BARRACUDA
NETWORKS

Version 5.x

Barracuda Spam & Virus Firewall User's Guide

Barracuda Networks Inc.
3175 S. Winchester Blvd
Campbell, CA 95008
http://www.barracuda.com

Copyright

Copyright 2005-2012, Barracuda Networks
www.barracudanetworks.com
v5.x-120314-01-0314

All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice.

Trademarks

Barracuda Spam & Virus Firewall is a trademark of Barracuda Networks. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders.

Managing your Quarantine Inbox

This guide describes how you can check your quarantined messages, classify messages as spam and not spam, manage whitelisting and blacklisting email addresses, and modify your user preferences using the Barracuda Spam & Virus Firewall interface. Some features covered in this guide may not appear on your system, depending on your level of permissions as set by your administrator.

Receiving Messages from the Barracuda Spam & Virus Firewall

The Barracuda Spam & Virus Firewall sends you the following two types of messages:

- Greeting Message
- Spam Quarantine Summary Report

Greeting Message

The first time the Barracuda Spam & Virus Firewall quarantines an email intended for you, the system sends you a greeting message with a subject line of *User Quarantine Account Information*. The greeting message contains the following information:

> Welcome to the Barracuda Spam & Virus Firewall. 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: <*your email address*>
>
> Password: <*your default password*>
>
> Access your Spam Quarantine directly using the following link:
> http://<*barracuda system address or name*>:8000

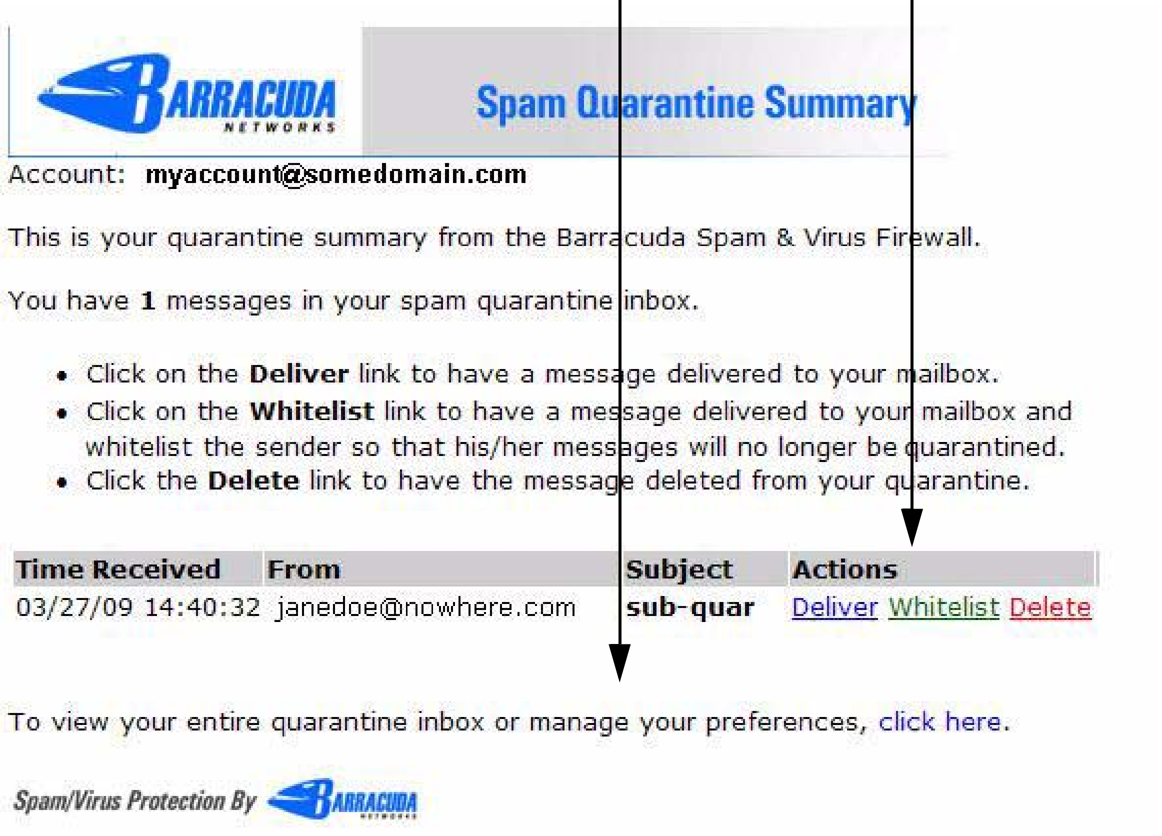
The Barracuda Spam & Virus Firewall automatically provides your login information (username and password) and the link to access the quarantine interface. You should save this email because future messages from the system do not contain your login information.

Quarantine Summary Report

The Barracuda Spam & Virus 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 that the quarantine summary report *only* goes out 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. Note also that 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.

The following figure shows an example of a quarantine summary report.



Click to access your quarantine interface to set preferences and classify messages

Select to deliver, whitelist or delete quarantined messages

Account: **myaccount@somedomain.com**

This is your quarantine summary from the Barracuda Spam & Virus Firewall.

You have **1** messages in your spam quarantine inbox.

- 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
03/27/09 14:40:32	janedoe@nowhere.com	**sub-quar**	Deliver Whitelist Delete

To view your entire quarantine inbox or manage your preferences, click here.

Using the Quarantine Interface

At the end of every quarantine summary report is a link to the quarantine interface where you can set additional preferences and classify messages as spam and 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 username and password, and click **Login**.

Your login information resides in the greeting message sent to you from the Barracuda Spam & Virus Firewall.

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 Barracuda Spam & Virus Firewall has a Bayesian learning engine which, if enabled by your administrator, 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 based on your whitelist and blacklist.

Note

To effectively "train" your Bayesian database, you must classify at least 200 *spam* messages and 200 *not spam* messages from your Quarantine Inbox, which will train the Bayesian database as to what word or phrase patterns that appear, perhaps multiple times, throughout a message you consider to be valid content or characteristic of spam. Continue to classify **an equal number** of each type of message as needed.

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

Action	Description
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 Barracuda Spam & Virus 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 Barracuda Spam & Virus Firewall adds the sending email address exactly as it appears in the message to your personal whitelist. Note that 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*. See the section on managing your whitelists and blacklists for tips on specifying whitelists with greater effectiveness.
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. *Note: 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 others' 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 blacklist (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 change your account password, modify your quarantine and spam settings, and manage your whitelist and blacklist.

Changing your Account Password

To change your account password, do one of the following:

- On the quarantine interface login page, click **Create New Password**, or

- After logging into your quarantine interface, go to **PREFERENCES > Password**. This option is not available if single sign on has been enabled via LDAP or Radius.

In the provided fields, enter your existing password and enter your new password twice. Click **Save Changes** when finished.

Note

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.

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 & Virus Firewall quarantines your messages. If you select **Yes**, the Barracuda Spam & Virus 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]:. The Barracuda Spam & Virus Firewall administrator can modify this prefix.
Notification Interval	The frequency the Barracuda Spam & Virus Firewall sends you quarantine summary reports. The default is daily. The Barracuda Spam & Virus 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 Barracuda Spam & Virus 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 Barracuda Spam & Virus Firewall are in UTF8 encoding.

Enabling and Disabling Spam Scanning of your Email

If you do not want the Barracuda Spam & Virus Firewall scanning your emails for spam content, you can disable spam filtering from the **PREFERENCES > Spam Settings** page. From this page you can also change the default spam scoring levels that determine when your emails are tagged, quarantined or blocked.

When the Barracuda Spam & Virus 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 Barracuda Spam & Virus Firewall either allows, quarantines, or blocks the message.

A setting of 10 for any setting disables that option.The following table describes the fields on the **PREFERENCES > Spam Settings** page.

Setting	Description
Spam Filter Enable/Disable	
Enable Spam Filtering	Select **Yes** for the Barracuda Spam & Virus Firewall to scan your emails for spam. Select **No** to have all your messages delivered to you without being scanned for spam.
Spam Scoring	
Use System Defaults	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.
Tag score	Messages with a score above this threshold, but below the quarantine threshold, are delivered to you with the word [BULK] added to the subject line. Any message with a score below this setting is automatically allowed. The default value is 3.5.
Quarantine score	Messages with a score above this threshold, but below the block threshold, are forwarded to your quarantine mailbox. The default setting is 10 (quarantine disabled). To enable the quarantine feature, this setting must have a value lower than the block threshold.
Block score	Messages with a score above this threshold are not delivered to your inbox. Depending on how the system is configured, the Barracuda Spam & Virus Firewall may notify you and the sender that a blocked message could not be delivered. The default value is 9.
Barracuda Bayesian Learning	
Reset Bayesian Database	Click **Reset** to remove your Bayesian rules learned by the Barracuda Spam & Virus Firewall from the point of installation. Use the Reset button on a regular basis to clear out old classifications of valid email versus spam to account for the fact that spam tactics change rapidly and the word and phrase patterns that appear in spam messages tend to change over time. Thus, by resetting your Bayesian database regularly and classifying 200 spam and not spam messages anew, you'll keep your Bayesian database refreshed such that it has the best chance of identifying spam with a very high level of accuracy.
Bayesian Database Backup	
Backup Bayesian Database	Click **Backup** to download a copy of your Bayesian database to your local system. This backup copy can then be uploaded to any Barracuda Spam & Virus Firewall, including this one, in the case of a corrupt Bayesian installation.
Restore Database	Click **Browse** to select the backup file containing your Bayesian database, and then click **Upload Now** to load the Bayesian settings to this Barracuda Spam & Virus Firewall. The backup file does not need to have originated from this Barracuda Spam & Virus Firewall, nor from the same user database.

Adding Email Addresses and Domains to Your Whitelist and Blacklist

The **PREFERENCES > Whitelist/Blacklist** 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 & Virus Firewall blocks a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blacklist	The list of senders from whom you never want to receive messages. The Barracuda Spam & Virus Firewall immediately discards messages from senders on your blacklist. 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 blacklisted email address is delivered is if the same email address also appears in your whitelist.

To whitelist or blacklist senders, follow these steps:

1. Go to the **PREFERENCES > Whitelist/Blacklist** page.
2. A list of your existing whitelisted and blacklisted addresses appears on this page.
3. To delete a whitelist or a blacklist 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.

Tips on specifying addresses

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

- If you enter a full email address, such as *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 *barracudanetworks.com*, all subdomains are also included, such as *support.barracudanetworks.com* and *test.barracudanetworks.com*.
- Mass mailings often come from domains that do not resemble the company’s Web site 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 blacklist 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 drop-down menu in the upper right corner of the **QUARANTINE INBOX** and **PREFERENCES** tabs. 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.

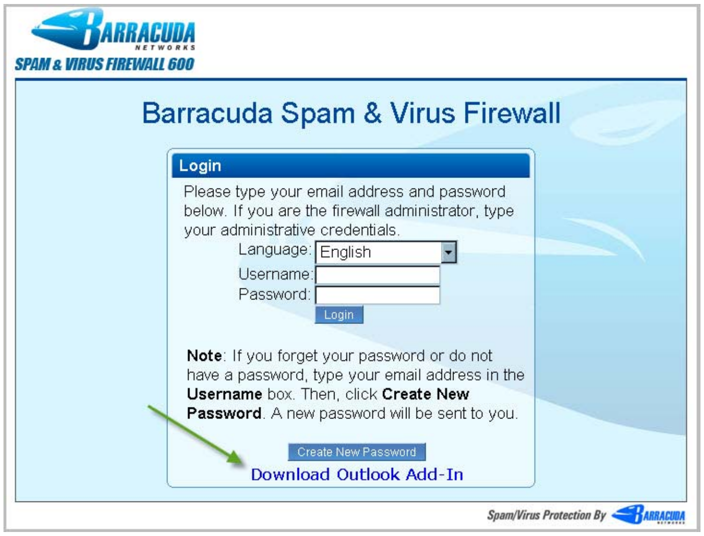
Using Microsoft Outlook and Lotus Notes to Classify Messages

Instead of using your quarantine inbox to classify your email messages, you can download a client plugin that lets you classify messages from your Microsoft Outlook or Lotus Notes application.

Your Barracuda Spam & Virus Firewall administrator may chose not to make this plugin available. If this is the case, you need to use your quarantine inbox to classify your messages.

Downloading the Client Plugin

To download the client plugin that is needed to classify messages from Microsoft Outlook or Lotus Notes, go to the login page of the administration interface and click the link below the login information, as shown in the following example:



Barracuda Spam & Virus Firewall

Login

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

Language: English

Username:

Password:

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.

BARRACUDA NETWORKS
SPAM & VIRUS FIREWALL 600
Login
Create New Password
Download Outlook Add-In
Spam/Virus Protection By BARRACUDA NETWORKS

If this link does not appear, then your Barracuda Spam & Virus Firewall administrator has configured the system to not make the plugin available and the next section will not apply to your configuration.

Using the Microsoft Outlook and Lotus Notes Plugins

After downloading and installing the plugin, you can begin classifying messages using these buttons in your Microsoft Outlook or Lotus Notes client: ✓ ✗. The first (green) button marks messages as not spam and the second (red) button marks messages as spam.

The Microsoft Outlook and Lotus Notes plugins are 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 Microsoft Outlook client and selecting **Options** | **Spam & Virus Firewall** tab.