



User Guide Anti-Spam Filter

V 09.12.09

TABLE OF CONTENTS

About the filter	2
Accessing your filter	2
SPAM.....	3
Held Messages.....	3
Release.....	3
Delete	3
Allow	3
Educate your filter with IsSpam – NotSpam.....	3
Settings	4
Filtering.....	5
Friends	6
Settings	6
Temporarily deactivate the filter	6
Friends address list.....	6
Deleting or Blocking addresses	7
Validation requests	7
Pending messages	7
Incoming messages.....	7
Outgoing messages.....	7
SPF	8
Logs.....	8



User Guide Anti-Spam Filter

If you have opted for spam filtering services upon opening your Web hosting account with Natmark-Concept, all emails linked to your domain are covered by our anti-spam filter. Each email account is independent and can control its own filter, whitelist, exceptions and other filter parameters.

Upon its activation, your filter was manually parameterized by our technicians, some of which would be better left unchanged if you wish to get the best from your filter in accordance with your email account. Others can be modified at will, to fit your personal tolerance to spam, which might by-pass the filter and find their way to your mailbox.

About the filter

First, know that no filter is 100% effective and that attempts by spammers to by-pass filters are relentless. Thus, the filter can just as well let through certain spams, as it can block some legitimate emails. This is why it is important that you **always keep an eye on your filter** (at least every 2 to 3 days) to prevent important emails from being lost.

What follows is a brief guide of the filter parameters which you can modify without risk. If you would like additional explanations, please feel free to contact us at info@natmark.net and we'll be glad to help.

Accessing your filter

You can access your personal anti-spam filter by entering <http://filter.natmark.net/> in your Web browser. We suggest you bookmark this link since you will need to access it frequently. This link will take you to the following page, inviting you to login. You do so by entering your full email address and password (the same password as for your email account).

If you have lost your password, don't bother clicking the « Forgot » button, since the filtering provider cannot help. **You will have to contact us.**

Please enter your email address below to login and change your mail filtering account settings.

Username

Password

Language ▼

Login

Forgot



SPAM)

The screenshot shows the SurgeMail webmail interface. At the top, there's a header with the SurgeMail logo and "(WebMail port)". Below that, a sub-header reads "Held spam messages (info@natmark.net)". On the left, there's a navigation menu with buttons for "Spam", "Filtering", "Friends", "SPF", "Log", and "Logout". The main content area is titled "Held spam messages" and includes "Settings" and "Held Messages" tabs. A message list is displayed with columns for "sel", "View", "Score", "From", "Subject", and "Date". Two messages are listed: one from "Angie R. Hatch" with a score of 18, and another from "Caroline Thibault" with a score of 5. Below the list, there are buttons for "Release", "Delete", "Allow", "IsSpam", and "NotSpam". A "Select all" button and a counter "2 out of 2, starting at 0" are also visible. A small text block at the bottom provides instructions for each action: "Release will deliver the message to you.", "Allow will deliver the message and all others from the same person, then add them as a friend.", and "Delete will delete the message."

Held Messages

Upon login, the filter greets you immediately with the page of Held Messages. This is where emails suspected of being spam are being held, awaiting your instructions. Each email is preceded by a checkbox allowing you to treat each message individually. **If no instruction is given to the filter for a given message after one week, it will be purged (erased).** Available options are:

Release

Release
Sometimes, it might be difficult to judge if a held message is spam or not, and the viewing interface (small « view » link) doesn't allow you to really decide. Clicking the « Release » button will let the selected message go through, nothing more. Once it has reached your mailbox, it might be easier to decide. The address of the sender will not be added to your friends list (*whitelist*). It merely allows the message to be released so you can decide for yourself if it was legitimate or not. During the first weeks of use, you will often be indecisive regarding the validity of certain emails, but you will soon learn to recognize spam.

Delete

Delete
You are sure that one or more held emails are indeed spam? Check the box at the left of each bad message and click « Delete » to permanently erase them from the filter queue.

Allow

Allow
Whoops! A message from a legitimate correspondent was blocked. Why was it blocked? It can be for a number of reasons like the weight of the email, the attached file(s), the format or even certain terms used in the message itself. Don't waste time wondering. The essential thing is that you've seen it. Check the box at the left of that message and click « Allow », which will release the email and add the email address of your correspondent to your *Friends* list. This way, the filter will no longer stop future messages sent by that contact (using that email) and always deliver them to your mailbox (or almost always... remember, the filter isn't magic...).

IsSpam

NotSpam

Educate your filter with IsSpam – NotSpam

Your filter really likes to know that he's doing a good job and invites you to continue its education if you wish (this is optional), by letting it know if a held message was indeed spam or not. Check the box at the left of a given message and click « IsSpam » if it is indeed spam or « NotSpam » if it isn't. Again, this is optional and you might not want to waste time on this. Your filter's database is routinely updated with the latest spam definitions, whether you do this or not.



Settings

As previously mentioned, your filter was parameterized upon activation. However, you can modify some of its parameters yourself, according to your personal tolerance to a legitimate email be lost, or to the daily quantity of spam that finds its way to your mailbox. As a comparative, know that it is normal for 5 to 7 spam messages to by-pass the filter daily. More than 7 means you filter might need adjusting.

Beware of adjusting your filter too high (severely), which would increase the chances of legitimate emails being held and forcing you to check your filter too frequently.

Spam settings

Settings | Held Messages

Based on the spam rating you can choose to hold*, reject*, or vanish* a message before you even see it. Simply set the value below for each action. These are applied **after** any exceptions you may have, and **before** Friends confirmations are sent

Hold when rating is: 4+ Probably spam

Vanish* when rating is: 10+ Definitely spam

* Hold means the message is kept for 2 weeks, in which time you can view the message(s) and choose to receive specific messages.
* Reject means do not accept the message, their server will notify them that you didn't get it.
* Vanish means throw the message away, sender doesn't know you didn't get it.

The vanish option is not recommended because the sender is not notified when the message is not delivered.

Save | **Use Defaults**

Do not modify --> **SpamPrivate Alias features**

Private suffix, e.g. "private" Use this address to skip spam/spf: info--@natmark.net

From suffix, e.g. "from" Use this address for web pages: info---WEBDOMAIN@natmark.net

Save | **Use Defaults** | **Help**

Email addressed to your private alias (user--PRIVATESETTING@domain.com) will bypass spam and SPF rules. You should be very careful with this private address, DO NOT enter it into web pages or use it when joining mailing lists or posting to news groups/web pages.

Do not modify --> **SPAM features (* SERVER DEFAULT is subject to change)**

NEVER modify subject Add the spam indicator to the message subject at this smite level eg level 4 = 'Spam:****, '

NEVER add headers Add spam indicator headers to the message body at this smite level.
(required to filter messages if using Microsoft Outlook)

Save | **Use Defaults**

The number selected on the « Hold when rating is » menu instructs the filter to hold for a period of one week, any message rated as having reached this level. This will allow you time to visit your filter and decide what to do. **The suggested grade is 5.**

The number selected on the « Vanish when rating is » menu instructs the filter to purge (delete) any message rated as having reached this level. **The suggested grade is 7.**

In all cases, when a message is purged, the correspondent will never know that his message never reached you.

Additional parameters (*SpamPrivate Alias features* et *SPAM features*), indicate to the filter when it needs to block or let specific messages through, modify their subject line by inserting the word [BULK] indicating a possible spam, or a feature that can interact with Outlook.

We suggest you **do not modify these parameters** unless you **fully** understand their effect. Basic parameters should be adequate for your present needs.



Filtering

Many users need to correspond with more than one person working at a given client company. This would make it time-consuming to individually add each and every correspondent's email to your whitelist. To cover this eventuality, the « Filtering » feature has been created to save time, allowing you to *whitelist all* emails coming from a given domain.

For example, in the next example (screenshot), since it is possible that more than one partner having a Natmark-Concept email address will write to you, we whitelisted the entire Natmark domain: **natmark.net**. This means that all messages coming from any correspondent with a **@natmark.net** email will automatically be sent to your mailbox and will not be blocked.

To add such a client to your exceptions, you must complete the instruction phrase given to the filter:

- Select « From » in the first dropdown menu;
- Type in the domain name to be authorized in the last field (without the www);
- Select the option « Accept » (last dropdown menu at the bottom);
- Click « Add ».

The « Filtering » feature can also serve to automatically block or purge emails coming from entire domains or emails containing subjects or content that you *know* to be spam (like the Acai berry stuff). However, caution should be used when using these possibilities, since a message coming from a legitimate correspondent forwarding such a message with his personal comments might just automatically get purged.

Exceptions and Filters

If the header

and...

or...

then to email address

reason for rejection

[Add](#) [clear](#)

ID	Sel	Header	Match	Text	Action	Destination*/Reason**
	<input type="checkbox"/>					

[Delete](#) [Move To top](#) [Move Up](#) [Move Down](#) [Move To Bottom](#)

Exceptions and Filters

If the header

and...

or...

then to email address

reason for rejection

[Add](#) [clear](#)

ID	Sel	Header	Match	Text	Action	Destination*/Reason**
<i>if</i> 0	<input type="checkbox"/>	From	contains	natmark.net	<i>accept</i>	edit copy

[Delete](#) [Move To top](#) [Move Up](#) [Move Down](#) [Move To Bottom](#)



Friends

In a previous section, you learned that by clicking « Allow » for a held message, your correspondent's email would be added to your friends list. This list is better known as a « whitelist » and allows you to keep a registry of your current correspondents. This accelerates the filtering process and lowers the chances that emails coming from your regular correspondents be blocked, held or purged.

Read the following carefully, since some of the parameters must not or cannot be modified in this next section.

Settings

Settings

Use Defaults

Friends - Settings

Settings | **Address list** | **Message** | **Pending** | **Incoming** | **Outgoing**

The Friends system allows you to maintain a list of acceptable addresses. It automatically holds email from unknown senders, awaiting a reply to a confirmation message. This checks they are a real person and not just a spam robot. See [here](#) for more details. Friends is applied **after** your Filters and **after** your Spam rules.

Disable Friends.

Kid safe - only accept mail from known senders. (You must specify senders in 'Address list')

Apply friends list but don't block anything or request confirmation.

Save | **Use Defaults**

Disable Blocking This allows you to allow all mail for 3 hours. Use it when expecting an urgent email from an unknown person, robot or mailing list

Help

Do not modify →

The friends list is the **last** verification step made by the filter before it definitely holds, blocks or purges an email. The filter first goes through all the instructions given to it and **then** compares all held messages with your whitelist. If the email address of your correspondent is on the whitelist, the filter will let it through.

Since it is best for your to be able to add specific unique correspondents to your whitelist (Friends list), do not modify this section's parameters.

Disable Blocking

Temporarily deactivate the filter

At the very bottom of the parameters page is the « Disable Blocking » button, which can be useful when you are expecting one or more urgent emails from unknown correspondents and won't have time to supervise your filter for the next few hours. The « Disable Blocking » button temporarily deactivates the filter for a period of three (3) hours, and lets ***all messages*** through (good AND spam...) without filtering them. You can expect to receive a large quantity of spam during this period since nothing will get filtered. It's the equivalent of having totally deactivated the filter.

After three hours, filtering will resume by itself, without intervention on your part.

Address list

Friends address list

You can create your own whitelist from your address book by clicking on the « Address list » button. You will then be presented with an interface where you can enter the emails of your already known friends and correspondents. To enter many addresses, simply type them in one per line. You can also import a CSV file of your own address book.

Reminder: The *Filtering* feature mentioned above will save you time for many correspondents from a same company.



Friends address list (next)

Friends - Address list

[Settings](#) [Address list](#) [Message](#) [Pending](#) [Incoming](#) [Outgoing](#)

This is your Friends address list. Addresses on this list are not subject to the CentiPaid or Spam systems.

Add address:

There is a limit to the number of addresses you can enter above, try not to add more than 350 at a time.
Wildcards are not allowed here, see 'exceptions' for wildcard Accept rules

[Add address](#)

[Browse...](#) [Import addresses \(CSV\)](#)

[Delete Address](#)

[Block Address](#)

Deleting or Blocking addresses

You were distracted and clicked « Allow » by mistake for a message which turned out to be spam, adding it to your friends list? No problem! Check the box next to the offender's email address and click « Delete Address ».

One of your friends turns out to be a stalker and you'd like to block him forever from your life? Check the box next to his email address and click « Block Address ». This feature takes the email OUT of your friends list and adds an exception in the « Filtering » page so all of his messages will be automatically blocked from now on. Your correspondent will never know that his emails have been refused. If, at a later date, you realize this was all one big misunderstanding, you'll have to go in the « Filtering » section to erase the rule that was created for his email address.

[Message](#)

Validation requests

The « Message » feature is a powerful tool which is not always appropriate to use. It makes the filter *request* each correspondent not already on your friends list, to identify himself to be able to correspond with you. This feature gets activated by default if you modify your parameters from « Friends » to « Kid safe ». In such a case, the filter will send back to each person a request for validation, for which you can control content. Since 99.9% of spam come from robots, only *human* correspondents will then be able to go through the validation process. Any validation request not answered will result in the deletion of the initial email. For a family email or child's email, this is an added security feature.

However, if you use your email for business purposes, it is not recommended to use this feature for fear of dissuading possible business correspondents. Since our clients are mostly businesses, each filter is thus parameterized to allow a whitelist, but NOT to send validation request messages. We strongly suggest that you **do not modify those parameters**.

[Pending](#)

Pending messages

Lists messages awaiting validation by a *human* correspondent.

[Incoming](#)

Incoming messages

Lists messages recently filtered and allows you to add specific addresses to your friends list if desired.

[Outgoing](#)

Outgoing messages

This feature relates to messages sent through a system using Webmail filtering, which is not our case. **Ignore**.



SPF

The SPF feature can force a correspondent's emails to bear a specific « signature » pertaining to the domain it is sent from. Since many people work from home or use email connections not having this special signature, it might not be wise to activate it and is thus deactivated for all our client accounts. **Do not activate it unless you fully understand SPF.**

SPF features

SERVER DEFAULT (false) Whether to block non spf compliant emails Do not modify ←

SPF stands for "Sender Policy Framework". It is a system which aims to verify an email from a domain is really coming from that domain. The system requires that domains publish SPF records to identify themselves. If an email arrives from a domain but the sender does not match the SPF record for that domain, or that domain has no SPF record it is considered a non-'SPF compliant' email.

SPF history

Show Max

0 out of 0, starting at

Do not modify →

IP addresses in **bold** are now known by the system and will be accepted in future.

Logs

Many users are afraid to forget to check their filter regularly. No problem, the filter can send you a customized report at given intervals to remind you to keep an eye and listing all decisions it has taken since its last report. By default, the filter does not send a report. It is up to you to give it this instruction.

Log

The Account log records actions performed by the Friends, CentiPaid, and Spam systems. You can check up on it by coming here. This log is emailed to your account.

Send an account status message if required at least every days

The last status message was sent: **Tue Mar 25 12:01:33 2008**

Include Friends pending message list.
 Include spam held message list.

Include these log messages in the status email:

<input checked="" type="checkbox"/> Allowed	<input type="checkbox"/> Pending	<input type="checkbox"/> Confirm	<input checked="" type="checkbox"/> Released	<input checked="" type="checkbox"/> Friend	<input checked="" type="checkbox"/> Vanished	<input type="checkbox"/> SPF
<input type="checkbox"/> Rejected	<input checked="" type="checkbox"/> Held	<input type="checkbox"/> Payment	<input type="checkbox"/> Purge	<input checked="" type="checkbox"/> Status	<input type="checkbox"/> Sms	<input type="checkbox"/> Copied
<input type="checkbox"/> Moved	<input type="checkbox"/> Forward	<input type="checkbox"/> Forward CC	<input type="checkbox"/> Enotify	<input type="checkbox"/> Virus	<input type="checkbox"/> View	

Show entries containing

Filter using above settings

In this page, tell the filter with the help of the dropdown menu and the check boxes, the frequency at which you wish to receive a report and what it should contain. When requested, a report contains a list of actions taken for *all* emails. You'll then be able to realize how well your filter is doing its job. But that might prove to be a bit overwhelming. As a guide, you can limit your reports to the following data which is probably what is most important to you:

- Allowed
- Released
- Friends
- Vanished
- Held → **WHAT YOU MOST WANT TO KNOW**
- Status

Reminder: The filter automatically purges all held emails for which no decision was taken or instruction given after 7 days.

When you are done, just click on the **Logout** button.