Managing SpamExperts service

- 2021-08-02 - SpamExperts

SpamExperts is a service provided for free with all of Top.Host's web hosting plans or you can activate it in VPS or Dedicated hosting, by choosing one of the SpamExperts Packs.

1. In order to activate the service for your shared hosting plan, you can follow the instructions mentioned here.

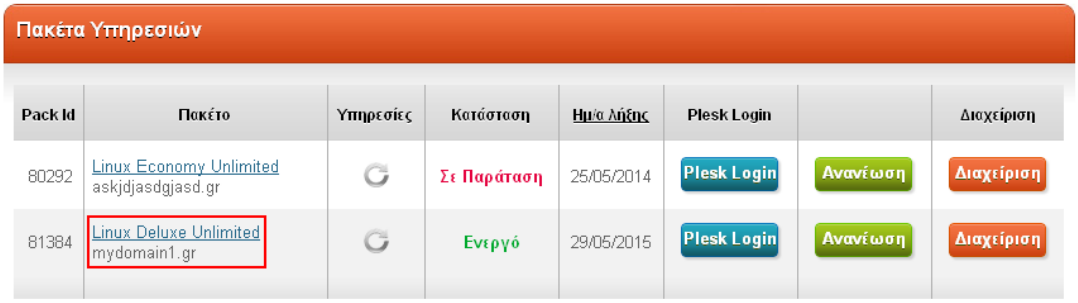
2. In order to activate the service in VPS or Dedicated hosting, you can follow the instructions mentioned here.

Managing SpamExperts service

1. Once the service is activated, you can **log into** SpamExperts control panel.

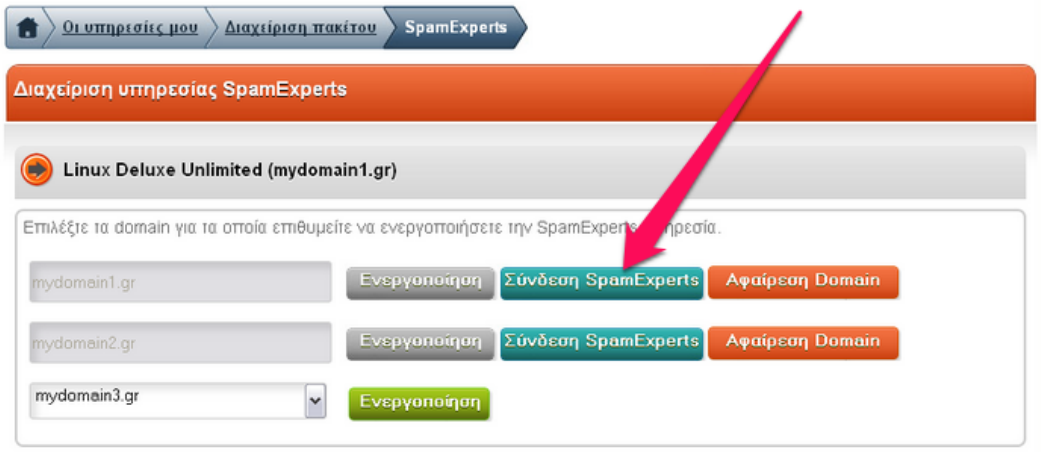
a) Log into myTophost Panel.

b) Click on **Manage** on the right, next to the hosting plan with the domain name whose SpamExperts service you wish to log into.



c) Click on **Manage Spam Experts**.

d) Click on **Connect Spam Experts**.



---

2. Options for **black & white lists**:

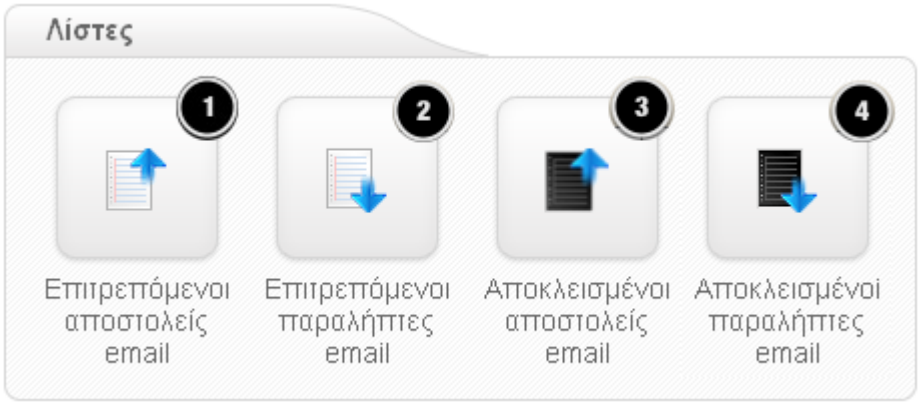
No1 - Allowed email senders: Here, you can define the email addresses you always want to receive emails from. You can enter separate sending addresses, e.g. info@randomdomain.gr or enter all the domain's mail-user accounts, simply by adding the corresponding domain, e.g. randomdomain.gr

No2 - Allowed email receivers: Here, you can define the approved receiver addresses of

your domain. Any email that is sent to these accounts, will always bypass all filters.

No3 - Excluded email senders: Here, you can define the email addresses that you want to block from sending you emails. You can enter separate addresses, e.g. info@randomdomain.gr or enter all the user-mail sending accounts for a domain, by entering the corresponding domain, e.g. randomdomain.gr

No4 - Excluded email receivers: Here, you can define the receiver addresses of your domain, from whom you want to exclude all incoming email.



---

3. Options for **Incoming email** (*cf. image*):

No1 - Researching logs: Allows you to research logs from the last 28 days for a specific incoming email.

No2 - Undesired quarantine: Here, you can find all the emails for your domain, which have been permanently blocked from the filtering system. You can delete them forever or allow them to be delivered.

No3 - Delivery waiting list: Here, you will find emails that are “on hold” to be delivered to your email along with the reason why the delivery was delayed. You have the option to

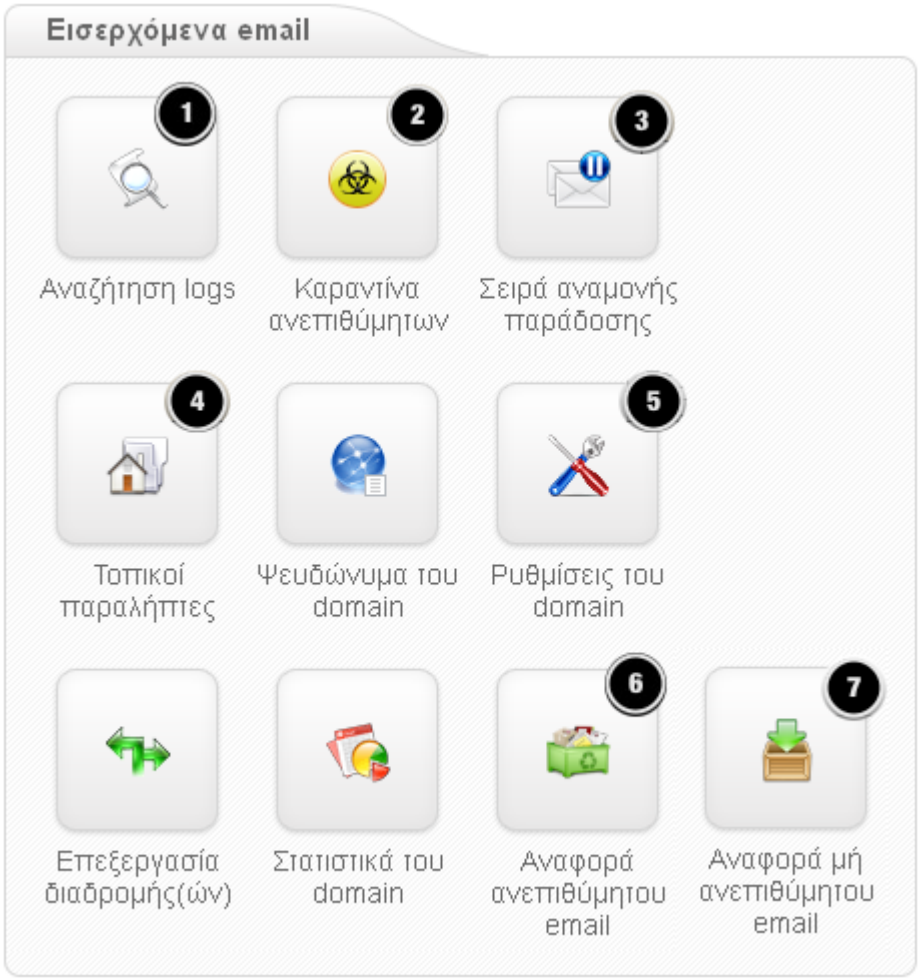
“force” the reception.

No4 - Local receivers: If you activate the **Use of local receivers**, the system will only accept messages destined to the receivers that you have defined in the list. Emails sent to receivers that are not on the list, will be permanently deleted.

No5 - Domain settings: Here, you can define the contact information, the maximum bounce number, enable/disable the registration of non valid receivers etc.

No6 - Reporting undesired email: Test your filter by uploading undesired messages to .eml files. A .eml file contains a header with the sender & receiver email addresses, the subject, the date, the time and mostly the body with the text of the email.

No7 - Reporting a non undesired email: Test your filter by uploading “non undesired emails” to .eml files.

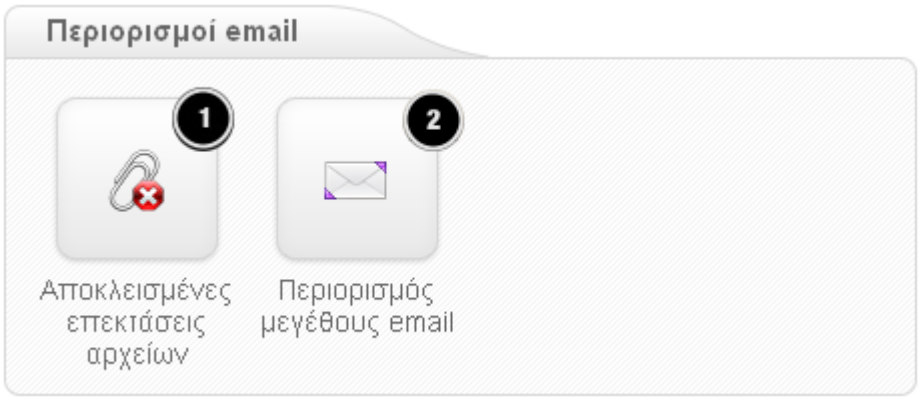


---

4. Options for **Email restriction** (*cf. image*)

No1 - Excluded file extensions: Define the emails to be excluded, based on the extension of the attached documents.

No2 - Email size restriction: You can leave the option "0", so that the size restriction applied is the one defined by Top.Host in the mail server (**16MB per email**). Otherwise, you can define a smaller size (below 16MB) and have the emails that exceed this limit, quarantined.



---

5. Options for **Service users**.

No1 - Managing email users: Here, you can add unique email users, which have the possibility to immediately log into the spam control panel to manage their email and quarantine settings.

No2 - Managing rights: Define the user rights when it comes to managing their emails.