

AirPear SPAM Instructions

2016



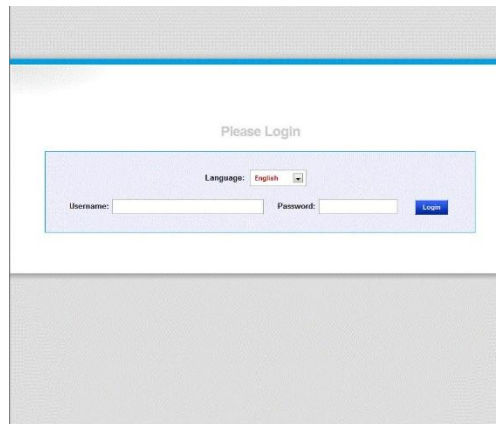
Table of Contents

| Subject | Page |
|-----------------------------|-----------|
| Getting Started | 2 |
| Logging into the system | 2 |
| Your Home Page | 2 |
| Manage your Account | 3 |
| Account Settings | 3 |
| Change your password | 3 |
| Junk Mail Digests | 4 |
| Digest Scheduling | 4 |
| Using Your Digest | 4 |
| Messaging Features | 5 |
| Your Message Queue | 5 |
| View Queued Messages | 5 |
| Whitelisting | 6 |
| Whitelist by "From" Address | 6 |
| Whitelist by "To" Address | 7 |
| Whitelist by Subject | 7 |
| Blacklisting | 8 |
| Blacklist by "From" Address | 8 |
| Blacklist by Subject | 9 |
| Spam Settings | 10 |
| Spam Aggressiveness | 10 |
| Advanced Settings | 10 |

Getting Started

Logging into the system

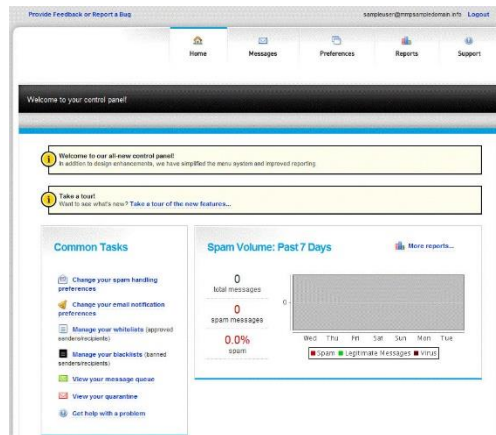
You can log into your spam management page <https://maxmail.gfi.com/> in your web browser. username will be your email address, and your password will either be your windows password or one you by your administrator.



by going to
Your
password
given to

Your Home Page

From this page, you can quickly jump to your important spam management tasks with just see an overview of your message volume and quarantined and queued messages.



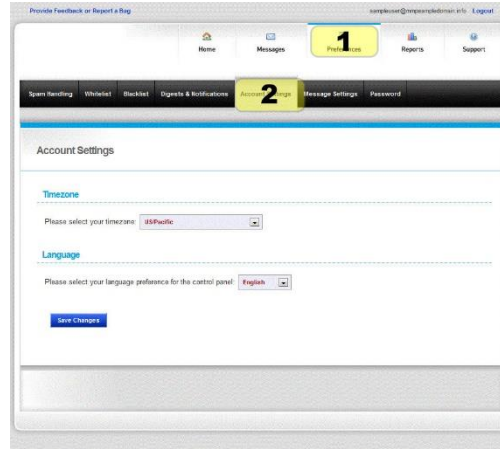
most
one click,
access your



Manage your Account

Account Settings

Enter the correct timezone so message delivery times are converted to your

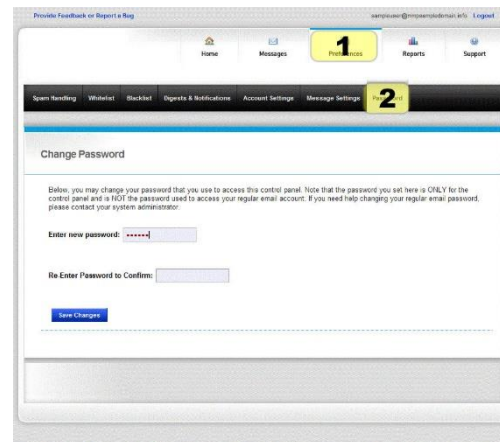


The screenshot shows a web interface for account management. At the top, there are navigation links: Home, Messages, Profile (with a '1' badge), Reports, and Support. Below this is a secondary navigation bar with links: Spam handling, Whitelist, Blacklist, Digests & Notifications, Account Settings (with a '2' badge), Message Settings, and Password. The main content area is titled 'Account Settings' and contains two sections: 'Timezone' with a dropdown menu set to 'US/Pacific' and 'Language' with a dropdown menu set to 'English'. A 'Save Changes' button is located at the bottom of the form.

and digest local time.

Change your password

This will only affect your MailProtection your actual email password. If you use password to log onto your computer your email, you might not be able to password through this screen (you contact your administrator).



The screenshot shows a web interface for changing a password. At the top, there are navigation links: Home, Messages, Profile (with a '1' badge), Reports, and Support. Below this is a secondary navigation bar with links: Spam handling, Whitelist, Blacklist, Digests & Notifications, Account Settings, Message Settings (with a '2' badge), and Password. The main content area is titled 'Change Password' and contains a warning message: 'Before, you may change your password that you use to access this control panel. Note that the password you set here is ONLY for the control panel and is NOT the password used to access your regular email account. If you need help changing your regular email password, please contact your system administrator.' Below the warning are two input fields: 'Enter new password' and 'Re Enter Password to Confirm'. A 'Save Changes' button is located at the bottom of the form.

login, and not the same and/or check change your would need to

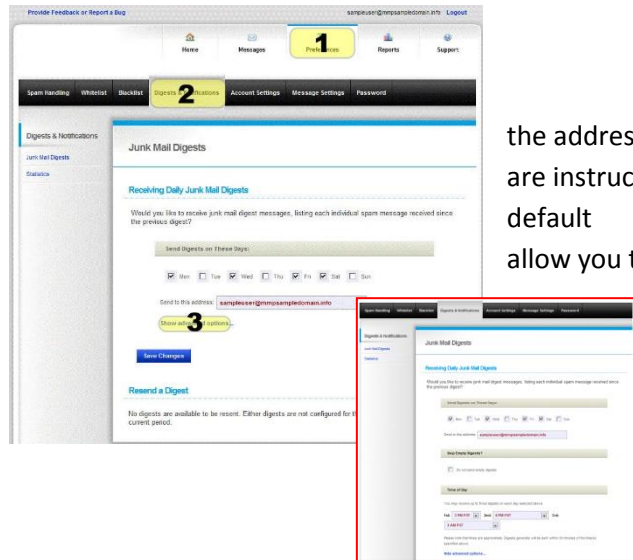


Junk Mail Digests

Junk Mail Digests give you a chance to inspect the mail we've quarantined as spam to reclaim any messages that were actually legitimate. Access the Digest settings by clicking **"Preferences"** (1), and then **"Digests and Notifications"** (2).

Digest Scheduling

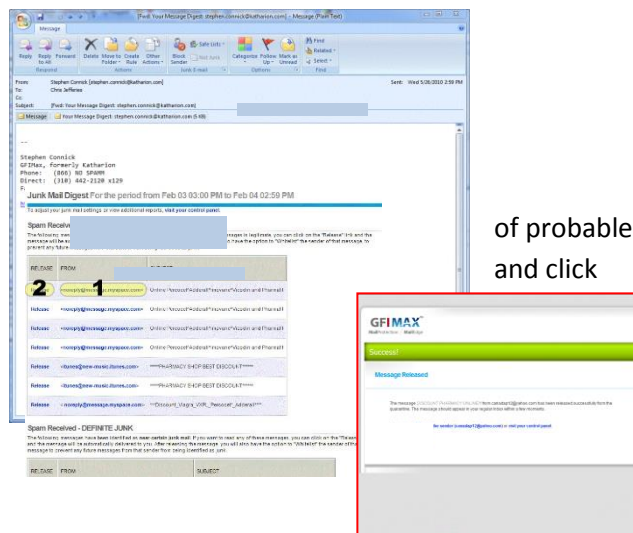
You can configure the days of the week and which your digest is delivered (unless you do otherwise, it is best to keep it as the address). **"Advanced Settings"** (3) will configure the approximate times of day (up to 3) the digests are delivered.



the address to are instructed default allow you to

Using Your Digest

The digest will arrive in your email as a list of definite spam. You can see the sender (1), **Release**(2) to deliver the message to your inbox, removing it from quarantine. You will be redirected to a success page and given the option to whitelist all messages from that sender.



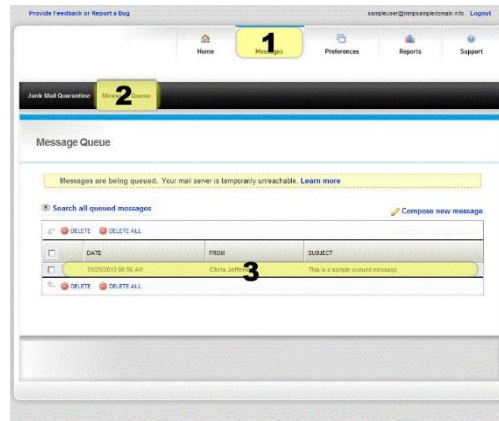
of probable and and click

Messaging Features

In the event your mail server goes down, we can provide you with a temporary means of maintaining email capabilities until your service is restored.

Your Message Queue

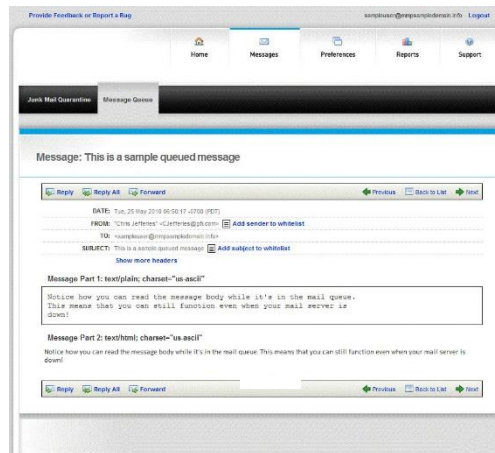
You can view and send email through clicking “Messages” (1) at the top of the “Message Queue” (2) on the navigation bar. Any mail that was unable to reach your server is Click on a message (3) to view it.



our interface by page, and then bar. Any mail that viewable here.

View Queued Messages

You will be able to read, reply to and queued email with our interface.



forward your

Whitelisting

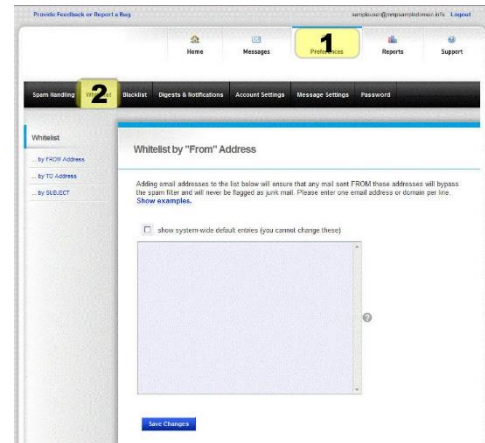
When used judiciously, whitelisting is a valuable tool in keeping your mail flowing. When configured incorrectly, it can be an open door for spam. Following these guidelines will help you achieve desired results.

Whitelist by “From” Address

Click: “Preferences”(1) , and then “Whitelist”(2).

Enter addresses, one per line, which you would like to have bypass spam filtering. All whitelisted senders will be delivered regardless of content, with the exception of viruses.

IMPORTANT: DO NOT WHITELIST YOUR OWN ADDRESS OR DOMAIN, AS THIS WILL CAUSE A LARGE AMOUNT OF SPAM TO REACH YOU.



Acceptable formats include:

- user@domain.com - (all mail from this address will be allowed through)
- domain.com - (all mail from all users from this domain will be allowed through)

Suggestions:

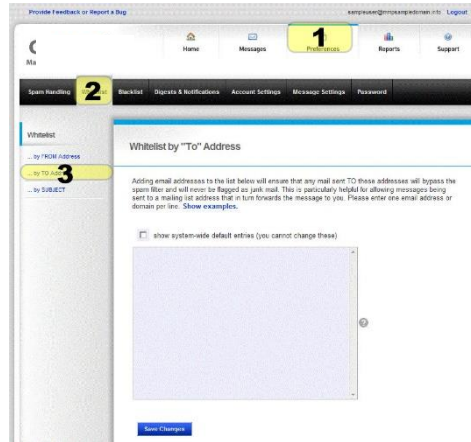
- Try not to pre-populate the whitelist with a large number of domains, but rather use it as a tool to correct false positives.
- Large, well-known domains shouldn't be whitelisted at the domain level (Microsoft.com, aol.com, etc), but rather at the individual address level you know and trust.
- Well-known addresses (notification@facebookmail.com, etc) are candidates for spoofing as well. The more widely-known the address is, the more caution you should use when deciding whether or not to whitelist.



Whitelist by "TO" Address (3)

This tool is usually used to allow all messages that are sent to you via a mailing list.

IMPORTANT: DO NOT WHITELIST YOUR OWN OR ANY OTHER ADDRESS WITHIN YOUR AS THIS WILL CAUSE A LARGE AMOUNT OF REACH YOU.



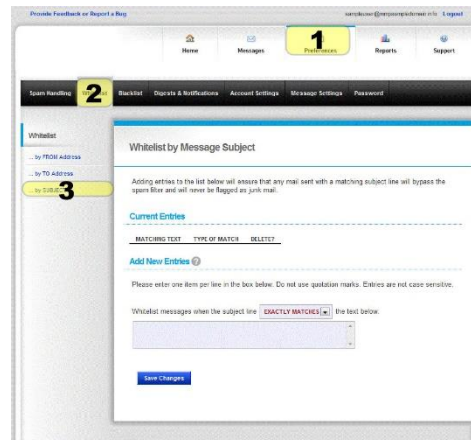
through

ADDRESS DOMAIN, SPAM TO

Whitelist by Subject (3)

This tool will allow you to have selected bypass filtering, regardless of sender, based subject line. Add entries based upon:

- Exact match
- Begins with
- Ends With
- Contains (recommended)



messages upon the



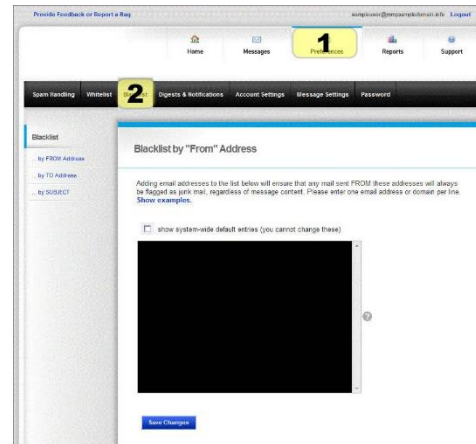
Blacklisting

Blacklisting is best used to combat the messages that you know you will never want, although they might not be spam to everyone.

Blacklist by “From” Address

Click: “Preferences”(1) , and then “Blacklist”(2). addresses, one per line, which you would like to automatically block without exception.

IMPORTANT: DO NOT BLACKLIST YOUR OWN OR DOMAIN, AS THERE ARE CERTAIN TIMES LEGITIMATE MAIL FROM THESE ADDRESSES EXTERNALLY.



Enter

**ADDRESS
WHEN
ARRIVES**

Acceptable formats include:

- user@domain.com - (all mail from this address will be blocked)
- domain.com - (all mail from all users from this domain will be blocked)

Suggestions:

- Try not to pre-populate the blacklist with a large number of domains, but rather use it as a tool to block recurring spam sources.
- Marketing emails you may have inadvertently opted into are a good blacklisting candidate, although you also have the option of clicking “unsubscribe” if the sender seems reputable. (ex: retail store marketing newsletter)
- Blacklisting for each piece of spam that reaches you is unnecessary and ineffective, as most spammers don’t use the same address repeatedly.



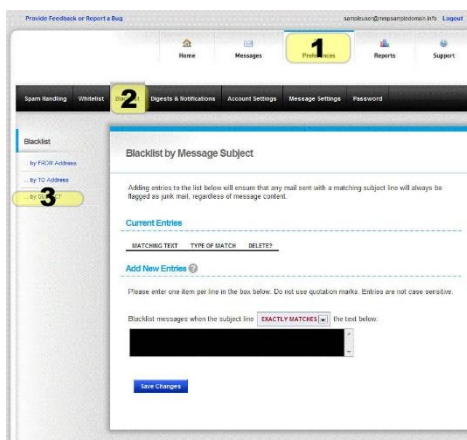
Blacklist by Subject (3)

This tool will allow you to have selected automatically classified as spam by the entries based upon:

- Exact match
- Begins with
- Ends With
- Contains (recommended)

These “Blacklisted by Subject” entries will digests and quarantine (but not your inbox)

“Hide Egregious Spam” enabled, as we have to accept the message to analyze the subject.



messages
subject line. Add

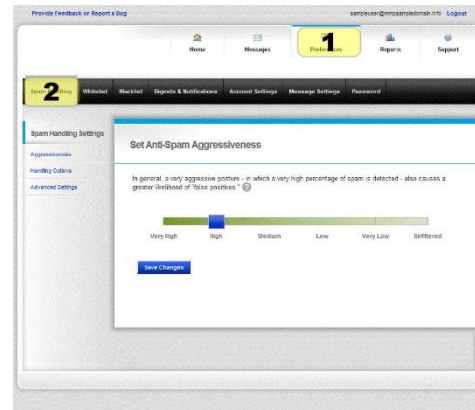
be visible in your
unless you have

Spam Settings

You can change the aggressiveness and handling of your spam filtering at any time by selecting the “Preferences”(1) icon at the top of the screen and then selecting “Spam handling”(2) via the navigation bar.

Spam Aggressiveness

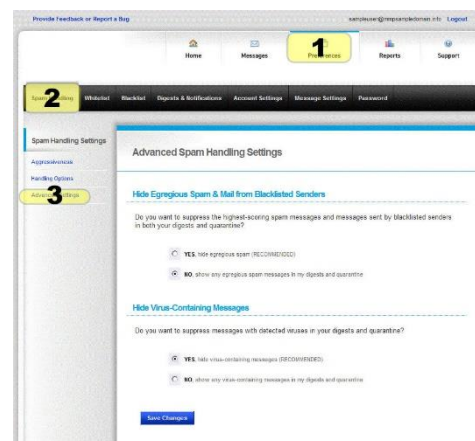
We recommend starting with a setting of “High”. From there, you can either move up to “Very High” if you are seeing spam pass through the filters, or “Medium” if you encounter a large number of positives.



“High”.
High” if you
down to
false

Advanced Settings (3)

Here you can choose to hide high-scoring spam and blacklisted messages from being your digests and quarantine, making it easier to misclassified mail. We recommend not enabling until you are confident you have not misconfigured your blacklist.



(egregious)
displayed in
scan for
this option
accidentally

WE DO NOT RECOMMEND CHANGING THE SETTINGS ON THE “HANDLING OPTIONS” SIDEBAR LINK FROM THE ADMINISTRATOR-CONFIGURED DEFAULTS.

