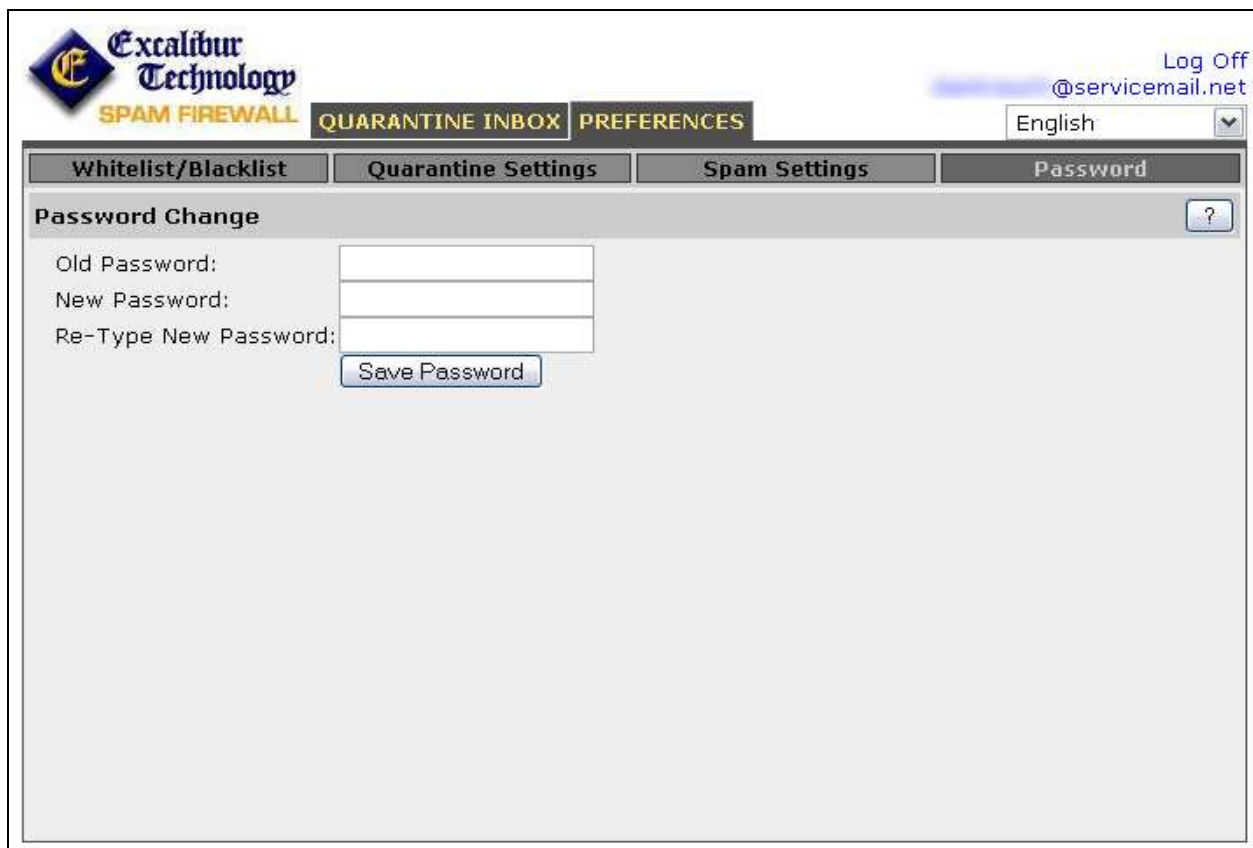
This section also allows you to Reset your personal Bayesian Learning database by pressing the 'Reset' button. This will reset the counters to zero and the effects of all messages classified as Spam, or Not Spam, will be lost. Use this with care and ONLY if you are certain you wish to take this action. This CANNOT be undone unless you have taken a backup as described in the next section.

**Bayesian Database Backup:** To backup your personal Bayesian Database, Click the 'Backup' button in this section to download a copy of your personal Bayesian Database to your local system. This backup copy can then be uploaded to any Excalibur Technology Spam Firewall, including this one, in the case of a corrupt Bayesian installation or to repopulate your Database

after a reset as described in the previous section. To perform a restore of the database, simply click on the 'Browse' button in this section, select the local backup copy in the resulting dialog, and then click on the 'Upload Now' button. The backup database file used to restore does not have to originate from this Excalibur Technology Spam Firewall, nor does it have to originate from your user account.

## Changing Your Password

The following describes how to change your password using the 'Password' configuration page within the 'Preferences' tab. Instructions for recovering a lost password are also included.



The screenshot shows the Excalibur Technology Spam Firewall interface. At the top left is the logo with the text 'Excalibur Technology SPAM FIREWALL'. To the right, there is a 'Log Off' link and an email address '@servicemail.net'. Below this is a language dropdown menu set to 'English'. The main navigation bar includes 'QUARANTINE INBOX' and 'PREFERENCES'. Under 'PREFERENCES', there are four tabs: 'Whitelist/Blacklist', 'Quarantine Settings', 'Spam Settings', and 'Password'. The 'Password' tab is active, showing a 'Password Change' dialog with three input fields: 'Old Password:', 'New Password:', and 'Re-Type New Password:'. A 'Save Password' button is located below the fields. A help icon (?) is in the top right corner of the dialog.

Figure 8 - Password Preferences Dialog

**Changing a Password:** After logging into your quarantine interface, select the PREFERENCES tab and then click on the 'Password' button. In the provided fields, enter your existing password in the first field and your desired password in both remaining fields. Click the 'Save Password' button when finished.

**Retrieving a Lost/Forgotten Password:** On the quarantine interface login page, displayed above in Figure 3, enter your full e-mail address in the username field and click the 'Create New Password' button. This will deliver a welcome message identical to that described in the 'Getting Started' section and displayed in Figure 1 above. Your password will be displayed in this message.

**A Note About Password Changes:** Changing your password breaks the links in your existing quarantine summary reports so you cannot delete, deliver, or whitelist messages from those reports. New quarantine summary reports will contain updated links that you can use the same as before.

## **Global Settings**

**Changing the Language of the Quarantine Interface:** You can change the language of your Quarantine interface at any time. Just select your desired language from the drop down menu in the upper right corner of the web interface. Supported languages include Chinese, Japanese, Spanish, French, and others. The language you select is only applied to your individual quarantine interface. No other user's interface is affected.

## **In Closing**

### **What to do if you still receive SPAM:**

First, you should understand that there is a difference between SPAM e-mail and simple unwanted e-mail. Unwanted e-mail might be a one-time solicitation from a local company, sales updates from a vendor with whom you do business with, or communications between members of your local club. Because many people might want to receive this type of mail, it cannot be banned from mail systems. It is up to you to make the appropriate requests to the sender to be removed from their mailings. If this still does not work, we suggest that you setup rules in your e-mail software that automatically moves messages from particular senders into a junk mail folder or straight into the recycle bin. Information on rules can be found in your software documentation. If you would like assistance with rules, please call our office for a telephone or Virtual Technician support session.

If you still receive blatant unsolicited junk mail, please forward your messages to [abuse@excaltech.com](mailto:abuse@excaltech.com). Our staff will make the appropriate changes necessary to ensure the integrity of your e-mail account. However, understand that no matter how advanced our SPAM filtering system is, occasional junk messages will get through. This is to be expected and will eventually cease as our scanning techniques continuously improve.

### **Removal for the SPAM scanning service:**

While this service is available to our clients free of charge, it is optional. Please call our office and speak to the web department if you would like to be removed from the SPAM service. We will route all mail directly to your boxes without any type of scanning. We hope that you continue to find our services of value and we will continuously improve our efforts to bring you the fastest, safest and cleanest e-mail service possible. If you have any further suggestions or comments, please contact our office. We appreciate your business and look forward to serving you for years to come.

Expect great things from our company – always.