



## Mail Services – SPAM Filtering

### Table of Contents

Subject	Page
<b>Getting Started</b>	<b>2</b>
Logging into the system	2
Your Home Page	2
<b>Junk Mail Digests</b>	<b>3</b>
Digest Scheduling	3
Using Your Digest	3
<b>Messaging Features</b>	<b>4</b>
Your Message Queue	4
View Queued Messages	4
<b>Whitelisting</b>	<b>5</b>
Whitelist by “From” Address	5
Whitelist by “To” Address	6
Whitelist by Subject	6
<b>Blacklisting</b>	<b>7</b>
Blacklist by “From” Address	7
Blacklist by Subject	8
<b>Spam Settings</b>	<b>9</b>
Spam Aggressiveness	9
Advanced Settings	9



## Mail Services – SPAM Filtering

### Getting Started

#### Logging into the system

You can log into your spam management page by going to <https://mailservices.aoscopy.com> in your web browser. Your username will be your email address and your password will be your windows password.

Please Login

Language: English

Username:  Password:  Login

#### Your Home Page

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

Provide Feedback or Report a Bug sampleuser@mmpsampledomain.info Logout

Home Messages Preferences Reports Support

Welcome to your control panel!

**Welcome to our all-new control panel!**  
In addition to design enhancements, we have simplified the menu system and improved reporting.

**Take a tour!**  
Want to see what's new? [Take a tour of the new features...](#)

**Common Tasks**

- [Change your spam handling preferences](#)
- [Change your email notification preferences](#)
- [Manage your whitelists \(approved senders/recipients\)](#)
- [Manage your blacklists \(banned senders/recipients\)](#)
- [View your message queue](#)
- [View your quarantine](#)
- [Get help with a problem](#)

**Spam Volume: Past 7 Days** [More reports...](#)

0 total messages  
0 spam messages  
0.0% spam

Wed Thu Fri Sat Sun Mon Tue

Spam Legitimate Messages Virus



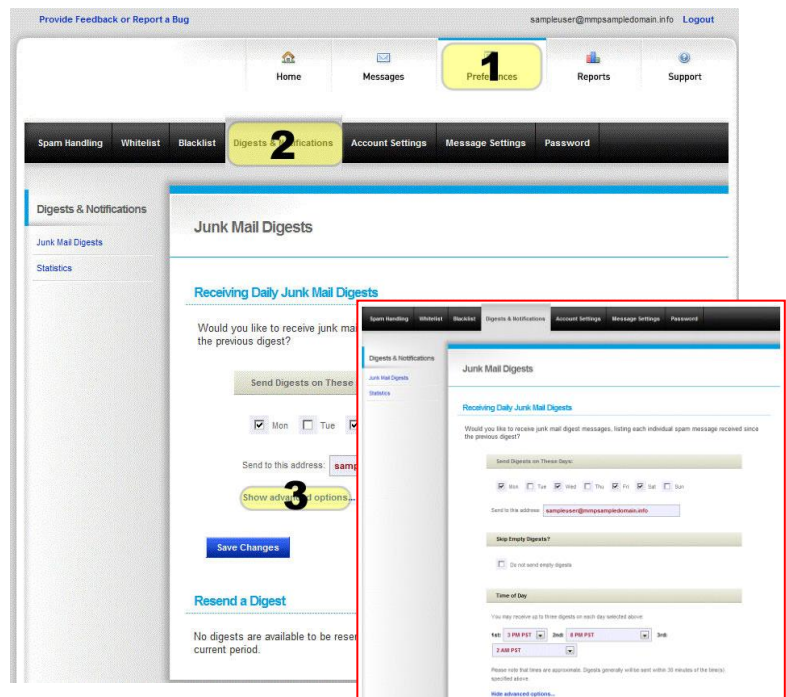
## Mail Services – SPAM Filtering

### 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).

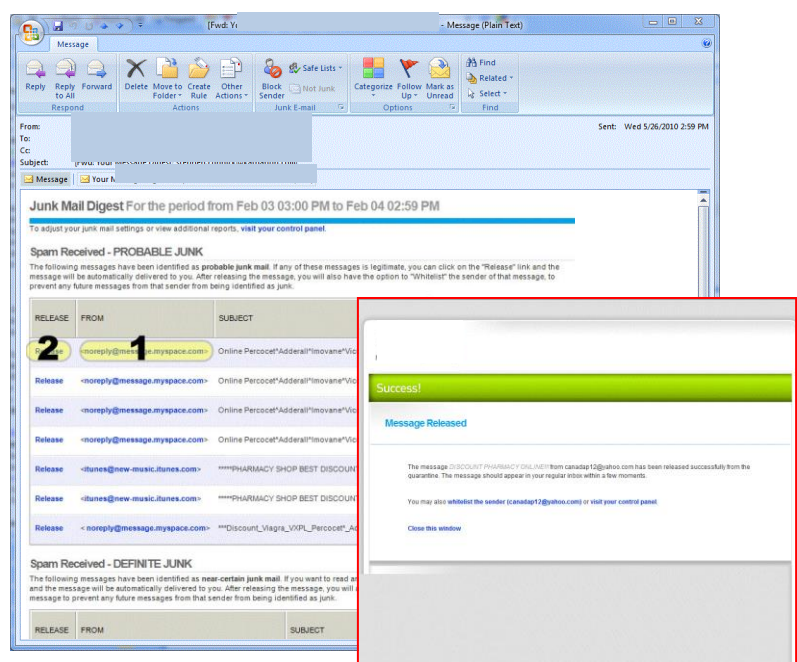
### Digest Scheduling

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



### Using Your Digest

The digest will arrive in your email as a list of probable and definite spam. You can see the sender (1), and click **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.





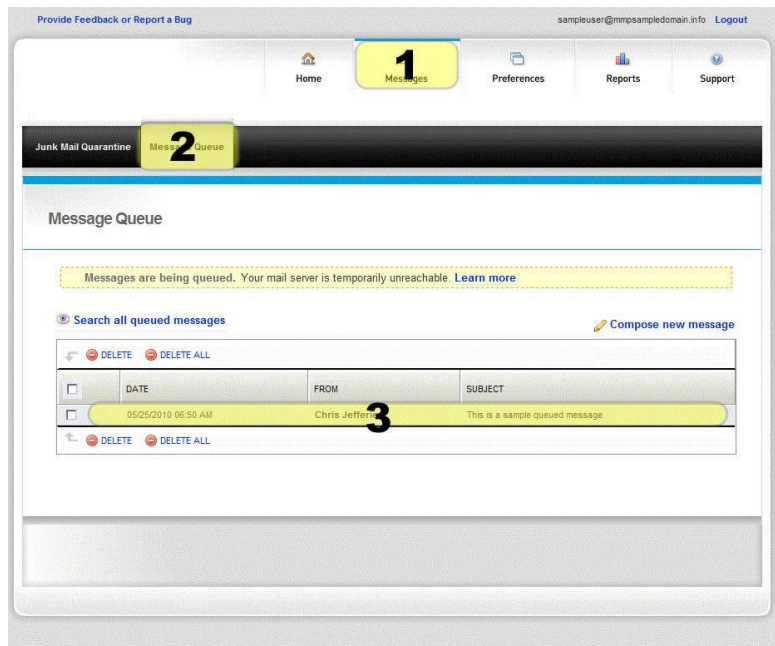
## Mail Services – SPAM Filtering

### 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.

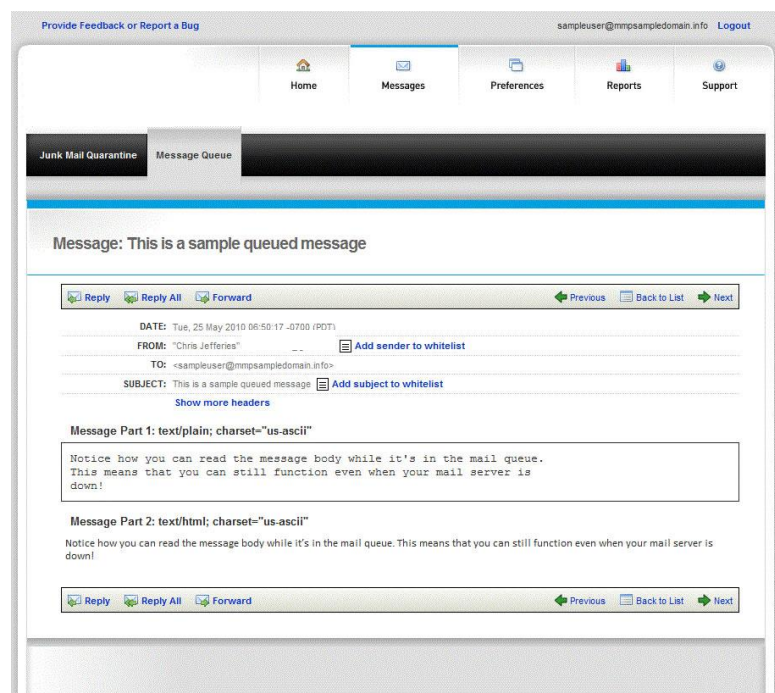
### Your Message Queue

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



### View Queued Messages

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





## Mail Services – SPAM Filtering

### 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.

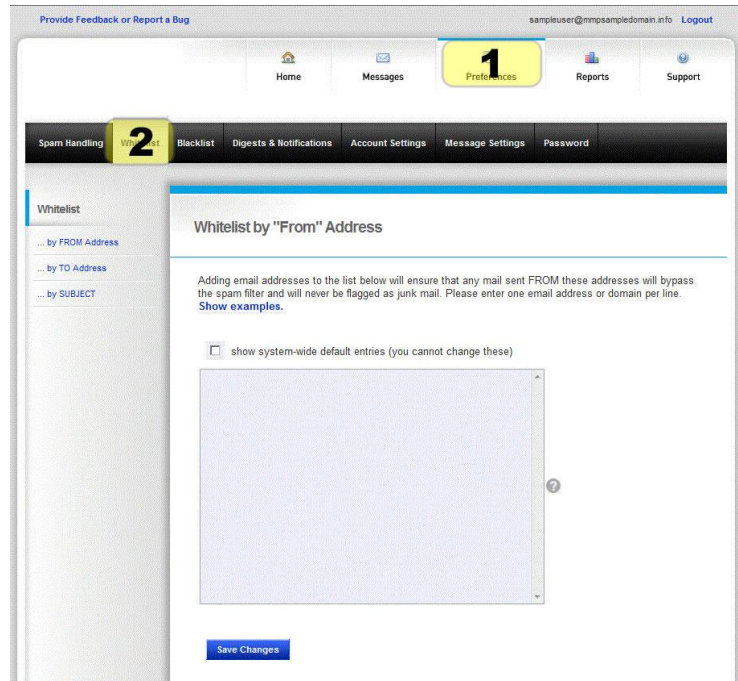
#### Whitelist by “From” Address

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.



## Mail Services – SPAM Filtering

### Whitelist by “TO” Address (3)

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

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

### Whitelist by Subject (3)

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

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

## Mail Services – SPAM Filtering

### Blacklisting

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

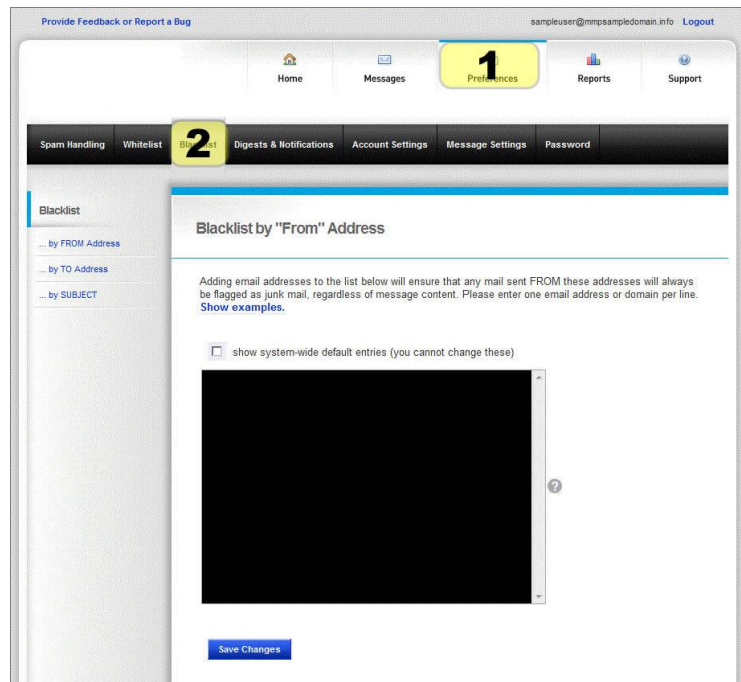
#### Blacklist by “From” Address

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

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

#### 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.



## Mail Services – SPAM Filtering

### Blacklist by Subject (3)

This tool will allow you to have selected messages automatically classified as spam by the subject line. Add entries based upon:

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

These “Blacklisted by Subject” entries will be visible in your digests and quarantine (but not your inbox) unless you have “Hide Egregious Spam” enabled, as we have to accept the message to analyze the subject.





## Mail Services – SPAM Filtering

### 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 down to “Medium” if you encounter a large number of false positives.

### Advanced Settings (3)

Here you can choose to hide high-scoring (egregious) spam and blacklisted messages from being displayed in your digests and quarantine, making it easier to scan for misclassified mail. We recommend not enabling this option until you are confident you have not accidentally misconfigured your blacklist.

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