GWGuardian™
ADVANCED MESSAGING FIREWALL

# GWGuardian WebQuarantine

## Reference Guide

provided by the

Northern Nishnawbe Education Council

Technical Services Department

Version 1.0

# GWGuardian WebQuarantine User Guide

## About GWGuardian & WebQuarantine

The GWGuardian WebQuarantine is a web application that allows you to access and manage your quarantined email from anywhere in the world through the Internet. This guide will walk you through each step of the tasks you can perform through the web interface.

The NNEC GWGuardian WebQuarantine is located at:

http://mail.nnec.on.ca/quarantine/Login.aspx

Alternatively, if you are still using an @dfc.nnec.on.ca email address your GWGuardian WebQuarantine is located at:

http://mail.dfc.nnec.on.ca/quarantine/Login.aspx

Current links will always be available at:

http://mail.nnec.on.ca/

## Technical Support

If you have a technical support question, please consult the Technical Services Department www.nnec.on.ca/tech or call (807) 737-1371, and a member of our technical support team will contact you as soon as possible during regular business hours.

## How to Use This Guide

This guide is intended to complement the GWGuardian WebQuarantine application, and introduces concepts in the same order as the layout of the console.

# Table of Contents

# 1.0 Starting a GWGuardian WebQuarantine Session

GWGuardian WebQuarantine requires you to identity yourself as a user with an email address and password. From the login screen you can also change the language of the display.

## 1.1 Logging In

To start a new mail session:

1 Open your Internet browser and go to the URL provided by your Administrator for your GWGuardian login page. These addresses are located at the beginning of this guide.
2 Enter your email address and password.
3 Click Login.

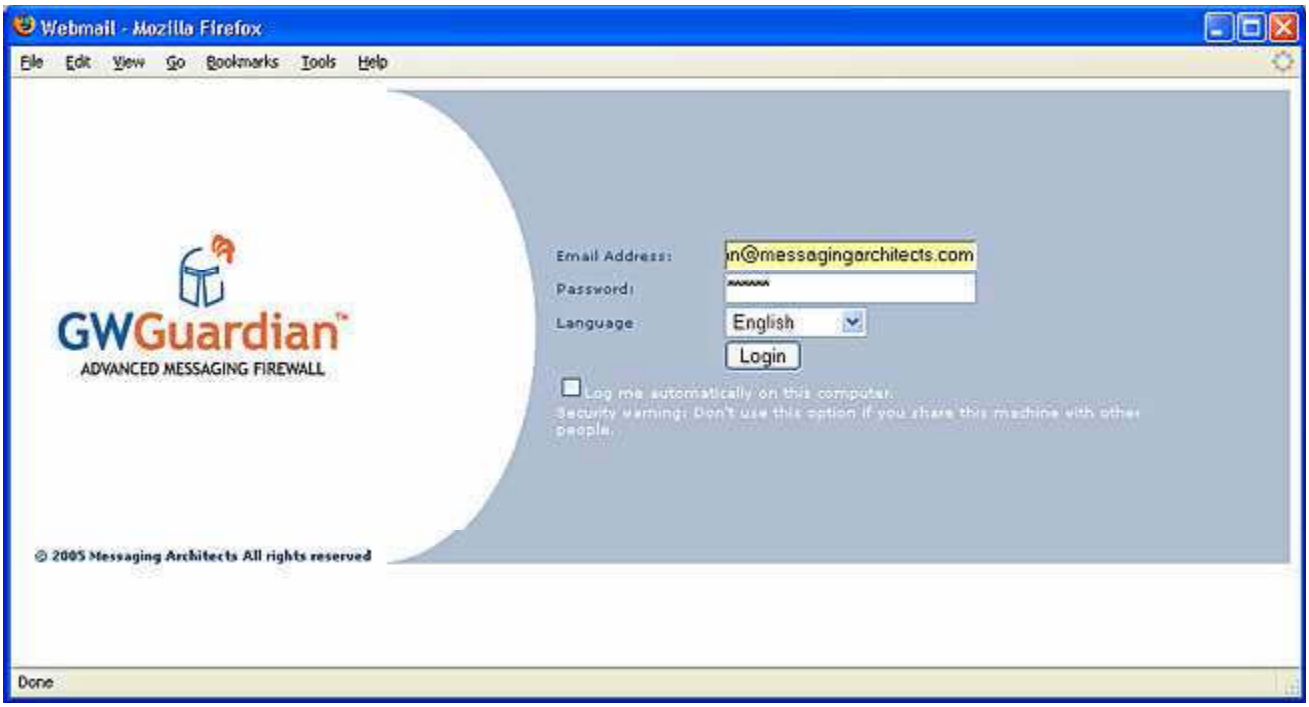


Figure 1: GWGuardian WebQuarantine Login Screen

# 2.0 The GWGuardian WebQuarantine Interface

Use the navigation bar at the top of every screen to go to the corresponding window.

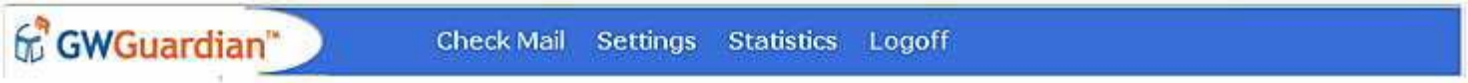


Figure 2: Navigation Bar

**Check Mail**: Click Check Mail to display your quarantine and see if any new mail has been quarantined since you logged in.

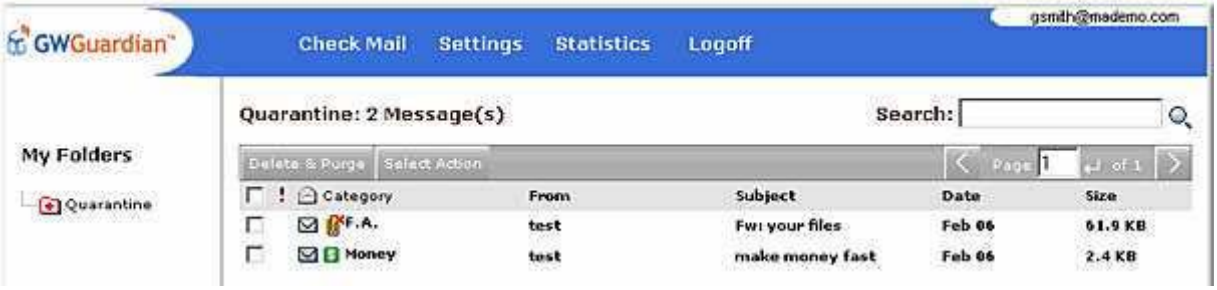


Figure 3: GWGuardian WebQuarantine

**Searching Quarantine**: You can search email in your Quarantine across the following criteria:

- Subject
- From
- To
- Cc

Enter your search criteria in the **Search** text box, and then click the magnifying glass to begin your search.

**Reviewing Quarantine**: You can review your quarantined email directly from your quarantine by double-clicking the message to open and review it. In the message window, click **Full header** to display full header details. Click **Partial header** to display basic header information. You can also print the message, add the sender to your Trusted Senders List, add the sender to your Blocked Senders List, or navigate through messages in your quarantine. Choose **Select Action** for a list of available message actions. Click **Close** to return to your mailbox.


Figure 4: Message Window

**Settings**: The settings menu provides access to the many configuration options you have for how GWGuardian WebQuarantine manages your mail account. These configuration options include personal settings (password, account identification options, etc.), email filtering and sorting options, auto-reply options, external account access, and the creation of aliases for your account.

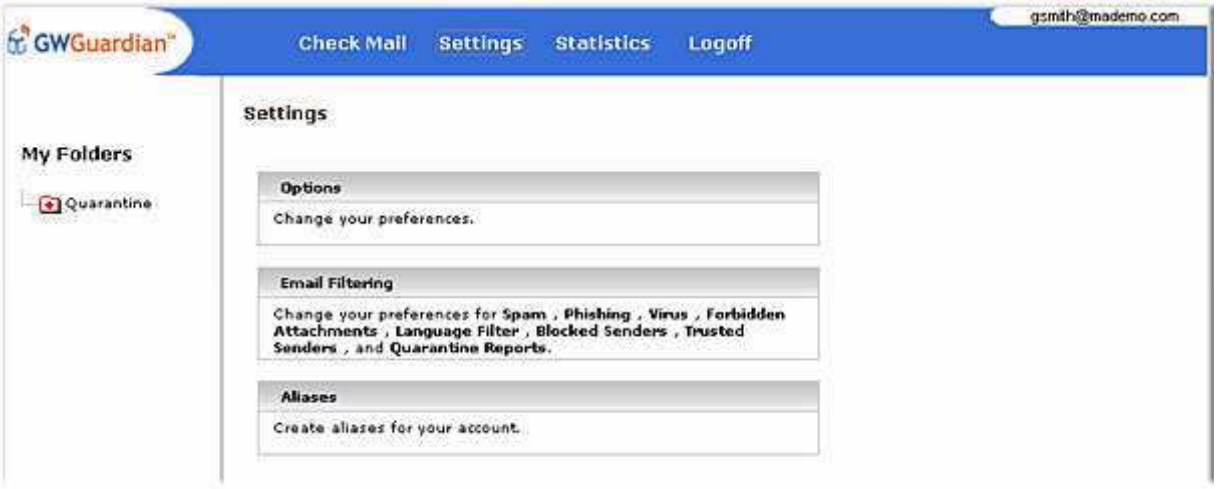


Figure 5: Settings Menu

**Statistics**: The Statistics page displays statistics of your email account's activity. On the Statistics page, you can choose to view:

- A histogram of daily, weekly, monthly, or yearly statistics for the amount of legitimate email versus the amount of spam, email with forbidden attachments or viruses that have been sent to your mailbox.
- A daily, weekly, monthly, or yearly comparison between the different types of spam received.

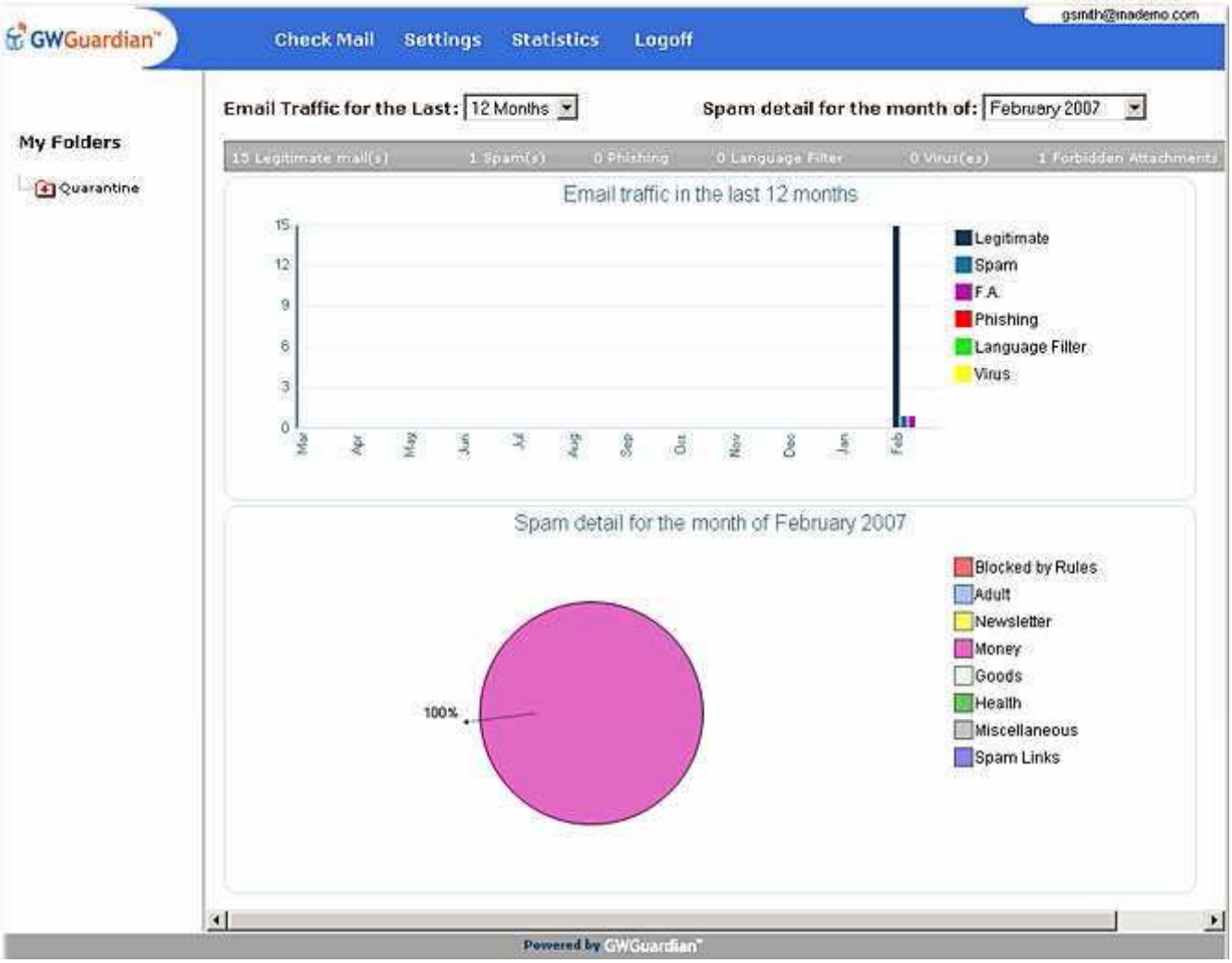


Figure 6: Mailbox Statistics

The Statistics page does not display statistics for email sent internally, only external email that is processed through GWGuardian.

**Paging**: For folders that contain many messages, the paging feature allows you to display portions of the message list. The number of messages displayed on each page is configurable, but the default is 15 messages per page.


Figure 7: Paging Feature

**Navigating List Pages**: Select the list page you want to go to by clicking the arrows representing the Next or Previous page.

# 3.0 Quarantine

The Quarantine feature filters incoming email to determine whether they are spam or contain forbidden attachments and/or viruses.

The Quarantine View shows you the name of the sender, the subject of the messages and their attachments. You can also open an email in Quarantine and view its contents; however, you cannot view attachments in Quarantine. Messages in Quarantine can be released to your Inbox or deleted and purged from the system.

Email containing attachments that have viruses (or which are attachments that are considered dangerous by the system) cannot be released to your Inbox. Only email considered to be spam can be released from Quarantine.

## 3.1 Quarantine Categories

There are 8 categories of mail that can be filtered into Quarantine:


Figure 8: Quarantine Categories

The other categories of email sent to Quarantine are **Virus** or **Forbidden Attachment**. A forbidden attachment is a type of file that your System Administrator identifies as being a possible threat.

## 3.2 False Positives

A False Positive is a message that is identified incorrectly as one of the filtered categories. False positive messages can be released to your Inbox and you can add the email address or domain to your Trusted Senders List so that messages from this source in future will not be quarantined (unless the system detects a virus).

**Releasing Email from the Quarantine**:

1. Select the message you want to release, and then use the **Select Action** dropdown menu to choose an action.

2. Select either:
   - **Release messages** to just release the message to your Inbox.
   - **Release and Report messages as Legitimate email** to release the message to your Inbox as well as send a copy of it for pattern analysis.

## 3.3 Quarantine Reports

GWGuardian WebQuarantine can be configured to email you Quarantine Reports at regular intervals (typically once a day). You will only receive a Quarantine Report email if you have messages in Quarantine at the time the system generates the reports.

A Quarantine report shows you Information about the email that has been sent to Quarantine since your last report, as well as information about the email that is currently in Quarantine.

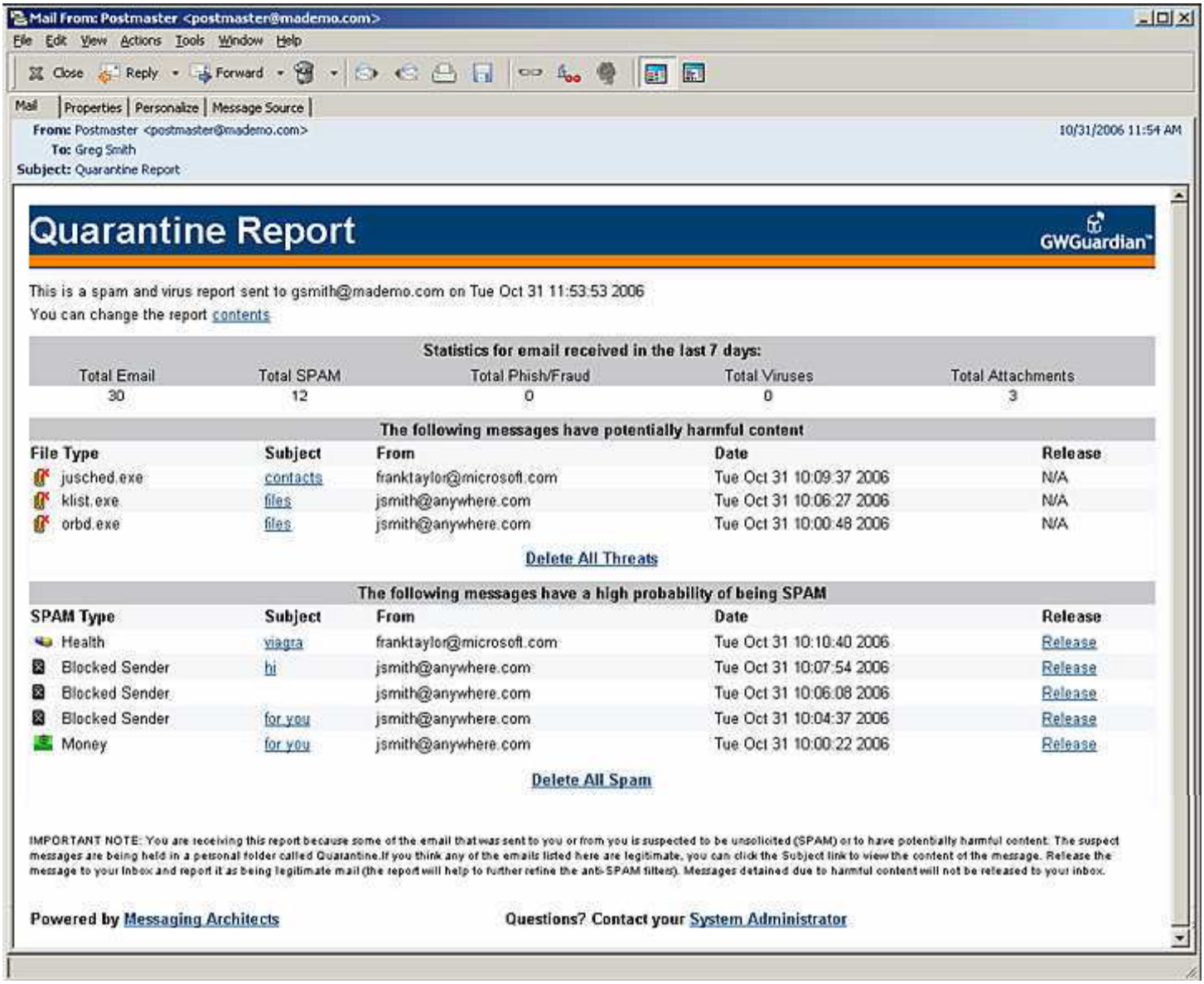


Figure 9: Quarantine Report

**Releasing or Deleting Quarantined Email from the Quarantine Report**:

1. Open your Quarantine Report Email View.

2. Click the hyperlinks in the report to either release or delete the quarantined message.
   - Release email to Inbox.
   - Release email and report email as a false positive.
   - Delete quarantined message.

# 4.0 Settings

Select **Settings** from the navigation bar to access the pages where you can set preferences for your account's quarantine rules.

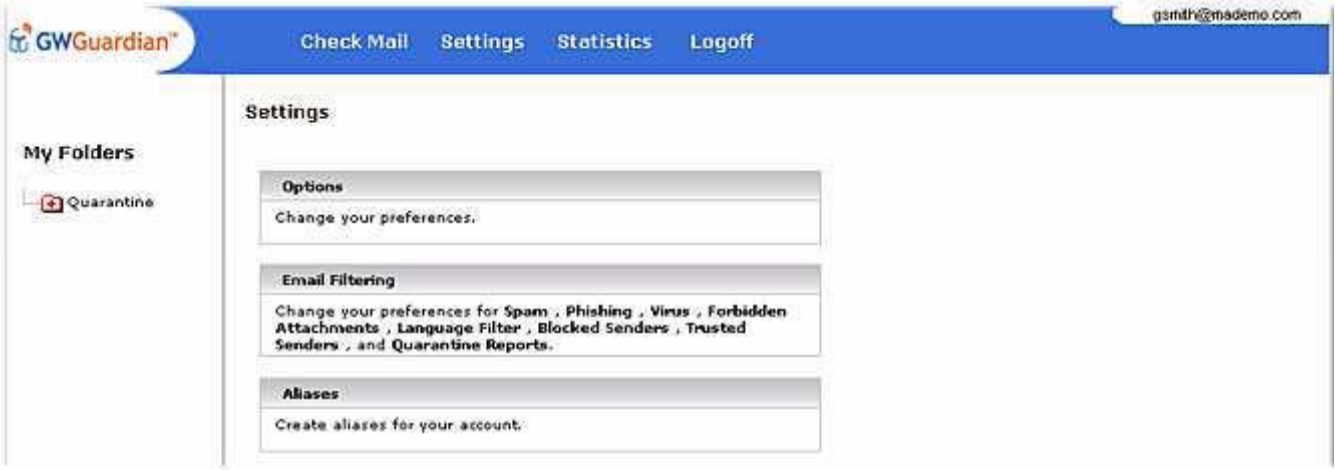


Figure 10: Settings Menu

## 4.1 Options

Go to **Settings > Options** to set list display preferences.

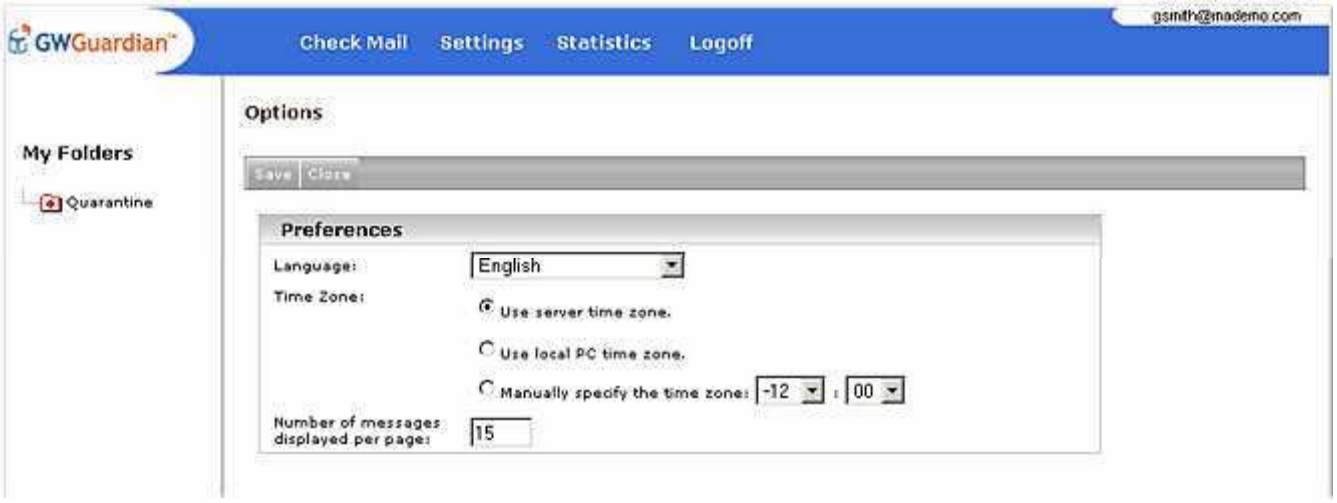


Figure 11: Options Menu

**Specify the number of messages to be displayed in lists**:

1 Choose the language you want to use.
2 Choose the time zone you want to use for message timestamps.
3 Enter the number of messages you want to view on each page.
4 Click **Save**.

## 4.2 Email Filtering

You can turn on or off, or modify the severity of the filters used to check incoming email for spam, viruses, and forbidden attachments.

It is possible that your Administrator has made these settings on your behalf and locked them. In this situation, you will not be able to modify the settings and you must contact your Administrator if you want to make changes.

Choose **Settings > Email Filtering** to do any of the following procedures.

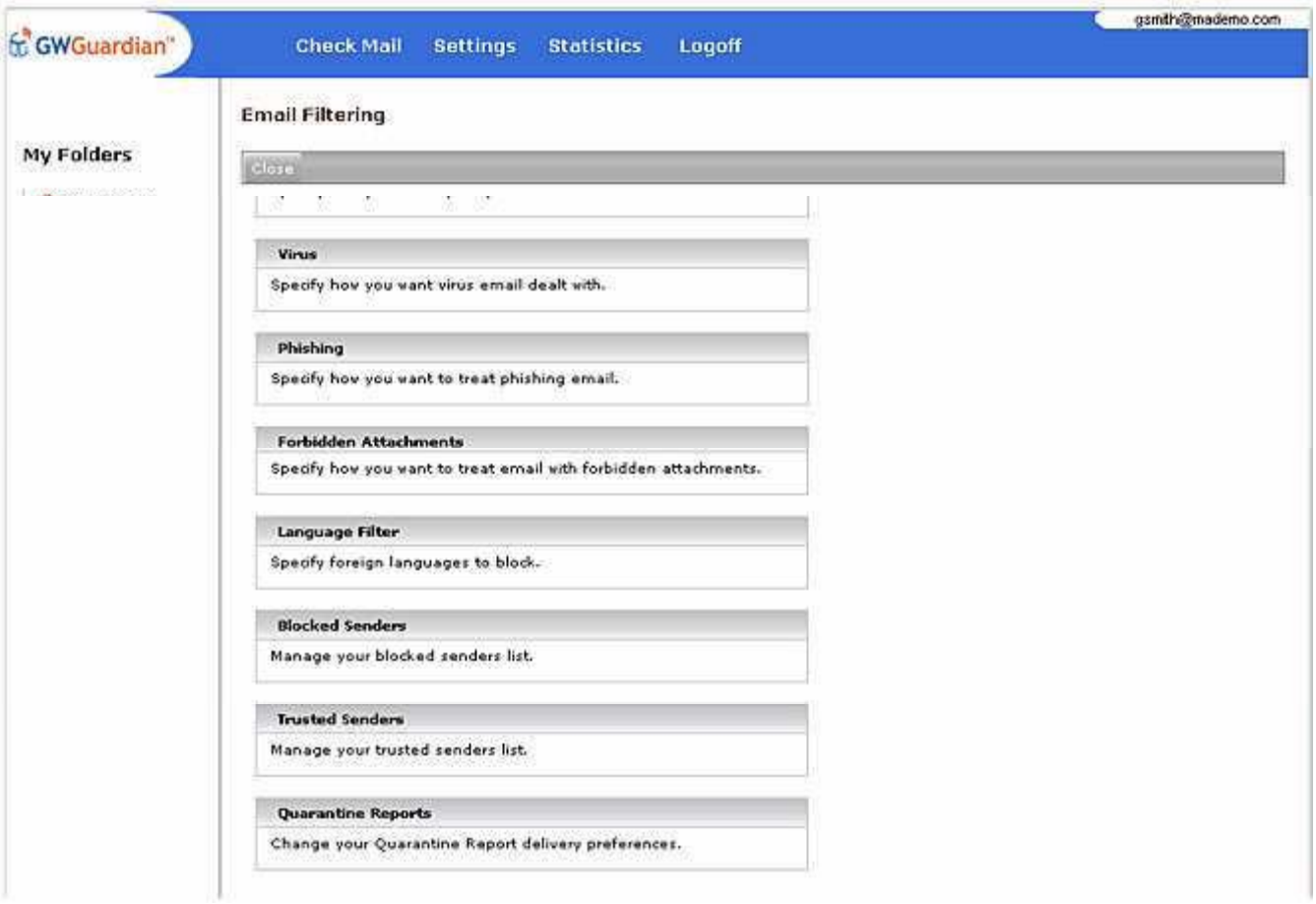


Figure 12: Filtering Menu

### 4.2.1 Modifying your Spam Filter Settings

To specify what you want to happen to email identified as spam, choose Settings **> Email filtering > Spam:**

1. Choose either:

- Delete message immediately (you will never be able to review messages identified as spam).
- Block message into Quarantine (you will be able to release the message to your Inbox).
- Tag messages as spam but allow them all through to your Inbox.

2. Click **Save**.

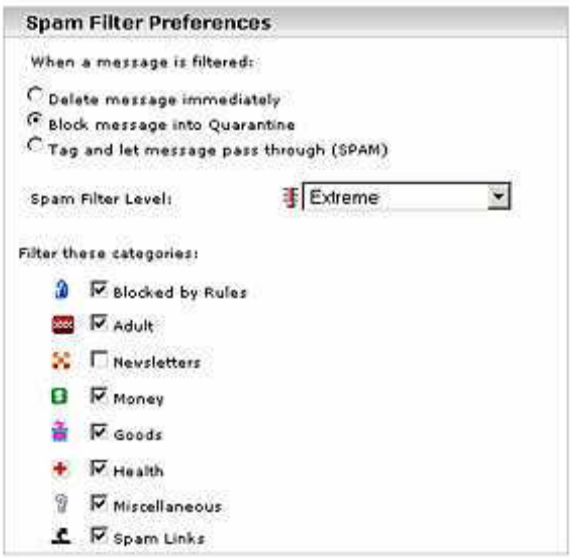


Figure 13: Spam Filter Preferences

**To choose the level of Spam Filtering**:

1. Choose either:

- **Disabled** (no spam filtering).
- **Normal** (basic spam filtering).
- **Strong** (advanced spam filtering used).
- **Extreme** (can occasionally result in false positives).

2. Click **Save**.

## 4.2.2 Modifying your Virus Filter Settings

**To specify what you want to happen to email with viruses, choose Settings > Email filtering > Virus**:

1. Choose either:

- Delete message immediately (you will never be able to review messages that have viruses).
- Block message into Quarantine (you will be able to read the message, but not to open any attachment that has a virus).

2. Click **Save**.

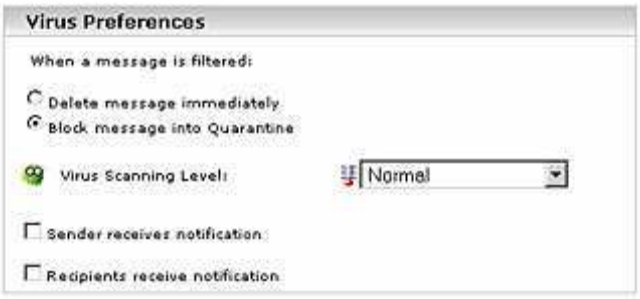


Figure 14: Virus Preferences

It is possible that your Administrator has made these settings on your behalf and locked them. In this situation, you will not be able to modify the settings and you must contact your Administrator if you want to make changes.

**To turn Virus Filtering on or off**:

1. Choose either:
- **Normal** to turn virus filtering on.
- **Disabled** to turn virus filtering off.

2. Click Save.

**To modify Virus notification settings**:

1. Choose either:

- **Sender receives notification** to let a sender know that they sent a virus.
- **Recipient receives a notification** to let a recipient know that they have email in Quarantine with a virus.

2. Click **Save**.

## 4.2.3 Modifying your Phishing Filter Settings

**To specify what you want to happen to email identified as phishing, choose Settings > Email filtering > Phishing:**

1. Choose either:

- Delete message immediately (you will never be able to review messages identified as phishing).
- Block message into Quarantine (you will be able to release the message to your inbox).

2. Click **Save**.


Figure 15: Phishing Preferences

**To choose the level of Phishing Filtering:**

1. Choose either:

- **Disabled** (no phishing filtering).
- **Normal** (basic phishing filtering).
- **Strong** (advanced phishing filtering used).
- **Extreme** (can occasionally result in false positives).

2. Click **Save**.

### 4.2.4 Forbidden Attachments

Forbidden Attachments are defined by the System Administrator. Typically a forbidden attachment is a file type that is deemed to pose an unnecessary risk to the system, such as a file with a ".vbs" extension which is commonly used to spread computer viruses via email.

Forbidden attachment settings are modified in the same way that your spam and virus settings are treated, which are explained in the previous section.

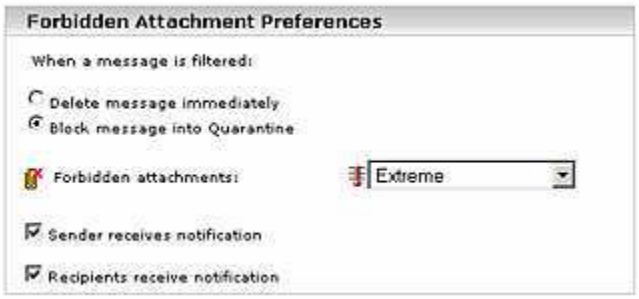


Figure 16: Forbidden Attachment Preferences

In GWGuardian WebQuarantine, you can change your preferences for the level of restriction for attachments, but you cannot define which file types are to be considered forbidden for each level (i.e., normal, strong, and extreme) of restriction. Please contact your System Administrator if you would like more information about forbidden file types.

## 4.2.5 Language Filter Preferences

To specify what you want to happen to email that contains foreign language content, choose Settings > Email filtering > Language Filter:

1. Choose either:

- Delete message immediately (you will never be able to review messages containing foreign language content).
- Block message into Quarantine (you will be able to release the message to your Inbox).
- Tag messages as containing foreign language content but allow them all through to your In box.

2. Click **Save**.

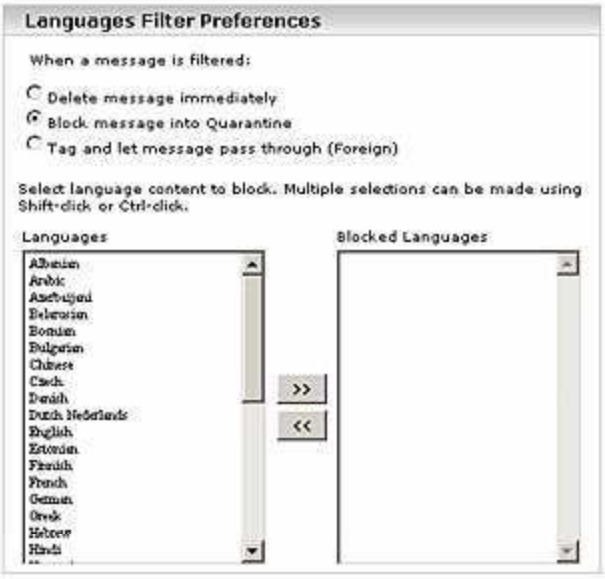


Figure 17: Language Filter Preferences

## 4.2.6 Blocked Senders and Trusted Senders

If you are viewing an email that has been quarantined, it is easy for you to correctly classify the address of the sender.

### Adding Addresses to your Trusted List:

1 Select a message and open the message view.
2 Click **Trusted List** to add the sender's address to your Trusted Senders List. (Email from this sender will always be sent to your Inbox.)
3 You can also add email addresses and domains to your Trusted Senders List by choosing **Settings > Email Filtering > Trusted Senders**.

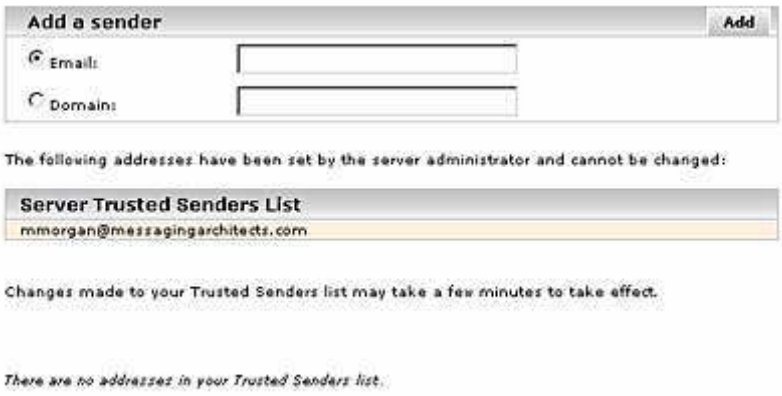


Figure 18: Trusted Senders List

### Adding Addresses to your Blocked List:

1 Select a message and open the message view.
2 Click **Block** to add this email address to your Blocked Senders List. (Email from this address will always be automatically quarantined or deleted, depending on the settings the System Administrator has chosen for the mail server.)
3 You can also add email addresses and domains to your Blocked List by choosing **Settings > Email Filtering > Blocked Senders**.

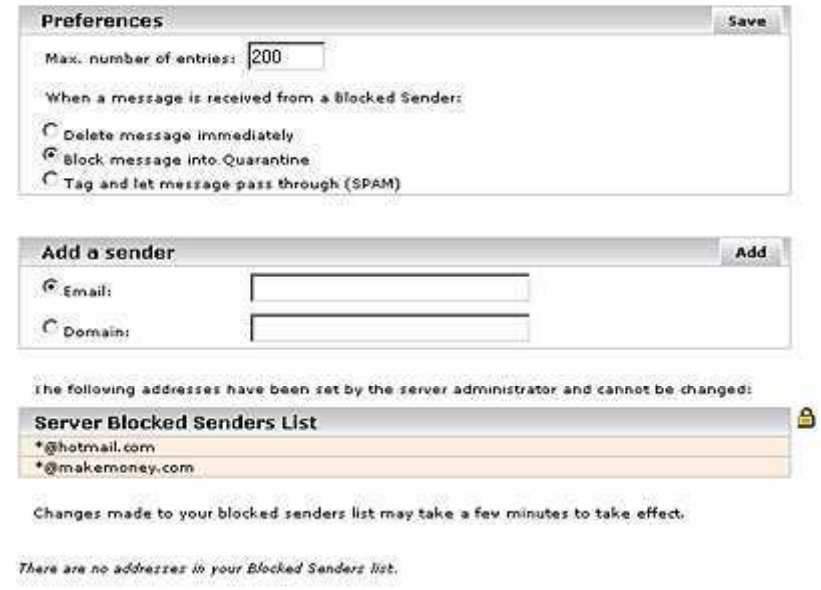


Figure 19: Blocked Senders List

## 4.2.7 Quarantine Report Preferences

You can select the frequency you prefer for receiving a Quarantine Report if you have been granted rights to override domain and server settings.

1 Choose **Settings > Email Filtering > Quarantine Reports**.
2 Choose the Report Schedule you prefer from the available options.
3 Choose the frequency you prefer from the drop-down list.
4 Choose which Report you prefer from the drop-down list. If you haven't created any custom quarantine reports, only the Default report will appear in the list.
5 Choose which items you want to include in your quarantine reports.
6 Click **Save** to save your changes.

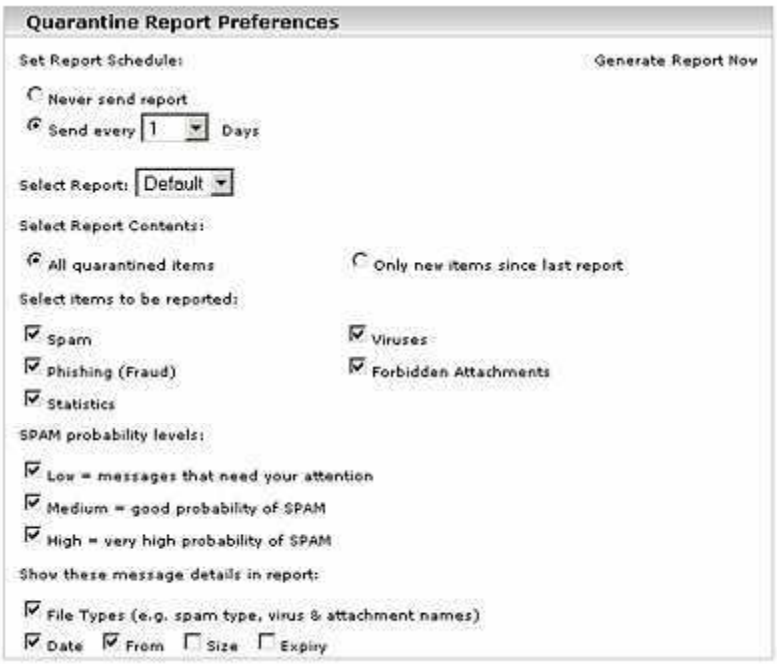


Figure 20: Quarantine Report Preferences

# 5.0 Glossary

**Alias**
An alternate name given to a mailbox.

**Auto-Reply**
An email message that is to be sent out automatically in response to any email received.

**BCC (Blind Carbon Copy or Blind Courtesy Copy)**
Recipient(s) in this list on an email are not displayed and are not visible to the direct or carbon-copied recipient(s) of an email.

**Blacklists**
See Blocked List.

**Blocked Senders List**
Allows users to designate a domain or IP address and email addresses from which no mail will be accepted.

**Browser (also Web Browser)**
This is a software application that allows you to view (or "browse") and interact with web sites on the Internet. Some of the most common web-browsing software applications are Microsoft Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera and Safari.

**Browser Compatibility**
The term "browser compatibility" refers to the fact that web-browsing applications from different companies sometimes display the same web pages with different formatting. This is to say that they interpret the code behind a web page (code which consists of HTML tags) differently. Sometimes these differences are minimal, but unfortunately these interpretational differences can sometimes also mean that you simply cannot view some parts of a website that has used particular HTML code tags because your web browser does not know how to display those parts (which use specific HTML tags).

**CC (Carbon Copy or Courtesy Copy)**
Recipient(s) in this field of an email's address list are not the direct recipients of the email. CC Recipients of an email are generally not required to take action on it, and their inclusion is usually for informational purposes only.

**Catch Rate**
The percentage of spam mail caught by a spam solution. It measures the efficiency of the solution at identifying and stopping spam.

**Content Filtering**
Scans plain text for key phrases that indicate that the message is spam.

**CSV (Comma Separated Values)**
This is a comma-delimited text file.

**Dial-up Internet Account**
This is an account that allows you to use a modem to connect to an Internet service provider who

then gives you direct access to the Internet.

**False Negative**
A false negative is an email that is spam, but which was not recognized by a spam solution and was released to your Inbox as legitimate email.

**False Positive**
A false positive is a legitimate email, but which was recognized by a spam solution wrongly as spam email and withheld from your Inbox.

**ISP (Internet Service Provider)**
A company that provides a connection to the Internet.

**Phishing**
A scam that uses spam to deceive people into disclosing their credit card numbers, bank account information, passwords and other sensitive information. Phishers often masquerade as trustworthy or well-known businesses.

**Quarantine**
To isolate files suspected of containing a threat such as a virus, so that it can not be opened.

**Quarantine Report**
A report of an account's quarantined email that is sent to a user's Inbox at regular intervals. This report is only generated when a user's account has email that has been identified either as spam or containing a virus and which has accordingly been withheld from the user's Inbox.

**Server**
A computer that runs administrative software (for the purposes of this user guide, a server is a computer on the Internet that runs an email exchange program).

**Spam**
Unsolicited, unwanted, bulk, commercial e-mail.

**Trusted Senders List**
Lets users designate a source or IP address from which all mail will be accepted, even if individual messages earn high spam ratings.

**URL (Universal or Uniform Resource Locator)**
This is an Internet address used by web browsers for a specific computer or a document (resource).

**Whitelists**
See Trusted Senders List.