

# Green House Data Spam Firewall User Guide

Spam Firewall User Guide.....	2
Quarantine Summary Report.....	2
Using the Quarantine Interface.....	3
Logging Into the Quarantine Interface.....	3
Using The Quarantine Inbox.....	4
Changing Your User Preferences .....	5
Changing Your Quarantine Settings.....	5
Adding Email Addresses and Domains to Your Whitelist and Blocklist .....	6
Changing the Language of the Quarantine Interface .....	7
Changing Your Spam Settings .....	7
Microsoft Outlook Add-in for Classifying Messages.....	8
Downloading the Add-in.....	8
Using the Microsoft Outlook Add-in.....	9

# Green House Data Spam Firewall User Guide

This guide describes how you can use the Spam Firewall web interface to:

- Check your quarantined messages
- Classify messages as Spam and Not Spam
- Manage whitelisting and blacklisting email addresses
- Modify your User Preferences

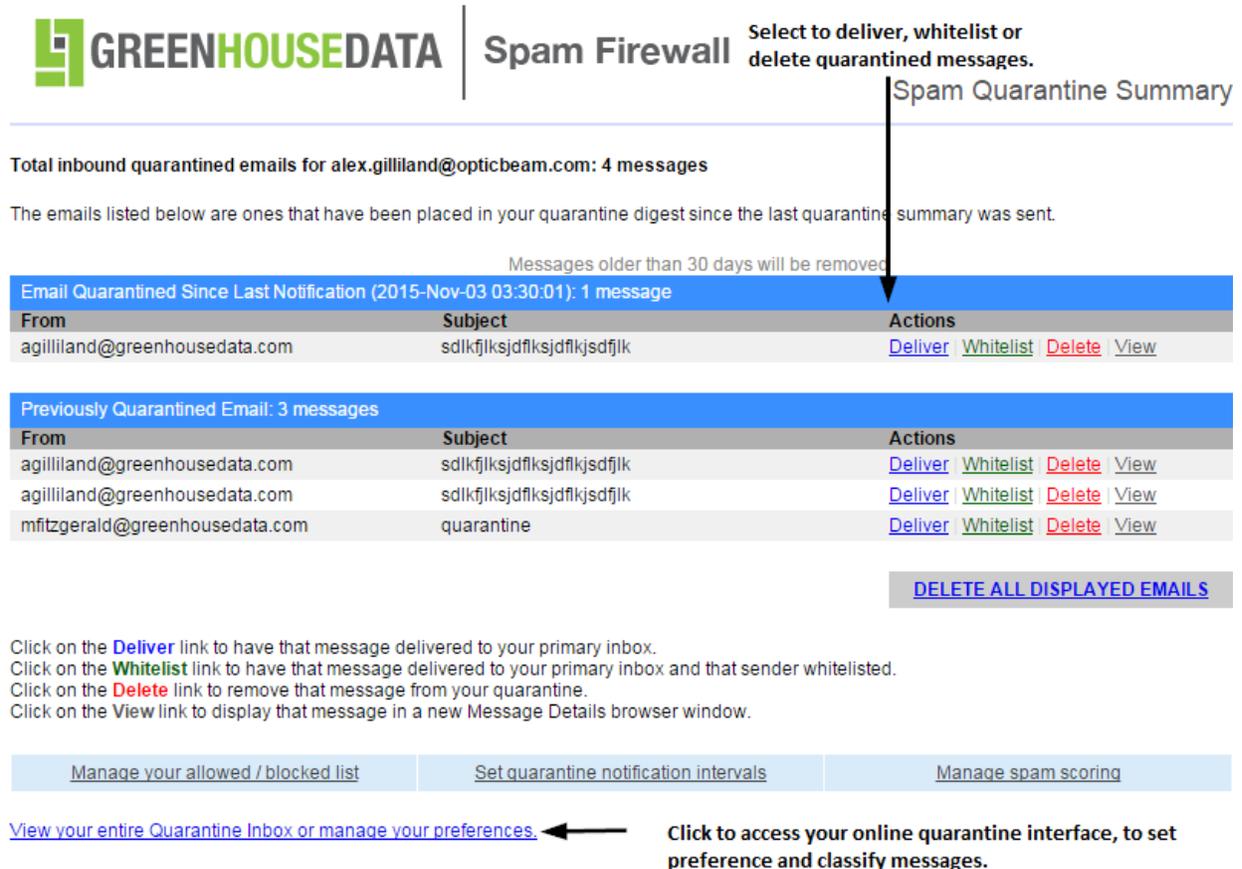
The guide also covers use of the Barracuda Microsoft Outlook Add-in for classifying messages as spam or not spam.

## Quarantine Summary Report

The Spam Firewall sends you a daily quarantine summary report so you can view the quarantined messages you did not receive. From the quarantine summary report you can also add messages to your whitelist, delete messages, and have messages delivered to your inbox.

**Note:** The quarantine summary report is only sent if new quarantined mail is saved in your account since the last notification cycle. Each day the quarantine notification service runs for all users. If there is no new quarantined mail for your account since the last notification cycle, or if you have logged into your account since then, no quarantine summary report will be generated and sent to you for that same 24-hour period. Links in the quarantine digest for viewing, delivering, whitelisting or deleting a message from the quarantine inbox expire in 5 days from the date the digest is sent out, however, the online digest will hold 30 days of quarantined email.

The following shows an example of a quarantine summary report:



**GREENHOUSEDATA | Spam Firewall** Select to deliver, whitelist or delete quarantined messages.

Spam Quarantine Summary

Total inbound quarantined emails for alex.gilliland@opticbeam.com: 4 messages

The emails listed below are ones that have been placed in your quarantine digest since the last quarantine summary was sent.

Messages older than 30 days will be removed

Email Quarantined Since Last Notification (2015-Nov-03 03:30:01): 1 message

From	Subject	Actions
agilliland@greenhousedata.com	sdlkfjksjdfkjsdfkjsdfjlk	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a> <a href="#">View</a>

Previously Quarantined Email: 3 messages

From	Subject	Actions
agilliland@greenhousedata.com	sdlkfjksjdfkjsdfkjsdfjlk	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a> <a href="#">View</a>
agilliland@greenhousedata.com	sdlkfjksjdfkjsdfkjsdfjlk	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a> <a href="#">View</a>
mfitzgerald@greenhousedata.com	quarantine	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a> <a href="#">View</a>

[DELETE ALL DISPLAYED EMAILS](#)

Click on the [Deliver](#) link to have that message delivered to your primary inbox.  
 Click on the [Whitelist](#) link to have that message delivered to your primary inbox and that sender whitelisted.  
 Click on the [Delete](#) link to remove that message from your quarantine.  
 Click on the [View](#) link to display that message in a new Message Details browser window.

[Manage your allowed / blocked list](#)    [Set quarantine notification intervals](#)    [Manage spam scoring](#)

[View your entire Quarantine Inbox or manage your preferences.](#) ← Click to access your online quarantine interface, to set preference and classify messages.

Figure 1: Example quarantine summary report ('digest').

## Using The Quarantine Interface

There is a link at the end of every quarantine summary report to the online quarantine interface where you can set additional preferences and classify messages as spam or not spam.

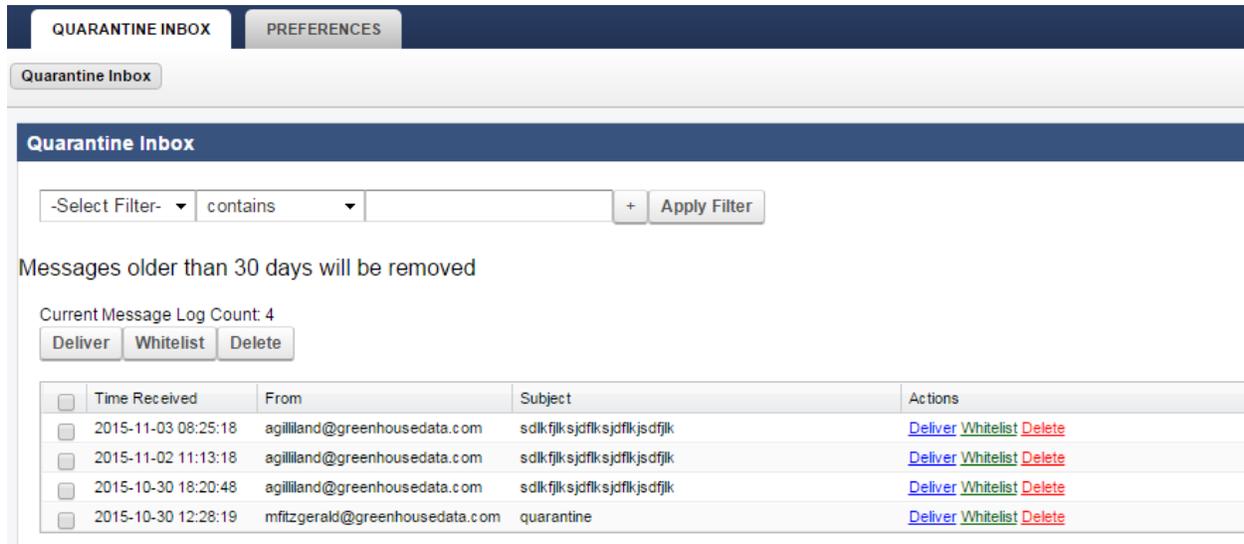
### Logging into the Quarantine Interface

To log into your quarantine interface:

- Click the link provided at the bottom of the Quarantine Summary Report (displayed above). The login page appears.
- Enter your hosted email address and password, and click Login.
- Access it directly via <https://filter.greenhousedata.com>

## Using your 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. Clicking on an email displays the message.



The screenshot shows the 'Quarantine Inbox' interface. At the top, there are tabs for 'QUARANTINE INBOX' and 'PREFERENCES'. Below the tabs, there is a 'Quarantine Inbox' header and a filter section with a dropdown menu set to 'contains' and an 'Apply Filter' button. A message is highlighted in blue. Below the message list, there is a 'Current Message Log Count: 4' and buttons for 'Deliver', 'Whitelist', and 'Delete'. The message list has the following data:

<input type="checkbox"/>	Time Received	From	Subject	Actions
<input type="checkbox"/>	2015-11-03 08:25:18	agilliland@greenhousedata.com	sdlkfjksjdfkjsdfkjsdfjk	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	2015-11-02 11:13:18	agilliland@greenhousedata.com	sdlkfjksjdfkjsdfkjsdfjk	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	2015-10-30 18:20:48	agilliland@greenhousedata.com	sdlkfjksjdfkjsdfkjsdfjk	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>
<input type="checkbox"/>	2015-10-30 12:28:19	mfitzgerald@greenhousedata.com	quarantine	<a href="#">Deliver</a> <a href="#">Whitelist</a> <a href="#">Delete</a>

The following table describes the actions you can perform from this page.

Action	Description
Deliver	<p>Delivers the selected message to your inbox.</p> <p>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 Spam Firewall delivers a message, it is removed from your quarantine list.</p>
Whitelist	<p>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.</p> <p>The Spam Firewall adds the sending email address exactly as it appears in the message to your personal whitelist.</p> <p><b>Note:</b> Some commercial mailings may come from one of several servers such as mail3.abcbank.com, and a subsequent message may come from mail2.abcbank.com.</p>

Delete	Deletes the selected message from your quarantine list. The main reason to delete messages is to help you keep track of which quarantine messages you have reviewed. You cannot recover messages you have deleted.
Classify as Not Spam	Classifies the selected message as not spam.  <b>Note:</b> Some bulk commercial email may be considered useful by some users and spam by others. For this reason, classifying such messages may not be very effective because users may counteract each other's classification. 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 blocklist (if you prefer not to receive them).
Classify as Spam	Classifies the selected message as spam.

### Changing Your User Preferences

After logging into your quarantine interface, depending on your account permissions, you can use the PREFERENCES tab to modify your quarantine and spam settings, and manage your whitelist and blocklist.

### Changing Your Quarantine Settings

The following table describes the quarantine settings you can change from the PREFERENCES > Quarantine Settings page, depending on how the administrator has configured your account:

Quarantine Setting	Description
Enable Quarantine	Whether the Barracuda Spam Firewall quarantines your messages.  If you select Yes, the Barracuda Spam Firewall does not deliver quarantined messages to your general email inbox, but you can view these messages from the quarantine interface and quarantine summary reports.  If you select No, all messages that would have been quarantined for you are delivered to your general email inbox with the subject line prefixed with [QUAR]:.

Notification Interval	The frequency the Spam Firewall sends you quarantine summary reports. The default is daily. The Spam Firewall only sends quarantine summary reports when one or more of your emails have been quarantined. If you select Never, you can still view your quarantined messages from the quarantine interface, but you will not receive quarantine summary reports.
Notification Address	The email address the Spam Firewall should use to deliver your quarantine summary report. Leave this field blank to use the email address associated with your user account.
Default Language	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 Spam Firewall are in UTF8 encoding.

### [Adding Email Addresses and Domains to Your Whitelist and Blocklist](#)

The PREFERENCES > Whitelist/Blocklist page lets you specify email addresses and domains from which you do or do not want to receive emails.

List Type	Description
Whitelist	The list of email addresses or domains from which you always wish to receive messages. The only time the Barracuda Spam Firewall blocks a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blocklist	The list of senders from whom you never want to receive messages. The Spam Firewall immediately discards messages from senders on your blocklist. These messages are not tagged or quarantined and cannot be recovered.  The sender does not receive a notice that the message was deleted, and neither do you. The only time a blocklisted email address is delivered is if the same email address also appears in your whitelist.

To whitelist senders or to add senders to your blocklist, follow these steps:

1. Go to the PREFERENCES > Whitelist/Blocklist page.
2. A list of your existing whitelisted and blocklisted addresses appears on this page.
3. To delete a whitelist or a blocklist entry, click the trash can icon next to the address.
4. To add an entry, type an email address into the appropriate field and click the Add button.

When adding addresses to your whitelist and blocklist, note the following tips:

- If you enter a full email address, such as [johndoe@yahoo.com](mailto:johndoe@yahoo.com), just that user is specified. If you enter just a domain, such as yahoo.com, all users in that domain are specified.
- If you enter a domain such as greenhousedata.com, all subdomains are also included, such as support.greenhousedata.com and filter.greenhousedata.com.
- Mass mailings often come from domains that do not resemble the company's 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 mailing that you are trying to whitelist or blocklist to determine what to enter.

### **Changing the Language of the Quarantine Interface**

You can change the language of your quarantine interface by selecting a language from the dropdown menu in the upper right corner of the QUARANTINE INBOX and PREFERENCES tabs. Supported languages include Chinese, Japanese, Spanish, French, and others.

### **Changing your Spam Settings**

If you are receiving spam, you can update your personal preferences if the administrator has allowed.

1. Navigate to PREFERENCES > Spam Settings
2. Select No for Use Domain Defaults
3. Click Save
4. Update the Block and Quarantine levels

5. Click Save

## Microsoft Outlook Add-in for Classifying Messages

**Note:** The add-in is currently only available for operating systems running a Microsoft Operating System.

Instead of using your quarantine inbox to classify your email messages, you can download a client add-in that lets you classify messages from your MS Outlook application.

### Downloading the Add-in

To download and install the client add-in that is needed to classify messages from Microsoft Outlook:

1. Go to the login page of the administration interface and click the link below the login information, as shown in the following figure:

Figure 2. The login page lets you download the client add-in



2. After clicking the link, you'll see a popup prompting you to save the executable file BsfOutlookAddIn.exe. Click Save File.
3. Close Microsoft Outlook on your system.
4. Run the file and follow the instructions in the setup wizard to install the add-in on your local system or network.
5. Start Microsoft Outlook.

### **Using the Microsoft Outlook Add-in**

#### Classifying Messages as Spam or Not-Spam

After downloading and installing the add-in, you can begin classifying messages using the green checkmark and the red X buttons in your Microsoft Outlook client. The green button marks messages as not spam and the red button marks messages as spam.



The Microsoft Outlook add-in is configured to automatically:

- Whitelist email addresses associated with sent messages and new contacts
- Move spam-declared messages to the Deleted Items folder in your mail client
- Whitelist the 'From:' email address within 'Not-Spam'-declared messages.

You can change the default behavior of the Outlook Add-in by going to the Tools menu in your MS Outlook client and selecting Options | Spam Firewall tab.