EXCALTECH℠
Making IT Simple

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

How does the Excalibur Technology SPAM & Virus Protection System 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 in case 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.

EXCALTECH℠
Making IT Simple

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

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 Technology 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 Technology 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.

Welcome to the Excalibur Technology Spam Firewall 1. This message contains the information you will need to access your Spam Quarantine and Preferences.

Your account has been set to the following username and password:
Username: [redacted]@servicemail.net
Password: da[redacted]yqt

Access your Spam Quarantine directly using the following link: https://filter1.excaltech.com:443/cgi-mod/index.cgi?user=[redacted]@servicemail.net&password=[redacted]f8e139989105a13f5f4&et=1273681651&role=_nodomains

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. Four 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, Delete and View. All messages displayed on this summary can be deleted from the Quarantine by clicking on the 'Delete All Displayed Mails' button in the lower left corner of the message. Further actions and the ability to perform any action 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. Direct access to allowed/block list, quarantine

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

notification interval and spam scoring preference panels is also available via links that appear beneath the quarantined message list. These preferences are explained later in this document.

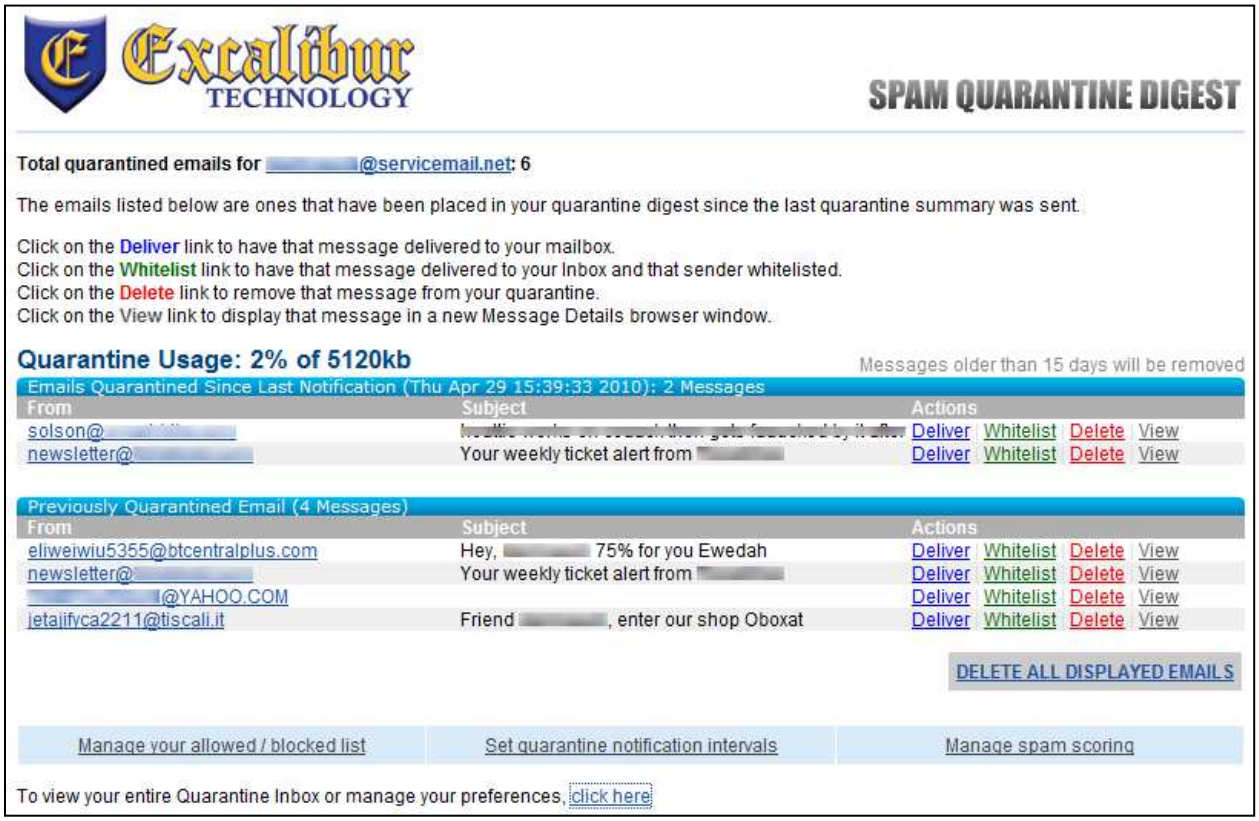

Figure 2 - Sample "SPAM Quarantine Summary" E-Mail

Users may also log in to their personal SPAM Quarantine Inbox by browsing to https://filter.excaltech.com 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.

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

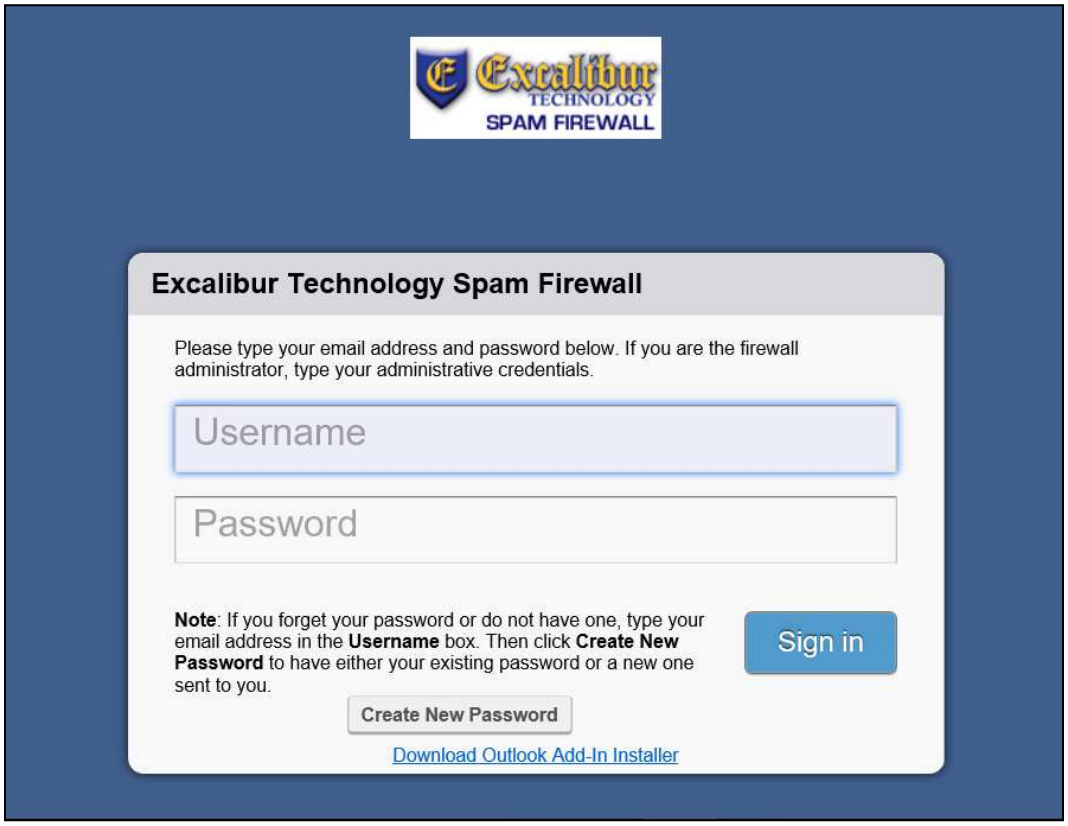

Figure 3 - Excalibur Technology SPAM Firewall Login WebPage

EXCALTECH℠
Making IT Simple

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

Managing Your Quarantine Inbox

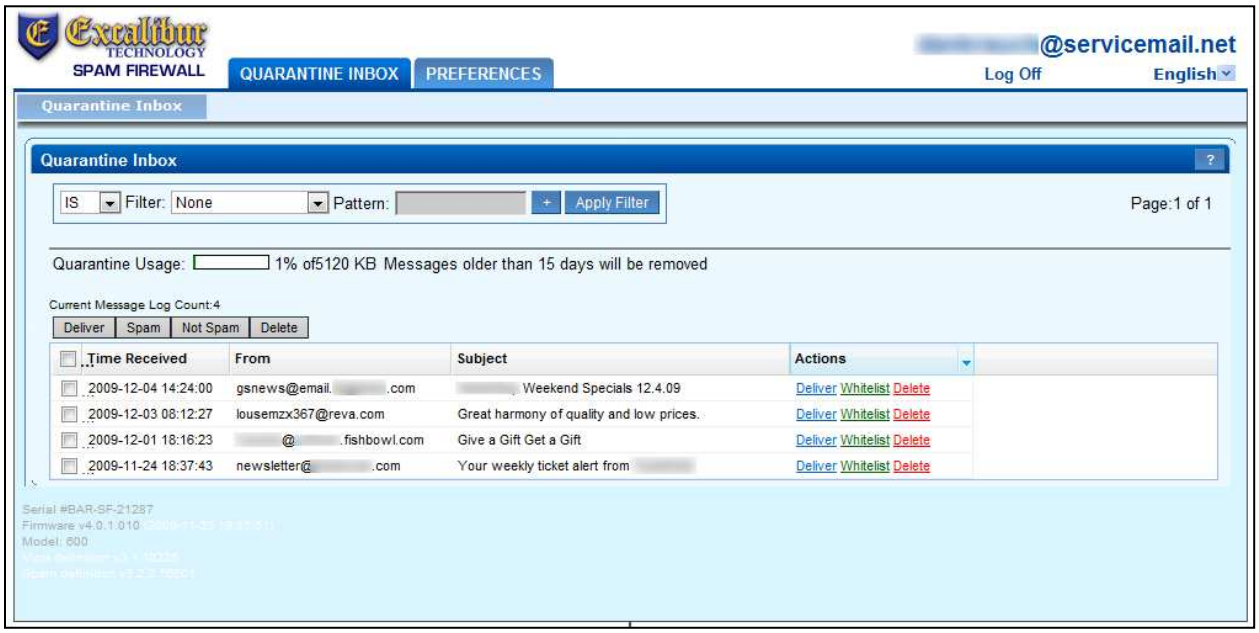

Figure 4 - SPAM Quarantine Inbox

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 handle future messages based on the ones you classify as being spam or 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 functions. Clicking on the subject 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.

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

Delete: Deletes the selected message from your quarantine list. This aids 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

Four actions 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 two of the actions described above (Deliver 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.

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.

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

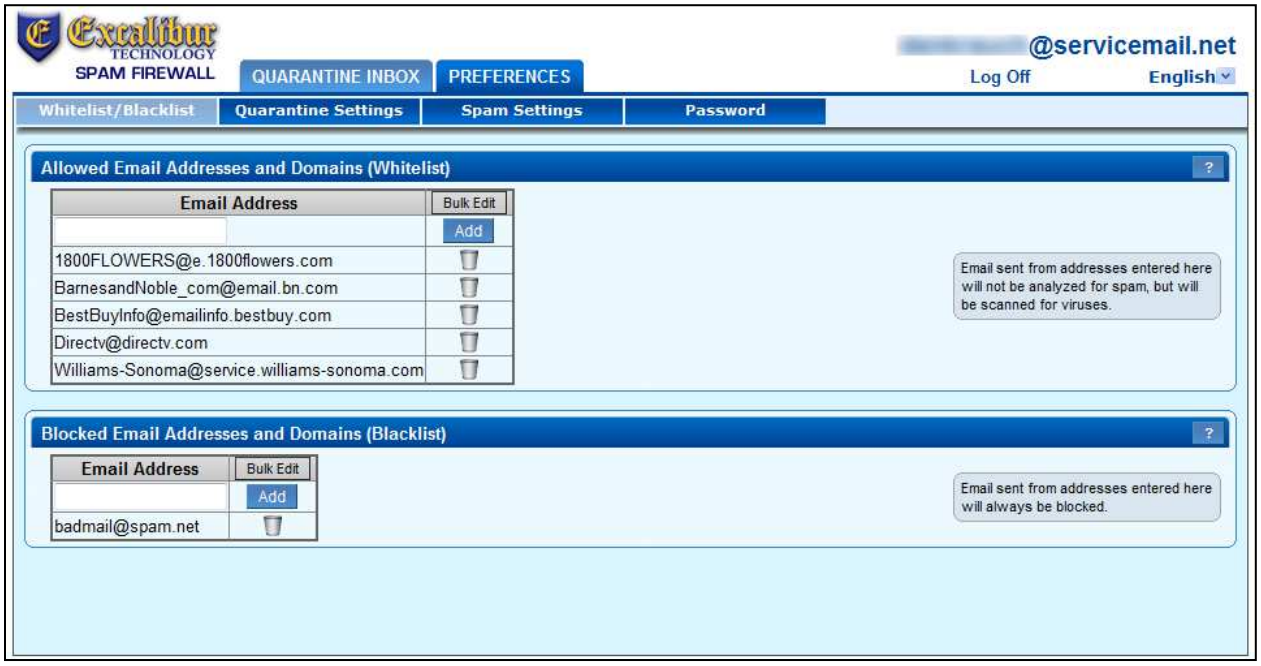

Figure 5 - Whitelist/Blacklist Dialog

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

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

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 the appropriate domain name to enter.

Changing Your Quarantine Settings

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

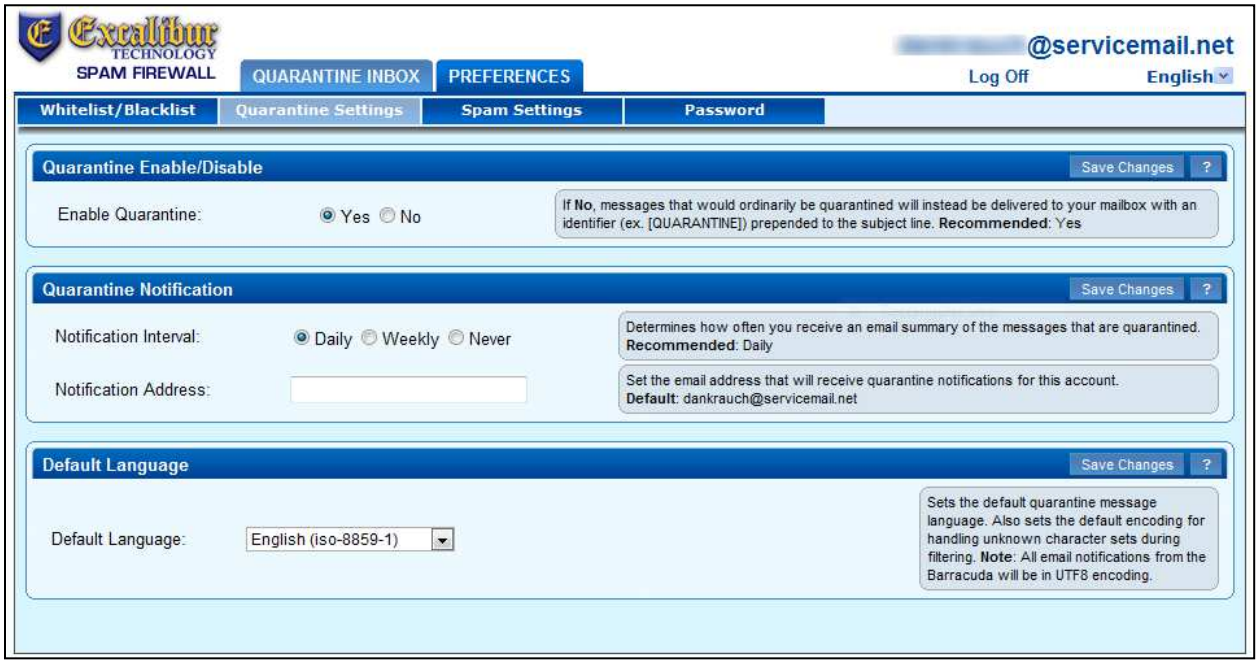

Figure 5 - Quarantine Settings Dialog

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

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

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 t*he 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.

EXCALTECH℠
Making IT Simple

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

Changing Your Spam Settings

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

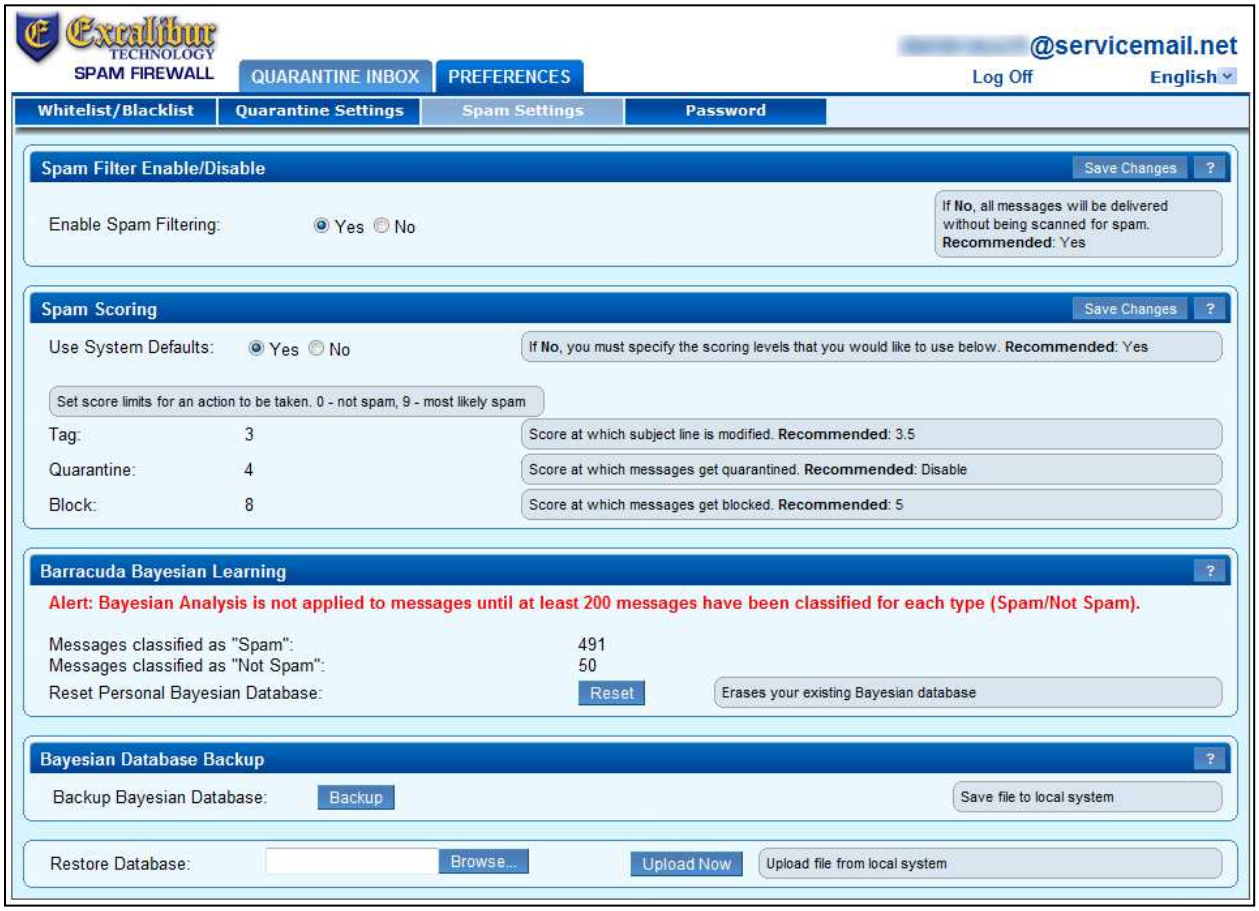

Figure 6 - Spam Settings Dialog

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

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

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 aid in Spam detection if either category has fewer 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 back up 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

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

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.

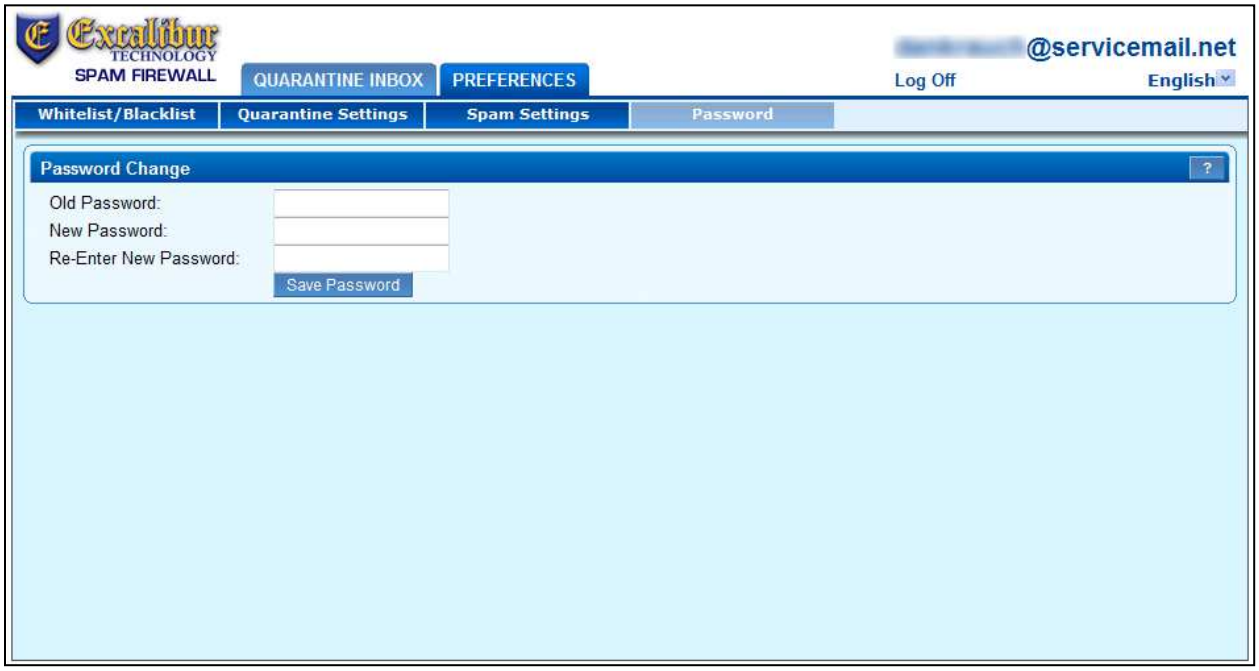

Figure 8 - Password Preferences Dialog

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.

ExcalTech℠
Making IT Simple

700 Fox Glen
Barrington, Illinois 60010
ph/fx: [847] 842 - 9570
www.excaltech.com
support@excaltech.com

Global Settings

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