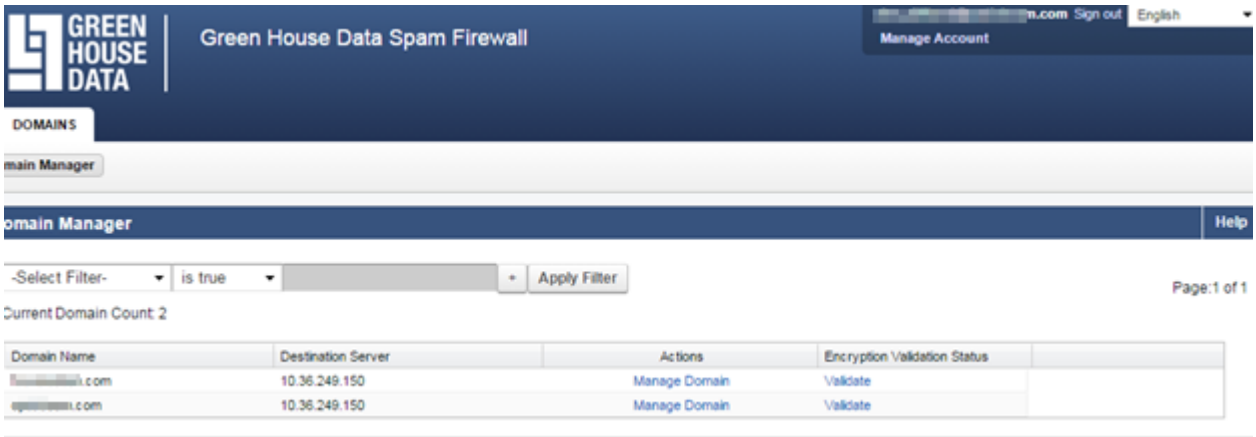
866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

Green House Data Spam Firewall Administrator Guide

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

Navigating the Web Interface

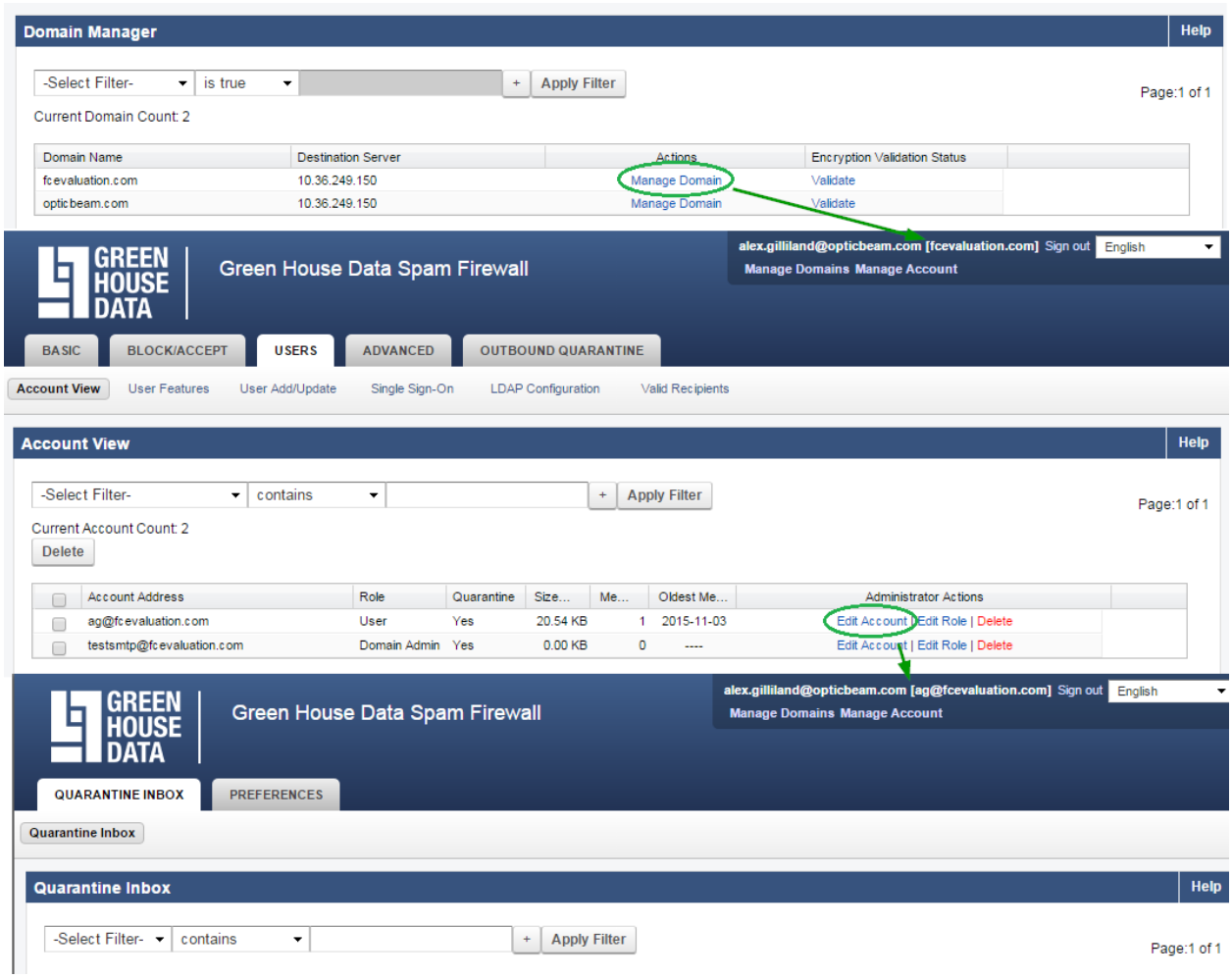
The links in the upper right corner of the web interface will indicate the login name and, if in the domain level scope, the domain being managed, or the name of the user account. The administrator can step into the domain-level scope of the web interface, which is what the Domain Admin and Helpdesk roles will see, from the DOMAINS page, by selecting a domain to manage. The DOMAINS page represents the "top level" of navigation of the web interface for Domain Admin and Helpdesk roles, as shown below. Clicking on Manage Domain enables managing domain-level settings and user accounts for that domain. The Domain Admin or Helpdesk role can "drill down" another level by selecting an account associated with that domain to edit from the USERS > Account View page (see Figure 2 below). Editing an account displays the quarantine inbox and preferences for the account, which is what the User role sees. Domain Admin and Helpdesk roles can also edit their own personal account settings and quarantine inboxes.



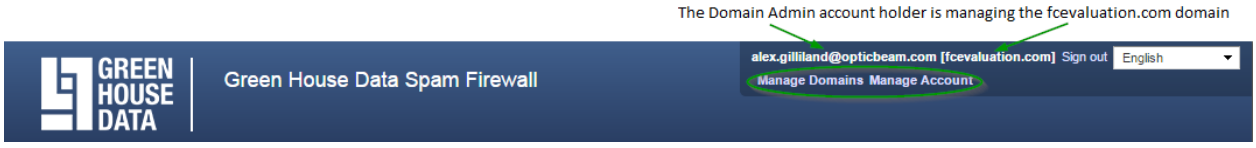
Clicking on Manage Domain enables the management of domain-level settings and user accounts for that domain. The Domain Admin or Helpdesk role can "drill down" another level by selecting an account associated with that domain to edit from the USERS > Account View page (see Figure 2 below). Editing an account displays the quarantine inbox and preferences for the account, which is what the User role sees. Domain Admin and Helpdesk roles can also edit their own personal account settings and quarantine inboxes.

How to Drill Down From the DOMAINS Page to Account Level

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007



The links in the upper-right enable the Domain Admin and Help Desk roles to return to the DOMAINS page or edit their own user account settings.



Message Logs

The domain Message Log displays email traffic that passes through the Spam Firewall for the domain. Under **Log Display** you can use the drop-down to select viewing Inbound, *Outbound*, or both. The page can be divided into 2 panes:

The Message List, which contains various details of the messages.

The Preview Pane, which is turned off by default, but can display the contents of a message on the right, left or bottom section of the page.

Note: If a message's subject or contents is not readable, the message may have multi-byte characters in it. Enable multi-byte or Unicode character encoding on your Web browser to see the message displayed correctly.

Actions to take with messages

Select one or more messages using the check boxes on the left-hand side of the log, then click the one of the action controls on the tool bar above the message list:

Deliver - attempt to deliver the selected message(s).

Categorize - Email Categorization allows for associating email that the user may, or may not, consider to be spam with a category that includes subscription-based emails, newsletters, monthly bills, shipping notices or other types of email that may not be unsolicited. Use the Categorize button to assign one or more messages in the Message Log to one of these categories:

Transactional Email - Order confirmations, bills, invoices, bank statements, delivery/shipping notices, and service-related surveys.

Corporate Email - Emails sent from an authenticated organization's Barracuda-verified mail server. Meant for general corporate communications only; no marketing or other mass mailings.

Marketing Materials - Promotional emails from companies such as Constant Contact.

Other - Use to enter a custom category. This action will simply update the category for that particular email message.

If the message was already categorized by the Email Categorization feature, that category will be shown in the Reason column; if you think the message belongs in a different category, then you can use the Categorize button and drop-down to switch categories. This action will submit the selected message(s) for recategorization to your selected category.

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

Deliver - Classify the selected message(s) as Not Spam and deliver the selected message(s).
Export - Export either selected or all messages to a CSV file:
Export Selected - Save selected messages to a CSV file. You will be prompted for a file name to save to your local desktop or network.
Export All - Save the entire message log to a CSV file. You will be prompted for a file name to save to your local desktop or network.
More Actions - Edit the whitelist or submit selected messages to Barracuda Central as follows:
Whitelist - Add the sending address(es) to the whitelist. Messages from whitelisted senders bypass spam scoring as well as all other blocklists. Virus scanning still applies.
Un-Whitelist - Remove the sending address(es) from the whitelist.
Submit to Barracuda Central As Spam - Classify the selected message(s) as Spam and send the selected message(s) to Barracuda Central for further analysis, a process which results in improved spam definitions and intent analysis.

Submit to Barracuda Central As Not Spam - Classify the selected message(s) as Not Spam and send the selected message(s) to Barracuda Central for further analysis, a process which results in improved spam definitions and intent analysis.

Whitelist an Email Address or Domain

This process outlines how to add a new domain or email address to your domain's whitelist.
Listed recipients' messages are not scored for spam but are still checked for viruses. Whitelisted recipients can also have some messages blocked due to IP controls.
Valid entries for the Email Address/Domain fields are domains, individual email addresses, or a pattern of email addresses. Entries in the Email Address/Domain field should be in one of the following formats:

- **mydomain.com** - Whitelists all email addresses that end with "@mydomain.com".
- **/mydomain.com/** - Whitelists all email address in all subdomains of mydomain.com, in addition to mydomain.com.
- **user@domain.com** - Whitelists only that one email address.
- **/list-.*@domain.com/** - Whitelists all email addresses in "domain.com" that start with "list-" (eg, list-reply@domain.com, list-notify@domain.com, list-bounce@domain.com, etc.)

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

How to:

1. Login to https://filter.greenhousedata.com
2. Select **Manage Domain**
3. Select the BLOCK/ACCEPT tab
4. Select Recipient Filters
5. Input the email address or domain per the formatting requirements within the ALLOWED EMAIL ADDRESSES AND DOMAINS field
6. Input a comment if required
7. Click Add

Add a Blocked Email Address or Domain

This process outlines how to add a new domain or email address to your domain's blocklist.

Add any email recipients to "blocklist". Listed recipients, with blocking selected, do not receive messages that are not whitelisted by IP, sender domain, or sender email address. If quarantine or tag is selected and these messages match in another spam filter layer, then these recipients' messages may still have their email blocked.

Valid entries for the Email Address/Domain fields are domains, individual email addresses, or a pattern of email addresses. Entries in the Email Address/Domain field should be in one of the following formats:

- mydomain.com - Whitelists all email addresses that end with "mydomain.com".
- /mydomain.com/ - Whitelists all email address in all subdomains of mydomain.com, in addition to mydomain.com.
- user@domain.com - Whitelists only that one email address.
- /list-.*@domain.com/ - Whitelists all email addresses in "domain.com" that start with "list-" (e.g., list-reply@domain.com, list-notify@domain.com, list-bounce@domain.com, etc.)

How to:

1. Login to https://filter.greenhousedata.com
2. Select Manage Domain
3. Select the BLOCK/ACCEPT tab
4. Select Recipient Filters

5. Input the email address or domain per the formatting requirements within the BLOCKED EMAIL ADDRESS AND DOMAINS field.
6. Input a comment if required
7. Select the action you wish to take: Block, Quarantine, Tag
8. Click Add

User Features

As a domain administrator, you're allowed to specify which features your users are allowed to modify within their preferences. To access these options, select the domain you wish to view and navigate to the USERS > User Features menu.

This outlines which features your users will be allowed to access when they log into their accounts. The settings chosen in the Default User Features section are applied to all new and existing user accounts that are created for this domain. To create exceptions for specific users, see the User Features Override section below. Click Save after making any updates.

The following default settings are available and will vary depending on what the administrator of this account has configured:

- Quarantine Enable/Disable - Controls the user's ability to enable/disable their personal quarantine inbox.
- Spam Scan Enable/Disable - Controls the user's ability to modify their personal spam settings.
- Notification Change - Controls the user's ability to change the frequency and language of their quarantine summary notifications.
- Whitelist/Blacklist - Controls the user's ability to add email addresses and domains into their personal whitelist and blacklist.
- Scoring Change - Controls the user's ability to change the spam scores at which their emails are tagged, quarantined, and blocked.

User Features Override

Specify which features the users for this domain will be allowed to access from their per-user quarantine account areas.

- User Accounts - Indicate user accounts that already exist for this domain for which you'd like to override settings. Enter one or more email addresses that you wish to change in the User Account(s) list box, select the options you wish to modify and click Save.

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

- Quarantine Enable/Disable - Controls the user's ability to enable/disable their personal quarantine inbox.
- Spam Scan Enable/Disable - Controls the user's ability to modify their personal spam settings.
- Notification Change - Controls the user's ability to change the frequency and language of their quarantine summary notifications.
- Whitelist/Blacklist - Controls the user's ability to add email addresses and domains into their personal whitelist and blacklist.
- Scoring Change - Controls the user's ability to change the spam scores at which their emails are tagged, quarantined, and blocked.

Note: With per-user quarantine enabled, if user features are disabled or if per-user quarantine is later disabled, account holders will lose previously configured per-user settings. For example, if an account holder has created a whitelist and blacklist in his/her account and the administrator disables the whitelist/blacklist feature or disables per-user quarantine, the account holder's whitelist/blacklist will be removed and cannot be restored.

Custom Spam Levels

Spam scoring limits can be set on a per-domain basis, as well as a per-user user basis. It is recommended to keep spam scanning enabled for all your domains by keeping the setting for Spam Scan Enabled set to Yes. To access the custom spam level options, select the domain you wish to view and navigate to BASIC > Spam Checking menu.

WARNING:
If you set Spam Scan Enabled to No, messages for user accounts with this domain will NOT be assigned spam scores. Consequently, messages will not be blocked, quarantined or tagged due to spam score. Other checks, such as the Barracuda Real Time System (BRTS), will still be performed to provide fingerprint analysis, virus protection and intent analysis. k

To exempt messages from a particular domain from all scanning, you can whitelist the sending IP address from the BLOCK/ACCEPT > IP Filters page, or whitelist the domain from the BLOCK/ACCEPT > Sender Filters page. Whitelisting domains is NOT recommended as spammers can easily spoof a domain name.

Once a message has passed the initial Barracuda Spam Firewall block/accept filters, it is given a score that indicates its spam probability. This score ranges from 0 (definitely not spam) to 9 or greater (definitely spam). Based on this score, the Barracuda Spam Firewall can take one of the actions listed below for your domain.

Note: A setting of 10 for any of the settings below disables that option.

- Block - Messages scoring equal to or greater than the Block threshold are not delivered to the recipient.
- Quarantine - Messages scoring equal to or greater than the Quarantine threshold, but below the Block threshold are quarantined. Messages are sent to a designated mailbox (specified in the BASIC > Quarantine screen), or into Per-User quarantine (if available).
- Tag - Messages scoring equal to or greater than the Tag threshold, but below the Quarantine threshold are delivered to the sender. Tagged messages contain a subject line of the message with the text specified in the Subject Tag as defined at the global level.

Dashboards

Upon selecting a domain, you will see a Dashboard appear that shows **only** that appliance's inbound and outbound email in the statistics. In order to view both Dashboards, login to https://filter01.greenhousedata.com and https://filter02.greenhousedata.com.

Reports

The Spam Firewall has a variety of system reports that can help you keep track of such statistics as the top spam senders and the top viruses detected by the system.

Reports can be created for data collected on the domain level and only for that specific appliance. You can run reports and configure report settings from the **BASIC > Reports** page, and online help for that page includes a table listing all reports, the kind of data each report includes for inbound and/or outbound mail, and types of graphs available. In order to run reports against both the appliances, login to https://filter01.greenhousedata.com and https://filter02.greenhousedata.com and then, generate reports.

On demand reports can cover data for a specified date range, but generating a report to view instead of to send as an email can potentially consume excessive system resources on the Spam Firewall. For this reason, discretion should be used when deciding on the date range a given report is to cover. To minimize the impact of report generation on the Spam Firewall, reports of over 7 days in length can only be generated through email.

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

User Roles

The Spam Firewall has two different user roles, the Domain Admin role and Help Desk role. Currently, the Domain Admin role can only be assigned by Green House Data, but the Help Desk role can be assigned by a user with the Domain Admin role.

Help Desk

This role has user level permissions plus the ability to:

- Change or update user account settings in the domain(s) to which the helpdesk user is assigned, which includes user spam scoring, whitelist/blocklist, quarantine enable/disable, and notification settings.
- View the Message Log for the domain(s) managed and deliver quarantined messages. The Helpdesk role cannot, however, view the body of messages in the Message Log.
- Log into an account with lesser permissions and manage the associated quarantine inbox – mark as spam/not spam, deliver, whitelist or delete messages.
- View domain-level status and reports (with the exception of the daily False Positive and False Negative, which can only be generated at the global level by the administrator).

Editing Accounts and Assigning Roles

From the USERS > Account View page in the domain scope, the domain administrator can manage accounts for that domain. The administrator can edit account roles, delete invalid accounts as needed and change account passwords. The USERS > Account View page displays role types and whether or not each account has quarantine enabled.

Note that links in the upper right of the page always indicate the login name of the current account holder, the Log Off link and, if applicable, links to manage the system, domains or user accounts.

Clicking Edit Role brings up the Edit Role page and the account can be assigned the Helpdesk role and the domains they are allowed to manage.

866.995.3282
www.greenhousedata.com
340 Progress Circle
Cheyenne, WY 82007

Attachment Filtering

The Spam Firewall performs attachment filtering and archive (zip, rar, etc) at the global level for inbound and outbound mail. Emails with these attachments will be blocked and the attachment filters **cannot** be changed by domain administrators. The blocked attachments are listed below.

.ade	.bat	.crt	.hta	.jar	.mda	.mdz	.ops	.reg	.shs	.wsc
.adp	.chm	.csh	.htr	.js	.mdb	.msc	.pcd	.scf	.url	.wsf
.app	.cmd	.exe	.inf	.jse	.mde	.msi	.pif	.scr	.vb	.wsh
.asp	.com	.fxp	.ins	.ksh	.mdt	.msp	.prf	.sct	.vbe	
.bas	.cpl	.hlp	.isp	.lnk	.mdw	.mst	.prg	.shb	.vbs	