Western University Spam Firewall User's Guide

The Western University Spam Firewall sits between the Internet and the internal mail servers and is designed to filter messages for spam and viruses. Since the firewall is part of Western University's mail services, there is no need to install any software on your local system.

Typically there is very little interaction with the spam firewall. This guide describes how to check quarantined messages, classify messages as spam and not spam, and modify preferences. It is broken down in the following topics:

- Receiving messages from the spam firewall
- Using the quarantine interface
- Changing User Preferences

Receiving Messages From the Spam Firewall

The spam firewall sends the following two types of messages:

- Greeting Message
- Spam Quarantine Summary Report

Greeting Message

The first time the spam firewall quarantines an e-mail intended for you, the system sends you a greeting message with the subject "User Quarantine Account Information". The greeting message contains the following information:

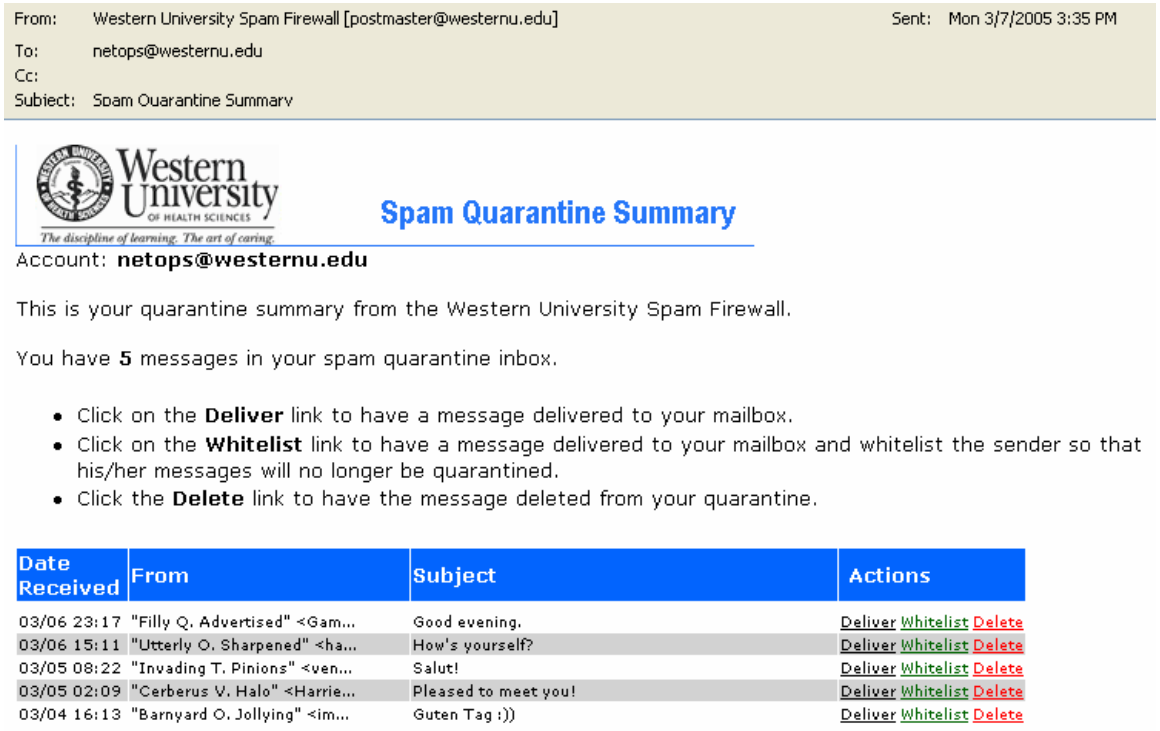
> Welcome to the Western University Spam Firewall. This message contains the information you will need to access your Spam Quarantine and Preferences.
>
> Your account has been set to the following username and password:
> Username: <your e-mail address>
>
> Access your Spam Quarantine directly using the following link:
> http://smtpgate.westernu.edu

The spam firewall automatically provides your username, which is your e-mail address and the link to access the quarantine interface. Your password is your e-mail password. You should save this email because future messages from the system do not contain your login information.

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. Your whitelist is people who you always want to receive mail from. It is discussed in more detail further in this document.

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



From: Western University Spam Firewall [postmaster@westernu.edu] Sent: Mon 3/7/2005 3:35 PM
To: netops@westernu.edu
Cc:
Subject: Spam Quarantine Summary

Western University of Health Sciences
The discipline of learning. The art of caring.

Spam Quarantine Summary

Account: **netops@westernu.edu**

This is your quarantine summary from the Western University Spam Firewall.

You have **5** 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.

Date Received	From	Subject	Actions
03/06 23:17	"Filly Q. Advertised" <Gam...	Good evening.	Deliver Whitelist Delete
03/06 15:11	"Utterly O. Sharpened" <ha...	How's yourself?	Deliver Whitelist Delete
03/05 08:22	"Invading T. Pinions" <ven...	Salut!	Deliver Whitelist Delete
03/05 02:09	"Cerberus V. Halo" <Harrie...	Pleased to meet you!	Deliver Whitelist Delete
03/04 16:13	"Barnyard O. Jollying" <im...	Guten Tag :))	Deliver Whitelist Delete

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 the quarantine interface:

1. Click the link at the bottom of the Quarantine Summary report or enter http://smtpgate.westernu.edu into your web browser.
2. Enter your username and password and click **Login**. Your username is your e-mail address and your password is your e-mail password.

Managing 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.

The 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 based on your whitelist and blacklist.

Clicking on an e-mail displays the message.

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

Action	Description
Deliver	Delivers the selected message to your standard e-mail 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 spam firewall delivers a message, it is removed from the 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 file type. The spam firewall adds the sending e-mail address exactly as it appears in the message to your personal whitelist. *Note: 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 and delivers the message to your standard e-mail inbox. *Note: Some bulk commercial mail 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 mail, 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 and deletes it from your quarantine.

Changing your User Preferences

After logging into the quarantine interface, select the PREFERENCES tab to change your account password, modify your quarantine and spam settings, and manage your whitelist and blacklist.

Changing your Account Password

Your password is tied to your e-mail account. If you change your e-mail password your Spam Firewall Password will change too. Your e-mail password can be changed using the web mail application located at https://mail.westernu.edu. Once logged on click on Options then select Change Password.

Changing Your Quarantine Settings

The following table describes the quarantine settings you can change from the PREFERENCES-->Quarantine Settings page.

Quarantine Setting	Description
Enable Quarantine	Whether the spam firewall quarantines your messages. If you select **Yes**, the spam firewall does not deliver quarantined messages to your general e-mail 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 e-mail inbox with the subject 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 e-mails 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 e-mail address the spam firewall should use to deliver your quarantine summary report. Leave this field blank to use your default Western University address.

Enabling and Disabling Spam Scanning of your E-mail

If you do not want the spam firewall scanning your emails for spam content, you can disable spam filtering from the PREFERENCES-->Spam Settings page.

Adding E-mail Address 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	A list of e-mail addresses or domains from which you always whish to receive messages. The only time the spam firewall filters a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blacklist	A list of senders whom you never want to receive messages. The spam 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.

To whitelist or blacklist senders, follow these steps:

1. Go to the PREFERENCES-->Whitelist/Blacklist page.
2. To add a whitelist or blacklist entry, type the e-mail address into the appropriate field and click the corresponding **Add** button.
3. To delete a whitelist of blacklist enrty, click on the trashcan icon next to the address.

Tips on specifying addresses

When adding addresses to your whitelists 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 *abcbank.com*, all subdomains are also included, such as *support.abcbank.com* and *accounts.abcbank.com*.

- Internal e-mail from Western University is not filtered by the spam firewall and will not be affected by any blacklist or whitelist entries.