



4PSA Spam Guardian 2.0.5
for Plesk 7.x Reloaded
User's Guide

Manual Version 0.92

For suggestions regarding this manual contact:

docs@4psa.com

© Copyrights 2002 – 2005 Rack-Soft. All rights reserved

Distribution of this work or derivative of this work is prohibited unless prior written permissions is obtained from the copyright holder.

Plesk is a Registered Trademark of SWsoft, Inc.

Linux is a Registered Trademark of Linus Torvalds.

RedHat is a Registered Trademark of Red Hat Software, Inc.

FreeBSD is a Registered Trademark of FreeBSD, Inc.

All other trademarks and copyrights are the property of their respective owners.

Table of Contents

Chapter 1. About 4PSA Spam Guardian 2.0.5.....	5
4PSA Spam Guardian 2.0.5 Features.....	5
Chapter 2. The Administrator Module	6
1. Protecting Domains Globally.....	7
Protecting the Entire Domain.....	8
Domain Statistics.....	8
Settings for Domain.....	10
Protecting Individual Mailboxes.....	14
Mailbox Statistics.....	15
Settings for Mailbox.....	17
2. Management Permissions	20
3. Statistics.....	21
Server Statistics Graph.....	22
Customize	22
Server Statistics	22
4. Server-Wide Settings	23
4PSA Spam Guardian Reports.....	23
Spam Engine Settings	24
White List Settings.....	25
Black List Settings	26
Trusted Networks	27
4PSA Spam Guardian Settings	28
Interface Settings.....	28
5. License Management.....	29
6. Testing Spam Settings	29
6. How to use the spam learning features of 4PSA Spam Guardian	30
Chapter 3. The Client Module	31
1. Protecting Domains Globally.....	32
Protecting the Entire Domain.....	32
Domain Statistics.....	33
Settings for Domain	34

Protecting Individual Mailboxes	38
Mailbox Statistics	39
Settings for Mailbox	41
2. Management Permissions	44
Chapter 4. The Domain User Module	45
1. Protecting the Entire Domain.....	45
Domain Statistics.....	46
Settings for Domain	48
2. Protecting Individual Mailboxes.....	52
3. Mailbox Statistics	53
Mailbox Statistics Graph.....	53
Customize	53
Mailbox Statistics.....	54
4. Settings for Mailbox	55
Spam Engine Settings for Mailbox	55
White List Settings for Mailbox.....	56
Black List Settings for Mailbox	57
Trusted Networks for Mailbox	57
Chapter 5. The Email User Module	58
1. Protecting the Mailbox.....	58
2. Mailbox Statistics	59
Mailbox Statistics Graph.....	60
Customize	60
Mailbox Statistics.....	60
3. Settings for Mailbox	61
Spam Engine Settings for Mailbox	62
White List Settings for Mailbox.....	63
Black List Settings for Mailbox	63
Trusted Networks for Mailbox	64
Appendix A. Server Compatibility.....	67



Chapter 1. About 4PSA Spam Guardian 2.0.5

4PSA Spam Guardian 2.0.5 is a server-level application that provides spam protection for the mailboxes on Plesk 7.x Reloaded servers. 4PSA Spam Guardian 2.0.5 has independent administrator, client and domain user modules to offer advanced, browser based management of the mailbox spam protection services.

4PSA Spam Guardian 2.0.5 Features

- Separate client, domain user and administrator modules
- Protect entire domains
- Protect separate mailboxes
- Improved spam detection using daily anti-spam definitions
- Client and domain user 4PSA Spam Guardian access permissions
- Separate client, domain user, email user and administrator modules
- Processed spam statistics
- Forward spam to other email addresses
- Automatic Bayesian learning process
- Advanced rendering engine for real time graphs generation
- Advanced server-wide spam filtering settings (details below)
 - Forward Spam - Can forward tagged spam or drop it
 - Required Hits - Number of hits required to match email as spam
 - White list - Email addresses or domains that are automatically trusted
 - Black list - Email addresses or domains that are automatically blocked
 - Trusted networks - Network addresses fully trusted
- Import black lists, white lists and trusted networks from text files
- Export black lists, white lists and trusted networks to text files
- Per domain spam detection settings
- Definable spam email tag text
- High performance low level C scripts
- No Qmail modification/patch necessary

- Uses SpamAssassin Open Source software as the spam engine
- SpamAssassin performance improved by 4PSA modules
- SpamAssassin 2.x and 3.x support
- Administrator easy management settings:
 - Automatically protect new domains
 - Automatically allow new clients to access the interface
 - Allow inheritance of White List, Black List and Trusted Networks settings
- Language packs support

Chapter 2. The Administrator Module

The 4PSA Spam Guardian administrator module can be accessed after you login to Plesk 7.x Reloaded using the admin account. In order to open the 4PSA Spam Guardian interface click the [4PSA Spam Guardian](#) link available in the Custom navigation menu located on the left side of the Plesk interface.



Note

When you install the product for the first time no client is allowed to access 4PSA Spam Guardian and no access link is available in the navigation menu. In order to give access rights to your hosting customers you must access 4PSA Spam Guardian after you login as admin to your Plesk 7.x Reloaded server. Then check the Permissions area to give access permissions to your clients. Further information is available in this chapter.

The 4PSA Spam Guardian tool bar is available on top of the application's interface. The tool bar provides an easy method for the server administrator to setup domains and mailbox protection, view mailbox, domain and server wide statistics, change domain and mailbox settings, give management permissions to clients and domain users, view a report about 4PSA Spam Guardian, setup server-wide settings for the spam detection engine, change interface settings, and manage the 4PSA Spam Guardian license key.

1. Protecting Domains Globally

The server administrator can protect entire domains against spam messages in the Domains area. In order to access this area, the administrator must click the **Domains** button available in the tool bar.

In this area the server administrator can view a list of all domains hosted on server. Next to the domain names 3 columns display the following information:

Protected mailboxes – The number of protected mailboxes on the domain

Total mailboxes – The total number of mailboxes on the domain

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the domain (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that domain.





Note

These statistics are available only if at least one mailbox that belongs to that domain is protected by 4PSA Spam Guardian and if the **Save statistics** option is enabled in the Settings area.

Next to these columns 3 action icons are available for each domain in the list:

Stats - By clicking the  **Statistics** icon, the server administrator will be able to view the statistics available for the selected domain

S - By clicking the  **Settings** icon, the server administrator will be able to define settings for the selected domain

Reset stats – By clicking the  **Reset statistics** icon, the server administrator will reset the statistics available in the Dropped/Total column for the corresponding domain. Both dropped and total statistics for the chosen domain will be reset.



Note

This column is available only if at least one mailbox that belongs to that domain is protected by 4PSA Spam Guardian and if the **Save statistics** option is enabled in the Settings area.


Protecting the Entire Domain

Protecting a domain means that all mailboxes available under this domain will be protected against spam messages. All the mailboxes added later to a protected domain will be automatically protected by 4PSA Spam Guardian.

To protect an entire domain, check the "Protect" checkbox for the chosen domain and click **Update**. You can later disable domain protection by unchecking the same checkbox and clicking **Update**.

The domain protection can be enabled/disabled for multiple domains at the same time.

Domain Statistics

To view the statistics for an entire domain, the server administrator must click the  **Stats** icon corresponding to the selected domain. A graphic with the domain statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian and the number of messages dropped by the spam engine for the selected domain.




The domain statistics are available only if at least one mailbox that belongs to that domain is protected by 4PSA Spam Guardian and if the **Save statistics** option is enabled in the Settings area.

Domain Statistics Graph

In this graph one curve represents the total number of emails received by the selected domain and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by the selected domain and dropped by the spam engine. The server administrator can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the selected domain and processed by the spam engine.

Customize

In this area the server administrator can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the server administrator must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by the selected domain and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by the selected domain and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Domain Statistics

In this area 4PSA Spam Guardian displays information about the domain statistics.

Total - The total number of emails received by the domain and processed by the spam engine

Dropped - The number of email messages received by the domain and dropped by the spam engine

Average processed - The average number of email messages received by the domain and processed every day by the spam engine

Average dropped - The average number of email messages received every day by the domain and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages for the domain. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages for the domain. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages for the domain. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages for the domain. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for the domain

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for the domain

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for the domain

The **Reset** button available in this area allows the server administrator to clear statistics for the selected domain. Both dropped and total statistics for the domain will be reset. The global statistics available in the Settings area will be updated by this reset.

Settings for Domain

In order to view the individual settings of the chosen domain the server administrator must click the  Settings icon on the domain row. In this area the server administrator can modify the spam engine settings that apply to the chosen domain.



Tip

Settings for mailboxes override settings for the corresponding domains. Settings for domains override global settings for server. If you want to enable higher or lower limits for a particular mailbox, change settings individually in the Settings for mailbox area.

Spam Engine Settings for Domain

In this area the server administrator can modify the settings of the spam engine for the chosen domain.

Reset domain settings - To reset the spam engine settings for the domain, the server administrator must enable this option and click **Update**. The domain settings will be reset to the global server settings.

Drop spam messages - When this option is enabled, 4PSA Spam Guardian will delete all spam messages received in the mailboxes of the chosen domain.

Spam message as attachment - When this option is enabled and a message received in one of the mailboxes of the chosen domain is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient announcing him that he has received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



Note

The **Drop spam messages** option cannot be enabled in the same time with the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag - When the previous option is enabled, the server administrator can write in this field the subject that he wants to be used for spam message tagging.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The server administrator can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the server administrator chooses the first option, he can write the value he wants in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Domain

Email messages originating from the addresses in the White list will not be processed by the spam protection engine.



Note

You can use wildcards for the White list entries: ***** to match any number of characters and **?** to match a single character. For security reasons, regular expressions are not allowed.

Email address - In this field the server administrator can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the domain’s White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Domain

Email messages originating from the addresses in the Black list will be tagged as spam.



Note

You can use wildcards for the Black list entries: ***** to match any number of characters and **?** to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the server administrator can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses – These are the email addresses currently available in the domain's Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Domain

Email messages originating from the networks in this list will not be processed by the spam protection engine. You can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 – single IP address

192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address – In this field the server administrator can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the domain's trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select


the name of the file and the path on your local machine where you want to save the file.


Protecting Individual Mailboxes


The server administrator can protect individual mailboxes against spam messages. The number of protected mailboxes for every hosted domain is available in the Protected Mailboxes column. For more details about the mailboxes, follow the link on the chosen domain name.

In the Mailbox protection area, the following columns are available next to the mailbox name:

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the mailbox (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that mailbox.

Stats - By clicking the  **Statistics** icon, the server administrator will be able to view the statistics available for the selected mailbox

S - By clicking the  **Settings** icon, the server administrator will be able to define settings for the corresponding mailbox

Reset stats – By clicking the  **Reset statistics** icon, the server administrator will reset the statistics available in the Dropped/Total column for the corresponding mailbox. Both dropped and total statistics for the chosen mailbox will be reset.



The statistics and the Reset stats column are available only if the corresponding mailbox is protected by 4PSA Spam Guardian and if the **Save statistics** option is enabled in the Settings area.

When no messages are processed, - is displayed in the Dropped/Total column on the corresponding mailbox row.

Protect – When enabled, 4PSA Spam Guardian protects the corresponding mailbox against spam messages




Note

When a domain is protected, all its mailboxes are protected and the corresponding “Protect” checkboxes are grayed out.

To protect a mailbox, check the “Protect” checkbox for the chosen mailbox and click **Update**. You can later disable mailbox protection by unchecking the same checkbox and clicking **Update**.

The mailbox protection can be enabled/disabled for multiple mailboxes at the same time.

Mailbox Statistics

To view the statistics for a protected mailbox, the server administrator must click the  **Stats** icon corresponding to the chosen mailbox. A graphic with the mailbox statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian for this mailbox and the number of messages received by this mailbox and dropped by the spam engine.



Note


The mailbox statistics are available only if the mailbox is protected by 4PSA Spam Guardian and if the **Save statistics** option is enabled in the Settings area.

Mailbox Statistics Graph

In this graph one curve represents the total number of emails received by the mailbox and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by this mailbox and dropped by the spam engine. The server administrator can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the mailbox and processed by the spam engine.

Customize

In this area the server administrator can change the time interval displayed in the graph and the graph’s look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the server administrator must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by this mailbox and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by this mailbox and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Mailbox Statistics

In this area 4PSA Spam Guardian displays information about the mailbox statistics.

Total - The total number of emails received by this mailbox and processed by the spam engine

Dropped - The number of email messages received by this mailbox and dropped by the spam engine

Average processed - The average number of email messages received by this mailbox and processed every day by the spam engine

Average dropped - The average number of email messages received every day by this mailbox and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for this mailbox

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for this mailbox

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for this mailbox

The **Reset** button available in this area allows the server administrator to clear statistics for the selected mailbox. Both dropped and total statistics for the mailbox will be reset. The global statistics available in the Settings area will be updated by this reset.

Settings for Mailbox

In order to view the individual settings of the chosen mailbox the server administrator must click the  **Setting** icon on the chosen mailbox row. In this area the server administrator can modify the limits that apply to the selected mailbox.



Tip

Settings for mailboxes override settings for the corresponding domains. Settings for domains override global settings for server.

Spam Engine Settings for Mailbox

In this area the server administrator can modify the settings of the spam engine for the selected mailbox.

Reset mailbox settings – To reset mailbox settings, the server administrator must enable this option and click **Update**. The mailbox settings will be reset to the global server settings or to the domain settings (if these exist).

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all messages detected as spam received in the mailbox.

Spam message as attachment - When this option is enabled and a message received in the mailbox is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient to announce him that he has received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



Note

The **Drop spam messages** option cannot be enabled in the same time with the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag – When the previous option is enabled, the server administrator can write in this field the subject that he wants to be used for spam message tagging.

Enable spam forwarding – When this option is enabled, spam messages are forwarded to a different email address. Only the messages supposed to be clean reach the mailbox.

Forward spam to address – When the option **Enable spam forwarding** is enabled, this is the address where spam messages are forwarded. The forward address must be on the same domain.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The server administrator can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the server administrator chooses the first option, he can write the value he wants in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Mailbox

Email messages originating from the addresses in the White list and received in the chosen mailbox will not be processed by the spam protection engine.

Email address – In this field the server administrator can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the mailbox White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list and received in the chosen mailbox will be tagged as spam.

Email address – In this field the server administrator can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses – These are the email addresses currently available in mailbox Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Mailbox

Email messages originating from the networks in this list and received in the chosen mailbox will not be processed by the spam protection engine. You can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 – single IP address
192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork



Note

This trusted network list is valid only for the selected mailbox.

IP address – In this field the server administrator can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the mailbox trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

2. Management Permissions

In this area (click the **Permissions** button available in the tool bar) the server administrator can grant 4PSA Spam Guardian management permissions to clients and domain users on the Plesk server. This means that clients and domain users will be able to choose for themselves which domains or mailboxes to protect from spam messages.

To grant management permissions to a client, check the “Allow access” checkbox on the chosen client row and click **Update**. The administrator can later

disable management permissions by unchecking the same checkbox and clicking **Update**. When management permissions are granted to a client, a custom link will be displayed in the Plesk navigation menu available in that client account. This link will be removed automatically when the management permissions are revoked.

The server administrator can grant / revoke management permissions for multiple clients at the same time.



Note

If you disable management permissions for a client, all domain users on the domains belonging to that client will not be able to access 4PSA Spam Guardian. The [4PSA Spam Guardian](#) link will not be available in the navigation menu.

To grant management permissions to a domain user, click the name of the client who owns the domain for which you want to enable management permissions. In the domain list that appears in the next page, check the "Allow access" checkbox corresponding to the chosen domain and click **Update**. You can later disable management permissions by unchecking the same checkbox and clicking **Update**.

The management permissions can be granted / revoked for multiple domain users at the same time.



Note

You must grant management permissions to the client owning the domain in order to grant management permissions to his domain users.

3. Statistics


In this area (click the **Statistics** button available in the tool bar) the server administrator can view a graph and information about the server wide statistics. These statistics are based on the total number of emails processed by 4PSA Spam Guardian and the number of messages received on the server and dropped by the spam engine.

Server Statistics Graph

On this graph one curve represents the total number of emails received and processed by 4PSA Spam Guardian on the server. The other curve represents the number of messages received on the server and dropped by the spam engine. The server administrator can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received on the server and dropped by the spam engine.

Customize

In this area the server administrator can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the server administrator must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received on the server and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received on the server and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Server Statistics

In this area 4PSA Spam Guardian displays information about the server statistics.

Total - The total number of emails received on the server and processed by the spam engine

Dropped - The number of email messages received on the server and dropped by the spam engine

Average processed - The average number of email messages received on the server and processed every day by the spam engine

Average dropped - The average number of email messages received every day on the server and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine on the server.

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails on the server.

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails on the server.

The **Reset** button available in this area allows the server administrator to reset statistics for the entire server. Both dropped and total statistics for the entire server will be reset.

4. Server-Wide Settings

In this area (click the **Settings** button available in the tool bar) the server administrator can view details about 4PSA Spam Guardian, modify the settings of the spam engine, add and remove items from the White list, Black list and Trusted networks list, settle management permissions for clients and domain users, and change interface settings.

4PSA Spam Guardian Reports

This area provides the following information about 4PSA Spam Guardian:

Product version – The version of the 4PSA Spam Guardian installed on the server

Spam Assassin engine version – The version of the Spam Assassin engine installed on the server

Total number of protected mailboxes – The total number of protected mailboxes on the server

Total number of dropped emails – The total number of email messages identified as spam and dropped by 4PSA Spam Guardian

Total number of processed emails – The total number of email messages processed by 4PSA Spam Guardian

Number of SPAM messages used for training – The total number of SPAM messages used by 4PSA Spam Guardian Bayesian filter to learn about spam

Number of HAM messages used for training – The total number of HAM messages used by Spam Guardian Bayesian filter to learn about clean messages

Spam Engine Settings

In this area the server administrator can modify the settings of the spam engine.

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all messages detected as spam.

Spam message as attachment - When this option is enabled and a message is detected to be spam, 4PSA Spam Guardian will send an email to the message recipient to announce him that he has received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



The **Drop spam messages** option cannot be enabled in the same time with the **Spam message as attachment** and **Modify spam message subject** options.

Spam message subject tag – When the previous option is enabled, the server administrator can write in this field the subject that he wants to be used for spam messages tagging.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The server administrator can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the server

administrator chooses the first option, he can write the value he wants in the Custom value field.

Save Statistics - When this option is enabled, usage statistics for processed and spam dropped messages are saved by 4PSA Spam Guardian.

Storage email address used for SPAM messages training - 4PSA Spam Guardian will learn about the messages arrived at this email address as being SPAM.

Storage email address used for HAM messages training - 4PSA Spam Guardian will learn about the messages arrived at this email address as being HAM.



Note

Messages in these email accounts will be automatically erased every 24 hours.

The system will also learn from the IMAP folders called *junk_learn* and *ham_learn* on every mailbox on the server.

All messages in the *junk_learn* folders will be learned as spam. Copy to this folder messages that are not detected by the engine as spam.

All messages in the *ham_learn* folders will be learned as ham. Copy to this folder messages that are detected by the engine as spam and they are not.

The messages on the *junk_learn* and *ham_learn* folders will also be erased automatically every 24 hours.

The *junk_learn* and *ham_learn* folders must be IMAP folders created in every mailbox where you want the system to learn spam and ham from. You can manage IMAP folders from webmail or from any email client that supports IMAP.

In order to save the changes you must click **Update**.

White List Settings

Email messages originating from the addresses in the White list will not be processed by the spam protection engine.



Note

You can use wildcards for the White list entries: * to match any number of characters and ? to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the server administrator can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file that contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings

Email messages originating from the addresses in the Black list will be tagged as spam.



Note

You can use wildcards for the Black list entries: * to match any number of characters and ? to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the server administrator can write the email addresses. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file that contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks

Email messages originating from the networks in this list will not be processed by the spam protection engine. You can include on this list single IP addresses, an entire network or subnetwork.

Example: 192.168.1.1 – single IP address
192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address – In this field the server administrator can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file that contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

4PSA Spam Guardian Settings

In this area are available several options which reduce the administration effort.

Allow 4PSA Spam Guardian access to new clients and domain users - When this option is enabled, all new added clients and domain users will have access to 4PSA Spam Guardian.

Automatically protect new domains - When this option is enabled, all new added domains will be automatically protected.

Allow clients to set permissions and activate protection for domains - When enabled, clients are able to change 4PSA Spam Guardian access and protection permissions for their domain users. Disable this option to prevent abuse.

Allow domain spam engine settings - When this option is enabled, clients are able to change the domain spam engine settings.

Allow mailbox spam engine settings - When this option is enabled, clients and domain users are able to change the mailbox spam engine settings.

Allow inheritance of White List, Black List and Trusted Networks settings – When this option is enabled, the settings from the White list, Black list and Trusted Networks list are inherited from the superior level. For example, mailboxes with particular settings inherit these settings from domains, while domains with particular settings inherit server settings.

Interface Settings

In this area the server administrator can choose the interface settings.

Language - Allows the server administrator to select the language that will be used by 4PSA Spam Guardian's interface.

Custom button title - The name of the custom button in the left panel. The server administrator can change the default 4PSA Spam Guardian with a more descriptive name for his clients.

Context help - The 4PSA Spam Guardian application description that will appear in the left navigation panel.

5. License Management

In this area you can manage the 4PSA Spam Guardian license. In order for 4PSA Spam Guardian to work correctly, a valid license key must be loaded. The license key must be generated by 4PSA based on your server IP and Plesk version installed on your server.

License key - The license key number. This is the key currently loaded on your server.

License key status - The status of the currently loaded license key.

Your server IP - The main IP address of your server. This is the IP for which the license key must be issued in order to work on this server. If the license is issued for another IP, it will not work.

License file - You can use this form in order to upload the license key to the server. The license key can also be executed in command line using the command: sh keyno.sh. If you can access other pages in 4PSA Spam Guardian there is no reason why you should upload a new key.

6. Testing Spam Settings

To test the spam engine settings you can send a message containing the following string of characters (in upper case and with no white spaces and line brakes)

```
-----  
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X  
-----
```

in the message body. You should send this test email from an account outside your network. The test message will have a spam score of 1,000 hits and it should be detected and tagged as spam by 4PSA Spam Guardian.

6. How to use the spam learning features of 4PSA Spam Guardian

By default automatic learning is enabled in Spam Assassin. The automatic learning features are more advanced in Spam Assassin 3.x, that's why it's recommended to use Spam Assassin 3.x under Linux. Under FreeBSD it's not currently possible to use Spam Assassin 3.x because the Plesk installation is monolithic and Spam Guardian depends on the installed Spam Assassin version.

You can use Spam Guardian for manual learning. The two email addresses that can be setup in Spam Guardian -> Settings:

Storage email address used for SPAM messages training

Storage email address used for HAM messages training

are designed for manual learning. The spam engine will automatically learn from the messages stored in these email accounts. The messages are automatically deleted every 24 hours, after the learning process completes.



Note

These two mailboxes must be created on the server for this special purpose. These messages must not be used for other purposes (regular email communication).

There are multiple ways in how you can get messages to the spam and ham boxes. The most efficient ones are:

1. Set the catch-all email for some domains to the SPAM training email box. Over 99% of the messages sent to an imaginary address are spam. Even if several messages are legitimate, they will not overall influence the spam engine.
2. Manually forward non detected spam messages to the SPAM training email box and clean messages detected as spam to the HAM training email box. Proceed with care, make sure that you do not add headers or content to the original emails.
3. Manually move messages on the server to the SPAM and HAM mailboxes (`<mailnames_path>/<domain>/<spam/ham_mailbox>/Maildir/new` folder). This is the not easiest way, but it can be efficient when working with a lot of messages.

Starting with Spam Guardian 2.0.5, all messages contained in the *junk_learn* and *ham_learn* IMAP folders, on every email account on the server are learned to be spam, respectively ham. The messages are deleted every 24 hours automatically. It's recommended to use this method for learning because it's very fast and efficient (all you have to do is to move the messages from the *Inbox* to the *junk_learn* or *ham_learn* folders, based on the message type (spam or ham)).



Note

Keep in mind that the engine must learn from at least 200 messages in order to be efficient. If you train by mistake a message to be spam or ham you should not worry about this.

Chapter 3. The Client Module

The 4PSA Spam Guardian client module can be accessed after you login to Plesk 7.x using a client level account. In order to open the 4PSA Spam Guardian interface click the [4PSA Spam Guardian](#) link available in the Custom navigation menu located on the left side of the Plesk interface.



Note

In order to access and manage 4PSA Spam Guardian, the client must have permissions from the server administrator.

The 4PSA Spam Guardian tool bar is available on top of the application's interface. The tool bar provides an easy method for the client to setup domain and mailbox protection, view domain and mailbox statistic graphs, change domain and mailbox settings, and give management permissions to domain users.

1. Protecting Domains Globally

The client can protect entire domains against spam messages in the Domains area. In order to access this area, the client must click the **Domains** button available in the tool bar.

In this area the client can view a list of his domains hosted on server. Next to the domain names there are three columns displaying the following information:


Protected mailboxes – The number of protected mailboxes on the domain

Total mailboxes – The total number of mailboxes on the domain

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the domain (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that domain. This column is available only if statistics are enabled on the server.

Next to these columns 3 action icons are available for each domain in the list.

Stats - By clicking the  **Statistics** icon, the client will be able to view the statistics available for the selected domain

S - By clicking the  **Settings** icon, the client will be able to define settings for the corresponding domain.

Reset stats – By clicking the  **Reset statistics** icon, the client will reset the statistics available in the Dropped/Total column for the corresponding domain.



These columns are available only if at least one mailbox that belongs to that domain is protected by 4PSA Spam Guardian and if statistics are enabled on the server.


Protecting the Entire Domain

Protecting a domain means that all mailboxes available under this domain will be protected against spam messages. All the mailboxes added later to a protected domain will be automatically protected by 4PSA Spam Guardian.

To protect an entire domain, check the “Protect” checkbox for the chosen domain and click **Update**. You can later disable domain protection by unchecking the same checkbox and clicking **Update**.

The domain protection can be enabled/disabled for multiple domains at the same time.

Domain Statistics

To view the statistics for an entire domain, the client must click the  **Stats** icon corresponding to the selected domain. A graphic with the domain statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian and the number of messages dropped by the spam engine for the selected domain.




The domain statistics are available only if at least one mailbox that belongs to that domain is protected by 4PSA Spam Guardian and if statistics are enabled on the server.

Domain Statistics Graph

In this graph one curve represents the total number of emails received by the selected domain and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by the selected domain and dropped by the spam engine. The client can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the selected domain and processed by the spam engine.

Customize

In this area the client can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the client must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by the selected domain and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by the selected domain and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Domain Statistics

In this area 4PSA Spam Guardian displays information about the domain statistics.

Total - The total number of emails received by the domain and processed by the spam engine

Dropped - The number of email messages received by the domain and dropped by the spam engine

Average processed - The average number of email messages received by the domain and processed every day by the spam engine

Average dropped - The average number of email messages received every day by the domain and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for the domain

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for the domain

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for the domain

The **Reset** button available in this area allows the client to clear statistics for the selected domain. Both dropped and total statistics for the domain will be reset.

Settings for Domain

In order to view the individual settings of the chosen domain the client must click the  **Settings** icon on the domain row. In this area the client can modify the

settings that apply to the chosen domain. This option is available only if the domain settings are enabled on the server.



Tip

Settings for mailboxes override settings for the corresponding domains. Settings for domains override global settings for server. If you want to enable higher or lower limits for a particular mailbox, change settings individually in the Settings for mailbox area.

Spam Engine Settings for Domain

In this area the client can modify the settings of the spam engine for the chosen domain.

Reset domain settings – To reset the domain settings, the client must enable this option and click **Update**. The domain settings will be reset to the global server settings.

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all spam messages received in the mailboxes of the chosen domain.

Spam message as attachment - When this option is enabled and a message received in one of the mailboxes of the chosen domain is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient to announce him that he has received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



Note

The **Drop spam messages** option cannot be enabled in the same time with the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag – When the previous option is enabled, the client can write in this field the subject that he wants to be used for spam message tagging.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam.

Messages that have scored a value above the set value will be tagged as spam. The client can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the client chooses the first option, he can write the value he wants in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Domain

Email messages originating from the addresses in the White list will not be processed by the spam protection engine.



Note

You can use wildcards for the White list entries: * to match any number of characters and ? to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the client can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the domain's White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Domain

Email messages originating from the addresses in the Black list will be tagged as spam.



Note

You can use wildcards for the Black list entries: * to match any number of characters and ? to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the client can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses – These are the email addresses currently available in the domain's Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Domain

Email messages originating from the networks in this list will not be processed by the spam protection engine. You can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 – single IP address
192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address – In this field the client can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the domain's trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.


Protecting Individual Mailboxes

The client can protect individual mailboxes against spam messages. The number of protected mailboxes for every hosted domain is available in the Protected Mailboxes column. For more details about the mailboxes, follow the link on the chosen domain name.

In the Mailbox protection area, the following columns are available next to the mailbox name:

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the mailbox (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that mailbox. This column is available only if statistics are enabled on the server.

Stats - By clicking the  **Statistics** icon, the client will be able to view the statistics available for the selected domain

S - By clicking the  **Settings** icon, the client will be able to define settings for the corresponding mailbox.

Reset stats – By clicking the  **Reset statistics** icon, the client will reset the statistics available in the Dropped/Total column for the corresponding mailbox.



Note

This column is available only if the mailbox is protected by 4PSA Spam Guardian and if statistics are enabled on the server.

Protect – When enabled, 4PSA Spam Guardian protects the corresponding mailbox against spam messages.




Note

When a domain is protected, all its mailboxes are protected and the corresponding “Protect” checkboxes are grayed out.

To protect a mailbox, check the “Protect” checkbox for the chosen mailbox and click **Update**. You can later disable mailbox protection by unchecking the same checkbox and clicking **Update**.

The mailbox protection can be enabled/disabled for multiple mailboxes at the same time.

Mailbox Statistics

To view the statistics for a protected mailbox, the client must click the  **Stats** icon corresponding to the chosen mailbox. A graphic with the mailbox statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian for this mailbox and the number of messages received by this mailbox and dropped by the spam engine.



Note


The mailbox statistics are available only if the mailbox is protected by 4PSA Spam Guardian and if the statistics are enabled on the server.

Mailbox Statistics Graph

In this graph one curve represents the total number of emails received by the mailbox and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by this mailbox and dropped by the spam engine. The client can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the mailbox and processed by the spam engine.

Customize

In this area the client can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the client must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by this mailbox and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by this mailbox and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Mailbox Statistics

In this area 4PSA Spam Guardian displays information about the mailbox statistics.

Total - The total number of emails received by this mailbox and processed by the spam engine

Dropped - The number of email messages received by this mailbox and dropped by the spam engine

Average processed - The average number of email messages received by this mailbox and processed every day by the spam engine

Average dropped - The average number of email messages received every day by this mailbox and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for this mailbox

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for this mailbox

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for this mailbox

The **Reset** button available in this area allows the client to clear statistics for the selected mailbox. Both dropped and total statistics for the mailbox will be reset.

Settings for Mailbox

In order to view the individual settings of the chosen mailbox the client must click the  **Settings** icon on the chosen mailbox row. In this area the client can modify the limits that apply to the chosen mailbox. This option is available only if mailbox settings are enabled on the server.



Tip

Settings for mailboxes override settings for the corresponding domains. Settings for domains override global settings for server.

Spam Engine Settings for Mailbox

In this area the client can modify the settings of the spam engine for the chosen mailbox.

Reset mailbox settings – To reset mailbox settings, the client must enable this option and click **Update**. The mailbox settings will be reset to the global server settings or to the domain settings (if these exist).

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all messages detected as spam received in the mailbox.

Spam message as attachment - When this option is enabled and a message received in the mailbox is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient to announce him that he received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



The **Drop spam messages** option cannot be enabled in the same time with the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag – When the previous option is enabled, the client can write in this field the subject that he wants to be used for spam messages tagging.

Enable spam forwarding – When this option is enabled, spam messages are forwarded to a different email address. Only the messages supposed to be clean reach the mailbox.

Forward spam to address – When the option **Enable spam forwarding** is enabled, this is the address where spam messages are forwarded. The forward address must be on the same domain.

Enable spam forwarding – When this option is enabled, spam messages are forwarded to a different email address. Only the messages supposed to be clean reach the mailbox.

Forward spam to address – When the option **Enable spam forwarding** is enabled, this is the address where spam messages are forwarded. The forward address must be on the same domain.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The client can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the client chooses the first option, he can write the value he wants in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Mailbox

Email messages originating from the addresses in the White list and received in the chosen mailbox will not be processed by the spam protection engine.

Email address – In this field the client can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the mailbox White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list and received in the chosen mailbox will be tagged as spam.

Email address – In this field the client can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses – These are the email addresses currently available in mailbox Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Mailbox

Email messages originating from the networks in this list and received in the chosen mailbox will not be processed by the spam protection engine. You can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 – single IP address
192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address – In this field the client can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the mailbox trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

2. Management Permissions

In the Permissions area (click the **Permissions** button available in the tool bar) the client can grant 4PSA Spam Guardian management permissions to domain users.

This means that domain users will be able to choose for themselves which mailboxes to protect from spam messages.

To grant management permissions to a domain user, check the "Allow access" checkbox corresponding to the chosen domain and click **Update**. You can later revoke management permissions by un-checking the same checkbox and clicking **Update**.

You can grant/revoke management permissions for multiple domain users at the same time.

Chapter 4. The Domain User Module

The 4PSA Spam Guardian domain user module can be accessed after you login to Plesk 7.x using a domain user account. In order to open the 4PSA Spam Guardian interface click the [4PSA Spam Guardian](#) link available in the Custom menu located on the left side of the Plesk interface.



Note

In order to access 4PSA Spam Guardian, the domain user must have permissions from the server administrator or from the client who owns his domain.

The 4PSA Spam Guardian tool bar is available on top of the application's interface. The tool bar provides an easy method for the domain user to setup domain and mailbox protection, to view domain and mailbox statistic graphs, to change and to reset mailbox settings.

1. Protecting the Entire Domain

Protecting the domain means that all mailboxes available under this domain will be protected against spam messages. All the mailboxes added later to the protected domain will be automatically protected by 4PSA Spam Guardian.

In this area the domain user can view three columns displaying the following information:


Protected mailboxes – The number of protected mailboxes on the domain

Total mailboxes – The total number of mailboxes on the domain

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the domain (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that domain. This column is available only if statistics are enabled on the server.

Next to these columns 3 action icons are available for each domain in the list.

Stats - By clicking the  **Statistics** icon, the domain user will be able to view the statistics available for his domain

S - By clicking the  **Settings** icon, the domain user will be able to define settings for his domain


Reset stats – By clicking the  **Reset statistics** icon, the domain user will reset the statistics available in the Dropped/Total column for his domain



These columns are available only if at least one mailbox that belongs to this domain is protected by 4PSA Spam Guardian and if statistics are enabled on the server.

To protect the entire domain, check the “Protect the entire domain” checkbox and click **Update**. You can later disable domain protection by unchecking the same checkbox and clicking **Update**.

Domain Statistics

To view the statistics for his domain, the domain user must click the  **Stats** icon corresponding to the domain. A graphic with the domain statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian and the number of messages dropped by the spam engine for this domain.




The domain statistics are available only if at least one mailbox that belongs to this domain is protected by 4PSA Spam Guardian and if statistics are enabled on the server.

Domain Statistics Graph

In this graph one curve represents the total number of emails received by the selected domain and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by the selected domain and dropped by the spam engine. The domain user can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the selected domain and processed by the spam engine.

Customize

In this area the domain user can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the domain user must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by his domain and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by his domain and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Domain Statistics

In this area 4PSA Spam Guardian displays information about his domain statistics.

Total - The total number of emails received by the domain and processed by the spam engine

Dropped - The number of email messages received by the domain and dropped by the spam engine

Average processed - The average number of email messages received by the domain and processed every day by the spam engine

Average dropped - The average number of email messages received every day by the domain and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for the domain

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for the domain

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for the domain

The **Reset** button available in this area allows the domain user to clear statistics for his domain. Both dropped and total statistics for the domain will be reset.

Settings for Domain

In order to view the individual settings for his domain the domain user must click the  **Settings** icon. In this area the domain user can modify the available settings.



Tip

Settings for mailboxes override settings for the corresponding domains. Settings for domains override global settings for server. If you want to enable higher or lower limits for a particular mailbox, change settings individually in the Settings for mailbox area.

Spam Engine Settings for Domain

In this area the domain user can modify the settings of the spam engine for his domain.

Reset domain settings – To reset the domain settings, the domain user must enable this option and click **Update**.

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all spam messages received in the mailboxes of his domain.

Spam message as attachment - When this option is enabled and a message received in one of the mailboxes is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient to announce him that he has received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



The **Drop spam messages** option cannot be enabled in the same time with the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag - When the previous option is enabled, the domain user can write in this field the subject that he wants to be used for spam message tagging.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The domain user can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the domain user chooses the first option, he can write the value he wants in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Domain

Email messages originating from the addresses in the White list will not be processed by the spam protection engine.



You can use wildcards for the White list entries: ***** to match any number of characters and **?** to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the domain user can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the domain's White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Domain

Email messages originating from the addresses in the Black list will be tagged as spam.



Note

You can use wildcards for the Black list entries: ***** to match any number of characters and **?** to match a single character. For security reasons, regular expressions are not allowed.

Email address – In this field the domain user can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses – These are the email addresses currently available in the domain's Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Domain

Email messages originating from the networks in this list will not be processed by the spam protection engine. You can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 – single IP address

192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address – In this field the domain user can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the domain's trusted networks list.


The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.


2. Protecting Individual Mailboxes

The domain user can protect individual mailboxes against spam messages. In the Mailbox protection area, the following columns are available next to the mailbox name:

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the mailbox (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that mailbox.

Stats - By clicking the  **Statistics** icon, the domain user will be able to view the statistics available for his mailbox

S - By clicking the  **Settings** icon, the domain user will be able to define settings for the selected mailbox

Reset stats – By clicking the  **Reset statistics** icon, the domain user will reset the statistics available in the Dropped/Total column for the corresponding mailbox.



The mailbox statistics are available only if the mailbox is protected by 4PSA Spam Guardian and if the statistics are enabled on the server.

Protect – When enabled, 4PSA Spam Guardian protects the corresponding mailbox against spam messages.




When a domain is protected, all its mailboxes are protected and the corresponding “Protect” checkboxes are grayed out.

To protect a mailbox, check the “Protect” checkbox for the chosen mailbox and click **Update**. You can later disable mailbox protection by unchecking the same checkbox and clicking **Update**.

The mailbox protection can be enabled/disabled for multiple mailboxes at the same time.

3. Mailbox Statistics

To view the statistics for a protected mailbox, the domain user must click the  **Stats** icon. A graphic with the mailbox statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian for this mailbox and the number of messages received by this mailbox and dropped by the spam engine.




The mailbox statistics are available only if the mailbox is protected by 4PSA Spam Guardian and if the statistics are enabled on the server.

Mailbox Statistics Graph

In this graph one curve represents the total number of emails received by the mailbox and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by this mailbox and dropped by the spam engine. The domain user can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the mailbox and processed by the spam engine.

Customize

In this area the domain user can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the domain user must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by this mailbox and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by this mailbox and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Mailbox Statistics

In this area 4PSA Spam Guardian displays information about the mailbox statistics.

Total - The total number of emails received by this mailbox and processed by the spam engine

Dropped - The number of email messages received by this mailbox and dropped by the spam engine

Average processed - The average number of email messages received by this mailbox and processed every day by the spam engine

Average dropped - The average number of email messages received every day by this mailbox and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for this mailbox

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for this mailbox

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for this mailbox

The **Reset** button available in this area allows the domain user to clear statistics for the selected mailbox. Both dropped and total statistics for the mailbox will be reset.

4. Settings for Mailbox

In order to view the individual settings of the chosen mailbox the domain user must click the  **Settings** icon on the chosen mailbox row. In this area the domain user can modify the limits that apply to the chosen mailbox.



These statistics are available only if the mailbox is protected by 4PSA Spam Guardian and if statistics are enabled on the server.

Spam Engine Settings for Mailbox

In this area the domain user can modify the settings of the spam engine for the selected mailbox.

Reset mailbox settings – To reset mailbox settings, the domain user must enable this option and click **Update**. The mailbox settings will be reset to the global server settings or to the domain settings (if these exist).

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all messages detected as spam received in the mailbox.

Spam message as attachment - When this option is enabled and a message received in the mailbox is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient to announce him that he received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



The **Drop spam messages** option cannot be enabled as the same time as the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag – When the previous option is enabled, the domain user can write in this field the subject that he wants to be used for spam messages tagging.

Enable spam forwarding – When this option is enabled, spam messages are forwarded to a different email address. Only the messages supposed to be clean reach the mailbox.

Forward spam to address – When the option **Enable spam forwarding** is enabled, this is the address where spam messages are forwarded. The forward address must be on the same domain.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The domain user can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the domain user chooses the first option, he can enter the desired value in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Mailbox

Email messages originating from the addresses in the White list and received in the chosen mailbox will not be processed by the spam protection engine.

Email address – In this field the domain user can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the email addresses currently available in the mailbox White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list and received in the chosen mailbox will be tagged as spam.

Email address – In this field the domain user can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses – These are the email addresses currently available in mailbox' Black list.

The Black Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Mailbox

Email messages originating from the networks in this list and received in the chosen mailbox will not be processed by the spam protection engine. On this list you can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 – single IP address
192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address – In this field the domain user can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the mailbox trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Chapter 5. The Email User Module

The 4PSA Spam Guardian email user module can be accessed after you login to Plesk 7.x using an email user account. In order to open the 4PSA Spam Guardian interface click the [4PSA Spam Guardian](#) link available in the Custom navigation menu located on the left side of the Plesk interface.



Note


In order to allow an email user to access the 4PSA Spam Guardian interface, the owner of the domain or the administrator must give management permissions to the corresponding domain user.


1. Protecting the Mailbox

The email user can protect his mailbox from spam messages. In the Mailbox protection area, the following columns are available next to the mailbox name:

Dropped / Total – There are two statistics displayed: the number of dropped email messages for the mailbox (emails that were not delivered to the destination because they were detected to be spam) / the total number of email messages processed by the spam engine on that mailbox

Stats - By clicking the  **Statistics** icon, the email user will be able to view the statistics available for his mailbox

S - By clicking the  **Settings** icon, the email user will be able to define the mailbox settings

Reset stats – By clicking the  **Reset statistics** icon, the email user will reset the statistics available in the Dropped/Total column for the mailbox



These columns are available only if the mailbox is protected by 4PSA Spam Guardian and if statistics are enabled on the server.


Protect – When enabled, 4PSA Spam Guardian protects the mailbox against spam messages.



When a domain is protected, all its mailboxes are protected and the corresponding “Protect” checkbox is grayed out.

To protect the mailbox, check the “Protect” checkbox and click **Update**. You can later disable mailbox protection by unchecking the same checkbox and clicking **Update**.

2. Mailbox Statistics

To view the statistics for his mailbox, the email user must click the  **Stats** icon. A graphic with the mailbox statistics is available in this area. These statistics are based on the total number of emails processed by 4PSA Spam Guardian for this mailbox and the number of messages received by this mailbox and dropped by the spam engine.



Note


The mailbox statistics are available only if the mailbox is protected by 4PSA Spam Guardian and if the statistics are enabled on the server.

Mailbox Statistics Graph

In this graph one curve represents the total number of emails received by the mailbox and processed by 4PSA Spam Guardian. The other curve represents the number of email messages received by the mailbox and dropped by the spam engine. The email user can change the look of this graph in the Customize area below. The oX axis displays the selected time period and the oY axis the total number of emails received by the mailbox and processed by the spam engine.

Customize

In this area the email user can change the time interval displayed in the graph and the graph's look.

Start and end date - The start and the end dates of the time interval for which the graph is plotted. In order to select a date the email user must click on the  **Calendar** icon.

Dropped color - The color for the curve that displays the number of email messages received by this mailbox and dropped by the spam engine

Totals color - The color for the curve that displays the total number of emails received by this mailbox and processed by the spam engine

Dots color - The color of the dotted lines across the graph

Label color - The color of the labels on the axis of the graph

Axis color - The color of the oX and oY axis

Arrow color - The color of the arrows at the end of the axis

Graph background color - The background color for the plotted region

Canvas background color - The background color for the entire canvas (beyond the plotted region)

Mailbox Statistics

In this area 4PSA Spam Guardian displays information about the mailbox statistics.

Total - The total number of emails received by this mailbox and processed by the spam engine

Dropped - The number of email messages received by this mailbox and dropped by the spam engine

Average processed - The average number of email messages received by this mailbox and processed every day by the spam engine

Average dropped - The average number of email messages received every day by this mailbox and dropped by the spam engine

Minimum processed - The date when the spam engine processed the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Minimum dropped - The date when the spam engine dropped the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.

Maximum processed - The date when the spam engine processed the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were processed that day.

Maximum dropped - The date when the spam engine dropped the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages were dropped that day.


Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam engine for this mailbox

Best day - The percentage of dropped emails and the date with the smallest percentage of dropped emails for this mailbox

Worst day - The percentage of dropped emails and the date with the biggest percentage of dropped emails for this mailbox

The **Reset** button available in this area allows the email user to clear statistics for his mailbox. Both dropped and total statistics for the mailbox will be reset.

3. Settings for Mailbox

In order to view the individual settings of the mailbox, the email user must click the  **Settings** icon. In this area the email user can modify the limits that apply to the mailbox.



Note

These settings are available only if the mailbox is protected by 4PSA Spam Guardian and if statistics are enabled on the server.

Spam Engine Settings for Mailbox

In this area the email user can modify the settings of the spam engine for the chosen mailbox.

Reset mailbox settings – To reset mailbox settings, the email user must enable this option and click **Update**. The mailbox settings will be reset to the global server settings or to the domain settings (if these exist).

Drop spam messages – When this option is enabled, 4PSA Spam Guardian will delete all messages detected as spam received in the mailbox.

Spam message as attachment - When this option is enabled and a message received in the mailbox is detected to be spam, 4PSA Spam Guardian sends an email to the message recipient to announce him that he received a spam message and attaches this message to the email.

Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the email message subject with the text available in the Spam message subject tag field.



Note

The **Drop spam messages** option cannot be enabled at the same time as the **Spam message as attachment** or **Modify spam message subject** options.

Spam message subject tag – When the previous option is enabled, the email user can write in this field the subject that he wants to be used for spam messages tagging.

Enable spam forwarding – When this option is enabled, spam messages are forwarded to a different email address. Only the messages supposed to be clean reach the mailbox.

Forward spam to address – When the option **Enable spam forwarding** is enabled, this is the address where spam messages are forwarded. The forward address must be on the same domain.

Spam engine sensitivity - Each message processed by the spam detection mechanism is assigned a score based on a generic algorithm indicating the probability of that message being a spam. The higher the score, more likely the message is spam. Messages that have scored a value above the set value will be tagged as spam. The email user can choose between the available options: custom value, very permissive, permissive, moderate, strict, and very strict. When the email user chooses the first option, he can enter the desired value in the Custom value field.

In order to save the changes you must click **Update**.

White List Settings for Mailbox

Email messages originating from the addresses in the White list and received in your mailbox will not be processed by the spam protection engine.

Email address - In this field the email user can write the email addresses. To add the address to the White list, click **Add**. To remove the address from the White list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses - These are the email addresses currently available in the mailbox White list.

The White List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list and received in your mailbox will be tagged as spam.

Email address - In this field the email user can write the email address. To add the address to the Black list, click **Add**. To remove the address from the Black list, click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always reject mail from these addresses - These are the email addresses currently available in mailbox' Black list.

The Black List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Trusted Networks for Mailbox

Email messages originating from the networks in this list and received in your mailbox will not be processed by the spam protection engine. On this list you can include on this list single IP addresses or an entire network or subnetwork.

Example: 192.168.1.1 - single IP address
192.168. - all the IP addresses in the 192.168.0.0/16 subnetwork

IP address - In this field the email user can write the IP address. To add the IP address to the list click **Add**. To remove the IP address from the list click **Remove**.

Import from file - Enter the name of the file which contains the email addresses that you want to be included in the list or click the **Browse...** button to locate the desired file.



Note

When both **Email address** and **Import from file** fields are filled in, 4PSA Spam Guardian will add to the server only the addresses from the file.

Always accept mail from these addresses – These are the IP addresses currently available in the mailbox trusted networks list.

The Trusted Networks List can be exported as a text file. In order to save it on your local computer, click the **Export** button. A file download dialog box opens. Select the name of the file and the path on your local machine where you want to save the file.

Appendix A. Server Compatibility

4PSA Spam Guardian for Plesk 7.x Reloaded is compatible with Plesk 7.x Reloaded installations only. You have to download the build based on the operating system installed on your machine.

The file `spam_guardian_buildRedHat7xXXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- RedHat Linux 7.3
- RedHat Enterprise Linux 2.1

The file `spam_guardian_buildRedHat9xXXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- RedHat Linux 9
- RedHat Enterprise Linux 3.0
- RedHat Enterprise Linux 4.0
- Fedora Linux Core 1
- Fedora Linux Core 2
- Fedora Linux Core 3

The file `spam_guardian_buildFreeBSD49XXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- FreeBSD 4.8
- FreeBSD 4.9

The file `spam_guardian_buildFreeBSD52XXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- FreeBSD 5.2.1
- FreeBSD 5.3

The file `spam_guardian_buildSuseXXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- Suse Linux 9
- Suse Linux 9.1

The file `spam_guardian_buildMandrakeXXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- Mandrake 10

The file `spam_guardian_buildDebianXXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- Debian 3.1