SmarterMail Internal Spam Block Quick Start Guide

Table of contents

What is it for?

The ***SmarterMail Internal Spam Block (SMISB)*** software allows to automatically block SmarterMail mailboxes (and/or mail domains) if they exceed the specified limit of sent (or received) email messages within a specified period of time.

But there is a built-in SmarterMail feature for this task, isn't there?

SmarterMail server software has a similar feature built-in, but:

1. There is no such a feature in the ***Professional*** version of the SmarterMail Server. You can find the "internal spam" related parameters in SmarterMail Server settings ("Abuse Detection - Internal Spammer" menu), but the mail server just ignores them if you have the Professional version.
2. There is a similar feature in the ***Enterprise*** version of the SmarterMail Server, but the ***SmarterMail Internal Spam Block*** tool has some advantages. The ***SMISB*** allows setting custom send/receive ***limits on domain and mailbox level***. Also the ***SMISB*** has ***white lists*** on both domain and mailbox levels.

System requirements

- ***SmarterMail Internal Spam Block*** was created for SmarterMail 15 (both Professional and Enterprise), but works fine with the older SmarterMail server versions too.
- Microsoft .NET Framework 4 must be installed on your computer.

Software registration

You need a license key to use the ***SmarterMail Internal Spam Block*** software. You can buy it at http://www.hoststools.com Once you got the key, please specify it in the ***smub.exe.config*** configuration file (see the ***Setup and security*** paragraph in this document below).

Run this tool on a server or PC?

We highly recommend to run ***SmarterMail Internal Spam Block*** on your mail server for security and performance reasons. However you can use it from your PC, just be sure it is not blocked by your server firewall. ***SmarterMail Internal Spam Block*** uses SOAP (HTTP over port 80 or HTTPS over port 443) to connect to SmarterMail servers.

How does it work?

The ***SmarterMail Internal Spam Block*** tool connects to the SmarterMail Server and receives send/receive statistics for all the mailboxes and mail domains. Then the tool goes through the list of the mailboxes (and domains) and processes the data in the following order for each of the mailboxes (and domains):

1. If some domain name is listed in ***white.domains.txt*** configuration file, the tool ignores that domain name.
2. If some mailbox is listed in ***white.mailboxes.txt*** configuration file, the tool ignores that mailbox.
3. If some mailbox is listed in ***throttling.params.txt*** configuration file, the tool acts according to the limits and actions specified in ***throttling.params.txt*** for that particular mailbox.

4. If some domain name was not found in the previous 3 lists (domain white list, mailbox white list, throttling parameters) the tool takes the global parameters from the main configuration file (***smub.exe.config***) and acts accordingly.

If some mailbox exceeds the specified limits the tool blocks that mailbox and adds its name to the blocked mailbox list in blocked.txt file. Also the tool saves the date and time when the mailbox was blocked. And during the nearest 24 hours the tool does not process any data related to that blocked mailbox.

> *If you unblock some mailbox you must remove it from the blocked.txt file manually if you wish the* **SmarterMail Internal Spam Block** *to monitor its activity during the first 24 hours after its last block.*

For example:

> You specified the daily limit of 2000 sent emails (on the global level for all the mailboxes of your mail server or as a custom level personally for sales@domain.com mailbox), but sales@domain.com user tried to send 5000 emails. Once the ***SmarterMail Internal Spam Block*** detects that, it blocks sales@domain.com mailbox and adds its name to the ***blocked.txt*** file along with the date and time. Let's say the client (sales@domain.com owner) contacts you and asks to unblock the mailbox. If you decide to unblock it you have 2 options:
>
> 1. Just enable the mailbox with SmarterMail administrator control panel. And do not edit the ***blocked.txt*** file. In this case the ***SMISB*** will not look at this particular mailbox stats during the 24 hours from the mailbox block. And this particular customer will be able to send unlimited emails during this day. However the next day the limit (of 2000 emails) becomes valid again.
> 2. Alternatively you can remove this mailbox from ***blocked.txt*** file (in addition to turning the mailbox on with the SmarterMail admin control panel). In this case you have to increase the limit to 5000 (at least) for this particular mailbox in ***throttling.params.txt*** configuration file. Otherwise the ***SMISB*** will block that mailbox again.

Setup and security

This application is **portable**, no installation is required. However you need to edit its main configuration file (***smub.exe.config***) and additional configuration files (TXT), and also create a Task Scheduler task.

Please use Notepad or other simple editor (for example, Notepad++) to edit the configuration files.

> *Do not use Microsoft Word, because it can break the configuration file structure.*

Schedule

SmarterMail Internal Spam Block is a command line tool. Please use some Task Scheduler (for example, the built-in Windows Task Scheduler) to run the ***SMISB*** regularly. We recommend running it every 5 to 20 minutes.

Configuration files (in brief)

The main configuration file name is ***smub.exe.config***, it is a text file, please use Notepad to edit it. There are also several TXT files with additional parameters:

- ***mail.template.txt*** – email template. This template is used to send notifications about the blocked mailboxes to the mail server administrator.
- ***throttling.params.txt*** – custom settings for mailboxes of your choice. Using this list you can set higher (or lower) limits for some mailboxes.
- ***white.domains.txt*** – the list of whitelisted domain names. The SMISB won't monitor and block these domain names. They are allowed to send unlimited emails.
- ***white.mailboxes.txt*** – the list of whitelisted mailboxes. The SMISB won't monitor and block these mailboxes. They are allowed to send unlimited emails.

There is also one special TXT file: ***blocked.txt*** – blocked mailboxes list. This file should not be edited by server administrators. The ***SmarterMail Internal Spam Block*** tool edits that file itself.

License key and administrator credentials

The ***SMISB*** needs the SmarterMail ***server admin*** user name and password to be specified in ***smub.exe.config*** file. By default the server admin user name is: ***admin***

Please find the following text in the configuration file and replace appropriate strings (bold text between <value> and </value> tags) with your server admin username, password and license key:

<smub.Properties.Settings>

<setting name="SmServerAdmin" serializeAs="String">

<value>***admin***</value>

</setting>

<setting name="SmServerPassword" serializeAs="String">

<value>***[-- PASSWORD HERE --]***</value>

</setting>

…

<setting name="KeySysKey" serializeAs="String">

<value>***[-- LICENSE KEY HERE --]***</value>

</setting>

Endpoint addresses (if you run the SMISB on your mail server)

If you run the ***SmarterMail Internal Spam Block*** on your mail server the default endpoints specified in the ***smub.exe.config*** configuration file should work. They are:

<endpoint address="http://***127.0.0.1:9998***/Services/svcDomainAdmin.asmx"

binding="basicHttpBinding" bindingConfiguration="svcDomainAdminSoap"

contract="SMDA.svcDomainAdminSoap" name="svcDomainAdminSoap" />

<endpoint address="http://***127.0.0.1:9998***/Services/svcUserAdmin.asmx"

binding="basicHttpBinding" bindingConfiguration="svcUserAdminSoap"

contract="SMUA.svcUserAdminSoap" name="svcUserAdminSoap" />

However if your mail server has different settings you should specify appropriate IP address (or domain name) and port in the configuration file.

For example:

address="http://192.168.10.2:87/Services/svcDomainAdmin.asmx"

or

address="http://my-mail-server.com/Services/svcDomainAdmin.asmx"

Endpoint addresses (if you run the SMISB on a PC)

We highly recommend to run **SmarterMail Internal Spam Block** *on your mail server for security and performance reasons.*

It is the same as when you run the app on your server (see above), but you need to specify the remote (external) endpoint addresses.

Thus, localhost:9998 or 127.0.0.1:9998 won't work.

If the webmail address is, let's say,

http://my-mail-server.com

the endpoint address is most probably

http://my-mail-server.com/Services/svcDomainAdmin.asmx

The mail server IP address may work too. For example:

http://123.123.123.123/Services/svcDomainAdmin.asmx

Be sure the server firewall allows access to ASMX web services and to the endpoint URL.

How to test the endpoint address

Just copy/paste the endpoint address from the configuration file to your browser URL field and open that page. If you see the list of the server functions the endpoint works fine. If you see an error message there are 3 most probable reasons: "incorrect address", "incorrect admin password" or "firewall blocks access to this address".

SSL

It is possible to use HTTPS instead of HTTP for better security.

You must have a valid SSL certificate installed on your mail server and bind it to appropriate endpoint URL.

First of all you have to specify the https endpoint address in the configuration file.

(For example: endpoint address="httpS://my-mail-server.com/Services/svcDomainAdmin.asmx")

And then add

<security mode="Transport" />

between <binding> and </binding> tags (for both svcDomainAdminSoap and svcUserAdminSoap) in <basicHttpBinding> section of ***smub.exe.config***.

Main settings (in smub.exe.config)

- ***GlobalThrottlingSentCount*** – daily limit of sent email messages per mailbox. It is a global parameter. (You can change the limit for particular mailboxes in ***throttling.params.txt*** configuration file). ***Default: 1550***
- ***GlobalThrottlingSentAction*** – action that should be taken by the ***SMISB*** if some mailbox exceeds the "sent" limit. Possible values: ***block*** – block that mailbox, ***none*** – do not block (just write the info to the log file). ***Default: block***
- ***GlobalThrottlingRecvCount*** – similar to ***GlobalThrottlingSentCount*** , but for received messages. ***Default: 2000***
- GlobalThrottlingRecvAction – similar to ***GlobalThrottlingSentAction*** , but for received messages. ***Default: none***

> *There are also **StatsTimeBegin** (00:00:00) and **StatsTimeEnd** (23:59:59) parameters. Do not change them, please!*

Notification settings (in smub.exe.config)

- ***UseAlertMail*** – send an email notification to the mail server administrator (when some mailbox is blocked). ***Default: True***
- ***UseAlertURL*** – open an URL (some custom notification script) when some mailbox is blocked. ***Default: True***
- AlertURL – the URL to open if ***UseAlertURL*** is ***True***.
  Default:
  http://server.zone/handler.php?mailbox=[#MAILBOX#]&sent=[#MESSAGES_SENT#]&recv=[#MESSAGES_RECV#]
  Variables (to be filled by the ***SMISB***): ***[#MAILBOX#]*** – blocked mailbox name, ***[#MESSAGES_SENT#]*** – number of sent messages, ***[#MESSAGES_RECV#]*** – number of received messages.
- ***SmtpHost*** – SMTP server address (the ***SMISB*** will use it to send the notifications). ***Default: localhost***
- ***SmtpPort*** – SMTP port. ***Default: 25***
- ***SmtpFrom*** – "From:" address of the notification emails. ***Default: alert-smub@hoststools.com***

> *Be sure you replace the default value!*

- ***SmtpTo*** – "To:" address of the notification emails. ***Default: support@server.zone***

> *Be sure you replace the default value!*

- ***SmtpSubject*** – subject of the notification emails. ***Default: Alert – SmarterMail mailbox exceeds its limit***
- ***SmtpAuthUser*** – SMTP user name.
- ***SmtpAuthPassword*** – password of the ***SmtpAuthUser***.

Blocked.txt – blocked mailboxes list

blocked.txt file contains the list of blocked mailboxes. There are tab-separated values (one mailbox per line):

MAILBOX< tab_stop_character_here>***DATETIME***

The ***SmarterMail Internal Spam Block*** puts a mailbox to this list when it exceeds the daily limit. At the same moment the ***SMISB*** disables the mailbox so it can not send any emails. However, the ***SMISB*** can block any particular mailbox only once a day.

> *So, if you enable some blocked mailbox manually, you must remove it from blocked.txt file too! Otherwise the SMISB "thinks" the mailbox is still blocked. See "**How it works?**" paragraph above for more info.*

Mail.template.txt – administrator email notification template

Mail.template.txt file contains an email notification template. (When the ***SMISB*** sends a notification about blocked mailboxes to the mail server administrator it uses this template.)

The default template is simple. But you can edit it, of course.

There are 3 variables (to be filled by the ***SMISB***): ***[#MAILBOX#]*** – blocked mailbox name, ***[#MESSAGES_SENT#]*** – number of sent messages, ***[#MESSAGES_RECV#]*** – number of received messages.

Throttling.params.txt – custom settings for mailboxes of your choice

Using this list you can set higher (or lower) limits for some mailboxes.

> *Specify one mailbox per line.*

Format:

MAILBOX, ***SENT***, ***RECV***

Where ***SENT*** has the following format: ***SENT_MESSAGES_COUNT#ACTION***

Where ***RECV*** has the following format: ***RECEIVED_MESSAGES_COUNT#ACTION***

Where ***ACTION*** can be either ***block*** (block this mailbox (or domain) if it exceeds the limit) or ***none*** (do not block, just write to the log file).

Example:

test.com,1000#block,500#none

info@MySite.com,1500#block,1000#none

white.domains.txt – the list of whitelisted domain names

The ***SMISB*** won't monitor and block these mail domains. They are allowed to send unlimited emails.

Specify one domain per line.

Example:

myhostingdomain.com

somecustomerdomain.com

white.mailboxes.txt - the list of whitelisted mailboxes

The ***SMISB*** won't monitor and block these mailboxes. They are allowed to send unlimited emails.

Specify one mailbox per line.

Example:

support@myhostingemail.com

sales@myhostingemail.com

Troubleshooting

If any troubles, first of all, please take a look at the application log files and Windows Event Logs. In most cases it helps to find the problem reason and fix the problem.

And of course, you can contact support@hoststools.com for support. If you decide to contact HostTools support team, please send us the app log files and the error message text (or its screenshot).

Please also add support@hoststools.com and sales@hoststools.com to your address book to be sure you get the reply direct to your Inbox (despite all those aggressive spam filters).

Thank you for using our software!