

CLOUD CALLING™



4PSA Spam Guardian 4.0.0 for Plesk 10.0.0 and newer versions User's Guide

For more information about 4PSA Spam Guardian, check:
<http://www.4psa.com>
Copyright © 2009 - 2011 4PSA.

User's Guide

Manual Version 84564.17 at 2011/10/18 10:26:53

For suggestions regarding this manual contact:

docs@4psa.com

Copyright © 2009 - 2011 4PSA.

All rights reserved.

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

Plesk is a Registered Trademark of Parallels, 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 property of their respective owners.

Table of Contents

Preface	5
Who Should Read This Guide	5
Chapter 1. The Administrator Module	6
Protecting Domains Globally	6
Statistics	28
Server Statistics Graph	28
Customize	28
Server Statistics	29
Reporting	30
Server-Wide Settings	31
4PSA Spam Guardian Reports	31
Spam Detection Engine Settings	32
White List Settings	35
Black List Settings	36
Trusted Networks	37
4PSA Spam Guardian Settings	38
Interface Settings	39
Email Templates	40
Custom Rules	40
License Management	40
Testing Spam Settings	42
Using the Spam Learning Features of 4PSA Spam Guardian	42
Chapter 2. The Reseller Module	44
Protecting Domains Globally	44
Protecting the Entire Domain	45
Domain Statistics	46
Settings for Domain	48
Global Settings for Domains	53
Protecting Individual Mailboxes	55
Global Settings for Mailboxes	56
Mailbox Statistics	58
Mailbox Settings	60
Settings	65
Global Settings	65
Interface Settings	66

Reporting	67
Chapter 3. The Customer or the Control Panel User Module	68
Protecting the Entire Domain	68
Domain Statistics	69
Domain Settings	72
Global Settings for Domains	77
Protecting Individual Mailboxes	78
Mailbox Statistics	79
Mailbox	80
Customize	80
Mailbox Statistics	81
Mailbox Settings	82
Spam Detection Engine Settings for Mailbox	82
White List Settings for Mailbox	84
Black List Settings for Mailbox	85
Trusted Networks for Mailbox	86
Global Settings for Mailboxes	87
Chapter 4. Contact and Support	89

Preface

Who Should Read This Guide

The administrator of the Plesk server must read this User's Guide. The hosting service user, be it Plesk reseller, customer/subscriber or Control Panel user, will also find useful certain sections of this User's Guide. The manual is structured in such a way that needed information can be easily found in its sections.

The Administrator Module

The 4PSA Spam Guardian administrator module can be accessed by logging in Plesk with the `admin` account. To access the 4PSA Spam Guardian interface, go to the left navigation menu and in the "Custom" area click the [4PSA Spam Guardian](#) link.



Note

When you install the product for the first time, no user has access to 4PSA Spam Guardian and no link is available in the navigation menu. To give access rights to your hosting customers, in the 4PSA Spam Guardian interface go to the Permissions area. Further information is available in this chapter.

The 4PSA Spam Guardian toolbar is available on top of the Plesk browser interface. The toolbar makes it easy for the server administrator to perform the following operations:

- Set up protection for entire domains and individual mailboxes.
- View statistics for mailboxes, domains, and the entire server.
- Change settings for domains and mailboxes.
- Edit server-wide settings for the spam detection engine.
- Grant management permissions to resellers, customers and control panel users.
- Change interface settings.
- Add custom spam detection rules.
- Manage the license key.

Protecting Domains Globally

In the Domains area, the server administrator can protect entire domains against spam messages.

To access this section, click the Domains button available in the toolbar.

The Domains area is represented by a table with eight columns. The Domain column displays the list of all domains hosted on the server.

The following three columns display the following statistics from left to right:

- Protected mailboxes - The number of protected mailboxes on the domain.
- Total mailboxes - The total number of mailboxes on the domain.

- Dropped/Total - The number of dropped email messages that have not been delivered because they were identified as spam, out of the total number of email messages processed by the spam detection engine.



Note

The **Dropped/Total** column is visible if there is at least one protected mailbox on that domain and if the **Save statistics** option is enabled in the Settings area.

The next three columns of the table display the following action icons:

- Stats - By clicking the Statistics icon, the server administrator will be able to view the recorded statistics 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 recorded for the corresponding domain.



Note

The **Reset stats** column is available if there is at least one protected mailbox on that domain and if the **Save statistics** option is enabled in the Settings area.

The Protected column, which can be found on the left of the domain name, comes with two clickable options describing whether the domain in question is protected or not. Here are the two options:

1. Click the Enable link to enable domain protection. The Yes status under the Protected column confirms that domain protection is enabled.
2. Click the Disable link to disable domain protection. The No status under the Protected column confirms that domain protection is disabled.

Protecting the Entire Domain

Protecting a domain means that all its mailboxes will be protected against spam-infected messages. 4PSA Spam Guardian will automatically protect every new mailbox added to a protected domain.


To protect an entire domain, go to the Protected column and click the Enable option corresponding to the domain in question. To cancel domain protection, click the Disable option next to the domain name.

Domain protection for several domains can be enabled or disabled at the same time. To do this, follow these steps:

1. Select the checkboxes on the right corresponding to the respective domains.
2. Click the Toggle protection button.

The domains that were not protected will be protected and the domains that were protected will be unprotected.

Domain Statistics

To view the statistics for an entire domain, click the  Stats icon corresponding to the selected domain. A graphic with the domain statistics is available in this area. Statistics take into consideration the total number of processed emails, the number of messages dropped, and the number of messages tagged by the spam detection engine.



Note

The domain statistics are available if there is at least one protected mailbox on that domain and if the **Save statistics** option is enabled. To enable this option, click the Settings tab on top of the interface and then select the box corresponding to **Save statistics**.


Domain Statistics Graph

In this graph, one curve represents the total number of emails received and processed by 4PSA Spam Guardian for the selected domain. The other two curves represent the number of email messages received and dropped by the spam detection engine and the number of email messages received and tagged. The server administrator can modify the looks of the graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval while the vertical oY axis the total number of emails received by the selected domain and processed by the spam detection engine.

Customize

In this section, the server administrator can change the time interval displayed in the graph and the graph's look. These are the available options:

- Start and End date - The start and the end dates of the time interval for the graph. To select a date, the server administrator must click the  Calendar icon.
- Tagged color - The color of the curve that displays the number of email messages received by the protected mailboxes of the selected domain and tagged as spam by the engine.
- Dropped color - The color of the curve that displays the number of spam email messages received by the protected mailboxes of the selected domain and dropped by the engine.
- Totals color - The color for the curve that displays the total number of emails received by the protected mailboxes of the selected domain.
- Dots color - The color of the dotted lines across the graph.
- Label color - The color of the graph axis' labels.
- Axis color - The color of the oX and oY axes.
- Arrow color - The color of the arrows at the end of the axes.
- Graph background color - The background color for the plotted region.
- Canvas background color - The background color for the entire canvas (surrounding the plotted region).

Domain Statistics

In this section, 4PSA Spam Guardian displays the following information:


- Total - The total number of emails received by the protected mailboxes of the selected domain.
- Tagged - The number of spam email messages tagged by the spam detection engine.
- Dropped - The number of spam email messages dropped by the spam detection engine.
- Average processed - The average number of email messages received by the protected mailboxes of the domain and processed every day.
- Average tagged - The average number of spam email messages tagged per day by the spam detection engine.
- Average dropped - The average number of spam email messages dropped per day by the spam detection engine.
- Minimum processed - The number of emails and the date when the minimum number of messages has been received by the protected mailboxes of the domain.

- Minimum tagged - The number of spam emails and the date when the minimum number of spam messages has been tagged by the spam detection engine.
- Minimum dropped - The number of spam emails and the date when the minimum number of spam messages has been dropped by the spam detection engine.
- Maximum processed - The number of emails and the date when the maximum number of messages has been received by the protected mailboxes of the selected domain.
- Maximum tagged - The number of spam emails and the date when the maximum number of spam messages has been tagged by the spam detection engine.
- Maximum dropped - The number of spam emails and the date when the maximum number of spam messages has been dropped by the spam detection engine.
- Percent dropped - The percentage of emails from the total number of emails received by the protected mailboxes of the domain, dropped by the spam detection engine.
- Percent tagged - The percentage of emails from the total number of emails received by the protected mailboxes of the domain, tagged by the spam detection engine.
- Best day - The percentage of spam emails and the date with the smallest percentage of spam emails received by the protected mailboxes of the domain.
- Worst day - The percentage of spam emails and the date with the biggest percentage of spam emails received by the protected mailboxes of the domain.

To clear statistics for the selected domain, click the Reset button. The global statistics available in the Settings area will be updated by this reset.

Domain Settings

To view the individual settings of a domain, follow these steps:

1. In the Domains table, click the  Settings icon corresponding to the chosen domain.
2. A new page opens allowing you to modify the settings of the spam detection engine for the chosen domain.



Note

The settings for the individual mailboxes override the settings of the domains they belong to. The settings for the domains override the global settings for the server. If you want to enable specific limits for a particular mailbox, use the corresponding controls.

Spam Detection Engine Settings for Domain

In this section, the server administrator can modify the following settings of the spam detection engine:

- Reset domain settings - To reset the settings of the spam detection engine for the domain, select the corresponding box and click Update. Consequently, the domain settings will be reset to the global server settings.
- Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option.)
- Spam message subject tag - When the previous option is enabled, this field contains the subject that will be used to tag spam messages.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate

- Strict
- Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Send daily statistics report - When you select this check box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

To save the changes, click Update.

White List Settings for Domain

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.



Note

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

- Import from file - Enter the name of the file that contains the email addresses you want in the list or click the Browse button to locate the chosen 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 - This select list contains all email addresses available in the domain's White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialog opens.
2. Name the file and choose the location where you want to save the file.

Black List Settings for Domain

Email messages originating from the addresses included in the Black list will be considered spam by the engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.



Note

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

- Import from file - Enter the name of the file that contains the email addresses you want in the list or click the Browse button to locate the chosen 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 - This select list contains all the email addresses available in the domain's Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks for Domain

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - all the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the IP address text box, fill in the address you trust.
2. Click the Add button



Note

You can select several IP addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the Always reject mail from these networks select list, choose one or more addresses.
2. Click the Removebutton.

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Global Settings for Domains

You can make the same changes to several domains:

1. In the list of domains, select the respective domains.
2. Click Global changes
3. Make the desired changes. The following options are available:
 - Reset domain settings - To reset the settings of the spam detection engine for the domain, select the corresponding check box and click Update. Consequently, the domain settings will be reset to the global server settings.
 - Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option)
 - Spam message subject tag - When the previous option is enabled, this field contains the subject that will be used to tag spam messages.
 - Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
 - Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
 - IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
 - Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
 - Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
 - Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that

message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:

- Custom value - When this option is enabled, you must fill in the Custom value text box.
- Very permissive
- Permissive
- Moderate
- Strict
- Very strict
- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

4. Click Update to save the changes.





Note

If you do not wish to modify a setting, select the **do not change** option.

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, click the domain name link.

In the Mailbox protection section, the following columns are available for each mailbox:

- Dropped/Total - The number of dropped email messages that were not delivered because they were identified as spam, out of the total number of email messages processed by the spam detection engine.
- Stats - By clicking the  Statistics icon, the server administrator will be able to view the recorded statistics 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 recorded for the corresponding mailbox.



Note

The **Statistics** and the **Reset stats** columns are visible only if the corresponding mailbox is protected by 4PSA Spam Guardian, and if the **Save statistics** option is enabled. To enable this option, click the Settings tab on top of the interface and select the check box corresponding to the **Save statistics** option. When no messages are processed "-" will be displayed in the **Dropped/Total** column, on the corresponding mailbox row.

- The Protected column, which can be found on the left of the mailbox name, comes with two clickable options describing whether the mailbox in question is protected or not. Here are the two options:
 1. Click the Enable link to enable mailbox protection. The Yes status under the Protected column confirms that mailbox protection is enabled.
 2. Click the Disable link to disable mailbox protection. The No status under the Protected column confirms that mailbox protection is disabled.



Note

When a domain is protected, all its mailboxes are protected.

To protect a mailbox, go to the Protected column and click the Enable option corresponding to the mailbox in question. To cancel mailbox protection, click the Disable option next to the mailbox name.

Protection can be enabled or disabled for several mailboxes at the same time. To do this, please follow the steps below:

1. Select the check boxes on the right corresponding to the respective mailboxes.
2. Click the Toggle protection button.

The mailboxes that were not protected will be protected and the mailboxes that were protected will be unprotected.

Mailbox Statistics

To view the statistics for a protected mailbox, click the  Stats icon corresponding to the chosen mailbox. A graphic with mailbox statistics is available

in this area. The statistics take into consideration the total number of processed emails, the number of messages dropped, and the number of messages tagged by the spam detection 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. To enable this option, click the Settings tab on top of the interface and select the box corresponding to **Save statistics**.


Mailbox Statistics Graph

In this graph, one curve represents the total number of emails received and processed by 4PSA Spam Guardian for the selected mailbox. The other two curves represent the number of email messages received and dropped by the spam detection engine and the number of email messages received and tagged. The server administrator can modify the looks of the graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval and the vertical oY axis the total number of emails received by the mailbox and processed by the spam detection engine.

Customize

In this section, 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 the graph. To select a date, the server administrator must click the  Calendar icon.
- Tagged colour - The colour of the curve that displays the number of email messages received by the protected mailbox and tagged as spam by the engine.
- Dropped colour - The colour of the curve that displays the number of spam email messages received by the protected mailbox and dropped by the engine.
- Totals colour - The colour for the curve that displays the total number of emails received by the protected mailbox.
- Dots colour - The colour of the dotted lines across the graph.
- Label colour - The colour of the graph axis' labels.
- Axis colour - The colour of the oX and oY axes.
- Arrow colour - The colour of the arrows at the end of the axes.

- Graph background colour - The background colour for the plotted region.
- Canvas background colour - The background colour for the entire canvas (surrounding the plotted region).

Mailbox Statistics


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

- Total - The total number of emails received by the protected mailbox.
- Tagged - The number of spam email messages tagged by the spam detection engine.
- Dropped - The number of spam email messages dropped by the spam detection engine.
- Average processed - The average number of email messages received by the protect mailbox and processed every day.
- Average tagged - The average number of spam email messages tagged per day by the spam detection engine.
- Average dropped - The average number of spam email messages dropped per day by the spam detection engine.
- Minimum processed - The number of emails and the date when the minimum number of messages has been received by the protected mailbox.
- Minimum tagged - The number of spam emails and the date when the minimum number of spam messages has been tagged by the spam detection engine.
- Minimum dropped - The number of spam emails and the date when the minimum number of spam messages has been dropped by the spam detection engine.
- Maximum processed - The number of emails and the date when the maximum number of messages has been received by the protected mailbox.
- Maximum tagged - The number of spam emails and the date when the maximum number of spam messages has been tagged by the spam detection engine.
- Maximum dropped - The number of spam emails and the date when the maximum number of spam messages has been dropped by the spam detection engine.
- Percent dropped - The percentage of emails from the total number of emails received by the protected mailbox, dropped by the spam detection engine.
- Percent tagged - The percentage of emails from the total number of emails received by the protected mailbox, tagged by the spam detection engine.

- Best day - The percentage of spam emails and the date with the smallest percentage of spam emails received by the protected mailbox.
- Worst day - The percentage of spam emails and the date with the biggest percentage of spam emails received by the protected mailbox.

To clear statistics for the selected mailbox, click the Reset button. The global statistics available in the Settings area will be updated by this reset.

Mailbox Settings

To view the individual settings for the chosen mailbox, the server administrator must click the  Settings icon on the chosen mailbox row. In this area, the server administrator can modify the limits that apply to the selected mailbox.



Note

The settings for the individual mailboxes override the settings of the domains they belong to. The settings for the domains override the global settings for the server. If you want to enable specific limits for a particular mailbox, use the corresponding controls.

Spam Detection Engine Settings for Mailbox

In this section, the server administrator can modify the following settings of the spam detection 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).
- Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option)
- 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 message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.

- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- 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, spam is diverted to the forward address.
- Forward spam to address - The administrator chooses from this field the address where spam messages are to be forwarded, after the option Enable spam forwarding has been enabled. The forward address must be on the same domain.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict

To save the changes, click Update.

- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field will be dropped by the engine. Use the drop-down list to select one of the available options:

- Custom value - When this option is enabled, you must fill in the Custom value text box.
- Very permissive
- Permissive
- Moderate
- Strict
- Very strict
- Send daily statistics report - When you select this check box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

White List Settings for Mailbox

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.
- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the mailbox White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the last address that you want to add

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list will be considered spam by the engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.
- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks for Mailbox

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - All the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the IP address text box, fill in the address you trust.
2. Click the Add button.



Note

You can select several IP addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.



Note

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

Global Settings for Mailboxes

You can make the same changes to several mailboxes:

1. In the list of mailboxes, select the respective mailboxes.
2. Click Global changes
3. Make the desired changes. The following options are available:
 - Reset mailbox settings - To reset mailbox settings, the reseller 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).
 - Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
 - Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
 - IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
 - Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
 - 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. (see next option)

- Spam message subject tag - When the previous option is enabled, the reseller can write in this field the subject that he wants to be used for spam messages tagging.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate

- Strict
- Very strict
- Send daily statistics report - When you select this check box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

4. Click Update to save the changes



Note

If you do not wish to modify a setting, select the **do not change** option.

Statistics

In this area, the server administrator can view a graph and information about the server-wide statistics. These statistics are based on the total number of processed emails and the number of messages dropped by the spam detection engine.

To access this section, click the Statistics tab available in the toolbar on the top of the interface.


Server Statistics Graph

In this graph, one curve represents the total number of emails received and processed by 4PSA Spam Guardian on the server. The other two curves represent the number of email messages received and dropped by the spam detection engine and the number of email messages received and tagged. The server administrator can modify the looks of the graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval and the vertical oY axis the total number of emails received by the server and processed by the spam detection engine.

Customize

In this section, 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 the graph. To select a date, the server administrator must click the  Calendar icon.
- Tagged colour - The colour of the curve that displays the number of email messages received by the server and tagged as spam by the engine.
- Dropped colour - The colour of the curve that displays the number of spam email messages received by the server and dropped by the engine.
- Totals colour - The colour for the curve that displays the total number of emails received by the server.
- Dots colour - The colour of the dotted lines across the graph.
- Label colour - The colour of the graph axis' labels.
- Axis colour - The colour of the oX and oY axes.
- Arrow colour - The colour of the arrows at the end of the axes.
- Graph background colour - The background colour for the plotted region.
- Canvas background colour - The background colour for the entire canvas (surrounding the plotted region).

Server Statistics

In this section, 4PSA Spam Guardian displays the following information about the server statistics:

- Total - The total number of emails received by the server.
- Tagged - The number of spam email messages tagged by the spam detection engine.
- Dropped - The number of spam email messages dropped by the spam detection engine.
- Average processed - The average number of email messages received by the server and processed every day.
- Average tagged - The average number of spam email messages tagged per day by the spam detection engine.
- Average dropped - The average number of spam email messages dropped per day by the spam detection engine.
- Minimum processed - The number of emails and the date when the minimum number of messages has been received by the server.
- Minimum tagged - The number of spam emails and the date when the minimum number of spam messages has been tagged by the spam detection engine.

- Minimum dropped - The number of spam emails and the date when the minimum number of spam messages has been dropped by the spam detection engine.
- Maximum processed - The number of emails and the date when the maximum number of messages has been received by the server.
- Maximum tagged - The number of spam emails and the date when the maximum number of spam messages has been tagged by the spam detection engine.
- Maximum dropped - The number of spam emails and the date when the maximum number of spam messages has been dropped by the spam detection engine.
- Percent dropped - The percentage of emails from the total number of emails received by the server, dropped by the spam detection engine.
- Percent tagged - The percentage of emails from the total number of emails received by the server, tagged by the spam detection engine.
- Best day - The percentage of spam emails and the date with the smallest percentage of spam emails received by the server.
- Worst day - The percentage of spam emails and the date with the biggest percentage of spam emails received by the server.

The Reset button available in the bottom right corner allows the server administrator to reset statistics for the entire server.

Reporting

In this area, the server administrator can obtain and export statistics reports about the domains and mailboxes protected by 4PSA Spam Guardian on each user level.

The page displays reports for resellers or customers.

Click on Export to Excel link to save the selected report in a CSV (comma separated value) file.

The resellers report is displayed under the form of a table containing the following data:

- Reseller - The name of the reseller; click the reseller name and the report of the reseller's customer will be displayed.
- Total Domains - This column displays the total number of domains owned by the reseller and all their customers.

- Protected Domains - This column displays the total number of protected domains owned by the reseller and all their customers.
- Total Mailboxes - This column displays the total number of mailboxes created for all the domains owned by the reseller and all their customers.
- Protected Mailboxes - This column displays the total number of protected mailboxes created for all the domains owned by the reseller and all their customers.

The customers report is displayed under the form of a table containing the following data:

- Customer - The name of the customer.
- Total Domains - This column displays the total number of domains owned by the customer.
- Protected Domains - This column displays the total number of protected domains owned by the customer.
- Total Mailboxes - This column displays the total number of mailboxes created for all the domains owned by the customer.
- Protected Mailboxes - This column displays the total number of protected mailboxes created for all the domains owned by the customer.

Server-Wide Settings

In this area, the server administrator can perform the following operations:

- View details about 4PSA Spam Guardian.
- Modify the settings of the spam detection engine.
- Add and remove items from the White List, Black list, and Trusted networks list.
- Change interface settings.

To access this area, click the Settings tab available in the toolbar on the top of the interface.

4PSA Spam Guardian Reports

This section 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 tagged emails - The total number of email messages identified as spam and tagged 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 the 4PSA Spam Guardian Bayesian filter to learn about spam.
- Number of HAM messages used for training - The total number of HAM messages used by the Spam Guardian Bayesian filter to learn about clean messages.

Spam Detection Engine Settings

In this section, the server administrator can modify the following settings of the spam detection engine:

- Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option)
- Spam message subject tag - When the previous option is enabled, this field contains the subject that will be used to tag spam messages.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.

- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field will be dropped by the engine. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Save Statistics - when this option is enabled, 4PSA Spam Guardian saves usage statistics for processed, tagged, and dropped messages.
- Do not scan emails larger than - This box allows you to set the maximum size of the email that will be checked by the spam detection engine. The engine will not scan emails with a bigger size than the one you set. By default, you can enter a value between 1 and 1,000 Kb.
- Use Razor2 - When you check this box, the engine will use Razor tests, if the required module is available.
- Razor2 timeout - This box allows you to set the number of seconds the engine can wait for a reply from a Razor server.

- Use DCC - When you check this box, the engine will use the DCC spam filtering mechanism, if the required module is available.
- DCC timeout - This box allows you to set the number of seconds the engine can wait for a reply from a DCC server.
- Use Pyzor - When you check this box, the engine will use the Pyzor spam filtering mechanism, if the required module is available.
- Pyzor timeout - This box allows you to set the number of seconds the engine can wait for a reply from a Pyzor server.
- Autowhitelisting - When you check this box, the engine will automatically add received messages to whitelists. Automatic whitelists track the long-term average score for each sender and take into consideration for new messages. An auto-white list is not intended as a general-purpose replacement for static whitelist entries.
- Use DNS tests - When you check this box, the engine will perform DNS tests on the received message, if the required module is available.
- Use Bayes test - When you check this box, the engine will use the naive-Bayesian-style classifier built into it. This allows you to disable the rules while leaving auto and manual learning enabled.
- Bayes autolearn - When you check this box, the engine will automatically add extreme scoring mails to its database. Currently the only supported system is a naive-Bayesian-style classifier.
- Autolearning consider non-spam messages scoring lower than - In this box you can write the threshold below which a mail has to score in order to be classified as non-spam by the engine.
- Autolearning consider spam messages scoring higher than - In this box you can write the threshold above which a mail has to score in order to be classified as spam by the engine.
- Start using Bayes after learning from spam messages - Use this box to write the number of emails the Bayes system has to learn from before using the engine on incoming emails.
- Start using Bayes after learning from ham messages - Use this box to write the number of ham emails the Bayes system has to learn from before using the engine on incoming emails.
- Accept messages encoded in - Use this drop-down list to select the accepted message encodings. When an email is received in a different encoding, the system will increment the message score to a higher value.
- Accept messages written in - Use this drop-down list to select the languages that do not increase the spam score. When the engine receives an email written in a different language, it will increment the message score to a higher value.

To save your changes, click Update.

White List Settings

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.



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.

- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.

2. Click the Remove button.

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Black List Settings

Email messages originating from the addresses in the Black list will be considered spam by the spam detection engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.



Note

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

- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive

email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the last address that you want to add.

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - All the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the IP address fill in the address you trust.

2. Click the Add button.



Note

You can select several IP addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the Always reject mail from these networks select list, choose one or more addresses.
2. Click the Remove button

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

4PSA Spam Guardian Settings

In this section, you can edit the following options to reduce the administration effort:

- Allow domain spam detection engine settings - When this option is enabled, resellers and customers are able to change the domain spam detection engine settings.
- Allow mailbox spam detection engine settings - When this option is enabled resellers and customers are able to change the mailbox spam detection engine settings.
- Automatically protect new domains - The administrator can choose between flowing options:
 - Never - The administrator decides that the newly added domains will not be automatically protected against spam-infected messages.
 - If their service plan includes 4PSA Spam Guardian - The administrator decides that the newly added domains will not be automatically protected against spam-infected messages unless they were created with Service Plans featuring an activated 4PSA Spam Guardian Additional Service.

- No matter their subscription plan - The administrator decides that the newly added domains will be automatically protected against spam-infected messages, even if they were created with Service Plans featuring an activated 4PSA Spam Guardian Additional Service.
- Allow resellers to manage the "Automatically protect new domain" permission for their customers - The administrator allows resellers to manage protection for their newly added domains. The administrator grants resellers access to the following options:
 - Never enable protection
 - If their service plan includes 4PSA Spam Guardian
 - No matter their subscription plan
- 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 inherit their settings from domains, while domains inherit the server settings.

Interface Settings


In this area, the server administrator can edit the following interface settings:

- Installed languages - Here all installed language packs are displayed. The interface will use the language pack setup in your account preference in Plesk. If this language pack is not available, the system will default to English. You can use only languages that have been installed in the Plesk interface.
- Display message to reseller - When enabled, this option will have the text in the Message for resellers field displayed under the form of an Info box in all the 4PSA Spam Guardian pages, at Reseller level.
- Message for resellers - The text in this field will be displayed in all the 4PSA Spam Guardian pages, at Reseller level. Such messages can accept HTML tags and have both an advertising and informative purpose.
- Display message to customers - When enabled, this option will have the text in the Message for customers field displayed under the form of an Info box, in all the 4PSA Spam Guardian pages, at both Customer and User level.
- Message for customers - The text in this field will be displayed in all the 4PSA Spam Guardian pages, at both Customer and User level.

Such messages can accept HTML tags and have both an advertising and informative purpose.

- Allow resellers to display their own message to their customers
- When enabled, this option will allow resellers to manage messages for customers in their own Settings area.

Email Templates

Click the  Email Template icon in order to edit the email template used to send statistics to customers and resellers. In order to send emails with statistics about the spam activity, simply enable the option Send daily statistics report per domain or mailbox basis.

Custom Rules

In this area, you can manage the 4PSA Spam Guardian custom anti-spam rules. It is recommended to add custom static anti-spam rules when you receive an email that follows a specific pattern. For example, you might wish to filter all emails that contain the word Viagra in the email subject. In order to do this, you must add a custom anti-spam rule and assign it a high score.

You can add multiple rules at a time. The following fields are available for input:

- Rule name - Set a descriptive name for the rule. This name must be unique.
- Rule score - The score you want to add to the overall email spam score when this rule is matched.
- If (any header, subject, body) (contains, starts with) - You can enter the keyword that triggers the rule. You can choose the position of the keyword in the email.

In order to delete existing rules, you must select them and click the Update button.

License Management

In this area, you can manage the 4PSA Spam Guardian license. The product requires a license key in order to work. The license key will be generated by 4PSA based on the server IP and Plesk version installed on the server.

You can use the following fields and controls to update or monitor your license:

- License key status
 - Your server IP - This is the main IP address of your server. The license key must be specifically issued for this IP otherwise it will not work.
 - License key status - The status of the currently loaded license key.
- Upload license key
 - License file - You can use this form to upload the license key to the server.



Note

If you can access other pages in 4PSA Spam Guardian, this means that your license is valid and you do not have to upload a new one.

- Get license key from licensing server - This form can be used to query the licensing server, using the activation code for your license key. This function can only be used when there is a license key loaded on the server. The first time you install the product you will be required to upload the license key.
- License by activation code - This form can be used to query the licensing server, using the activation code of your license key.
- License key properties - This section contains details about the current license.
 - Key number - The number of the license key.
 - Key ownership - The type of the license key ownership.
 - Maximum number of domains - The maximum number of allowed domains.
 - License key must autorenew before - The date when the license key expires and must be renewed.
 - Key renewed on - Last key renewal date.



Note

The Owned and Leased licenses automatically renew before the **License expire date**.

Testing Spam Settings

To test the settings of the spam detection engine you can send a message containing the following string of characters in the message body (use upper case and no white spaces or line breaks):

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

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.

Using the Spam Learning Features of 4PSA Spam Guardian

In Spam Assassin automatic learning is enabled by default. The automatic learning features are more advanced in Spam Assassin 3.x, therefore we recommend you use Spam Assassin 3.x under Linux. Under FreeBSD, it is not currently possible to use Spam Assassin 3.x because the Plesk installation is monolithic and 4PSA Spam Guardian depends on the installed Spam Assassin version.

Spam Training

You can use 4PSA Spam Guardian for manual learning. You can train the spam detection engine to consider certain emails as ham even if it previously identified them as spam. The engine can also be trained to consider certain ham messages as spam. In order to do this, you have to create folders where to move the mistakenly identified emails. The spam detection engine will learn from them to categorize emails more precisely.

Starting with 4PSA Spam Guardian 2.1.0, 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 is recommended to use this method for learning because it is very fast and efficient (all you have to do is to move the messages from the Inbox to the `junk_learn` and `ham_learn`, based on the message type (spam or ham)).



Note

Keep in mind that the engine must learn from a minimum number of messages in order to be operational. The minimum number of spam and ham messages the

engine must learn from can be set up in Settings, the options **Start using Bayes after learning from X spam messages** and **Start using Bayes after learning from X ham messages**.

The Reseller Module

The 4PSA Spam Guardian Reseller module can be accessed after logging in to Plesk from a Reseller level account. To open the 4PSA Spam Guardian interface, simply click the [4PSA Spam Guardian](#) link under the Links to Additional Services navigation menu on the left side of the Plesk interface.



Note

The reseller cannot access the 4PSA Spam Guardian unless the Additional Service is made available by the server administrator.



Note

In order to provide customers or Control Panel users with access to the 4PSA Spam Guardian, the reseller should enable the Additional Service application in their hosting Service Plans. Customers with a subscription created using a Service Plan with an active Additional Service will be allowed to access 4PSA Spam Guardian.

The 4PSA Spam Guardian toolbar is available on top of the Plesk browser interface. The toolbar makes it easy for the reseller to perform the following operations:

- Set up protection for entire domains and individual mailboxes.
- View statistics for mailboxes and domains.
- Change settings for domains and mailboxes.
- View usage statistics for its customers.
- Configure the auto-protection options for owned domains and their customers domains.

Protecting Domains Globally

In the Domains area, the reseller can protect entire domains against spam messages.




To access this area, click the Domains tab available in the toolbar.

The Domains area is represented by a table with eight columns. The Domains column displays the list of their domains hosted on the server. The following columns are displayed:

- Protected mailboxes - The number of protected mailboxes on the domain.
- Total mailboxes - The total number of mailboxes on the domain.

- Dropped/Total - The number of dropped email messages that were not delivered because they were identified as spam, out of the total number of email messages processed by the spam detection engine.

Each domain has three columns displaying the following action icons:

- Stats - By clicking the  Statistics icon, the reseller will be able to view the recorded statistics for the selected domain.
- S - By clicking the  Settings icon, the reseller will be able to define settings for the selected domain.
- Reset stats - By clicking the  Reset statistics icon, the reseller will reset the recorded statistics.



Note

These columns are visible if there is at least one protected mailbox on that domain and if statistics are enabled on the server.

The Protected column, which can be found on the left of the domain name, comes with two clickable options describing whether the domain in question is protected or not. Here are the two options:

1. Click the Enable link to enable domain protection. The Yes status under the Protected column confirms that domain protection is enabled.
2. Click the Disable link to disable domain protection. The No status under the Protected column confirms that domain protection is disabled.

Protecting the Entire Domain

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

To protect an entire domain, go to the Protected column and click the Enable option corresponding to the domain in question. To cancel domain protection, click the Disable option next to the domain name.


Domain protection for several domains can be enabled or disabled at the same time. To do this, follow these steps:

1. Select the check boxes on the right corresponding to the respective domains.

2. Click the Toggle protection button.

The domains that were not protected will be protected and the domains that were protected will be unprotected.

Domain Statistics

To view the statistics for an entire domain, click the  Stats icon corresponding to the selected domain. A graphic with the domain statistics is available in this area. The statistics take into consideration the total number of processed emails, the number of messages dropped, and the number of messages tagged by the spam detection engine.



Note

The domain statistics are available if there is at least one protected mailbox on that domain and if statistics are enabled on the server.


Domain Statistics Graph

In this graph, one curve represents the total number of emails received and processed by 4PSA Spam Guardian for the selected domain. The other two curves represent the number of email messages received and dropped by the spam detection engine and the number of email messages received and tagged. The reseller can modify the looks of the graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval while the vertical oY axis the total number of emails received by the selected domain and processed by the spam detection engine.

Customize

In this section, the reseller can change the time interval displayed in the graph and the graph's look. These are the available options:

- Start and End date - The start and the end dates of the time interval for the graph. To select a date, the reseller must click the  Calendar icon.
- Tagged colour - The colour of the curve that displays the number of email messages received by the protected mailboxes of the selected domain and tagged as spam by the engine.
- Dropped colour - The colour of the curve that displays the number of spam email messages received by the protected mailboxes of the selected domain and dropped by the engine.

- Totals colour - The colour for the curve that displays the total number of emails received by the protected mailboxes of the selected domain.
- Dots colour - The colour of the dotted lines across the graph.
- Label colour - The colour of the graph axis' labels.
- Axis colour - The colour of the oX and oY axes.
- Arrow colour - The colour of the arrows at the end of the axes.
- Graph background colour - The background colour for the plotted region.
- Canvas background colour - The background colour for the entire canvas (surrounding the plotted region).

Domain Statistics

In this section, 4PSA Spam Guardian displays the following information:


- Total - The total number of emails received by the protected mailboxes of the selected domain.
- Tagged - The number of spam email messages tagged by the spam detection engine.
- Dropped - The number of spam email messages dropped by the spam detection engine.
- Average processed - The average number of email messages received by the protected mailboxes of the domain and processed every day.
- Average tagged - The average number of spam email messages tagged per day by the spam detection engine.
- Average dropped - The average number of spam email messages dropped per day by the spam detection engine.
- Minimum processed - The number of emails and the date when the minimum number of messages has been received by the protected mailboxes of the domain.
- Minimum tagged - The number of spam emails and the date when the minimum number of spam messages has been tagged by the spam detection engine.
- Minimum dropped - The number of spam emails and the date when the minimum number of spam messages has been dropped by the spam detection engine.
- Maximum processed - The number of emails and the date when the maximum number of messages has been received by the protected mailboxes of the selected domain.

- Maximum tagged - The number of spam emails and the date when the maximum number of spam messages has been tagged by the spam detection engine.
- Maximum dropped - The number of spam emails and the date when the maximum number of spam messages has been dropped by the spam detection engine.
- Percent dropped - The percentage of emails from the total number of emails received by the protected mailboxes of the domain, dropped by the spam detection engine.
- Percent tagged - The percentage of emails from the total number of emails received by the protected mailboxes of the domain, tagged by the spam detection engine.
- Best day - The percentage of spam emails and the date with the smallest percentage of spam emails received by the protected mailboxes of the domain.
- Worst day - The percentage of spam emails and the date with the biggest percentage of spam emails received by the protected mailboxes of the domain.

To clear statistics for the selected domain, click the Reset button. The global statistics available in the Settings area will be updated by this reset.

Settings for Domain

To view the individual settings of a domain, follow these steps:

1. In the Domains table, click the  Settings icon corresponding to the chosen domain.
2. A new page opens allowing you to modify the settings of the spam detection engine for the chosen domain.



Note

Settings for individual mailboxes override the settings of the domains they belong to. Settings for domains override the global settings for the server. If you want to enable specific limits for a particular mailbox, edit the corresponding options.

Spam Detection Engine Settings for Domain

In this section, the reseller can modify the following settings of the spam detection engine:

- Reset domain settings - To reset the settings of the spam detection engine for the domain, enable this option and click Update. The domain settings will be reset to the global server settings.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option)
- Spam message subject tag - When the previous option is enabled, this field contains the subject that will be used to tag spam messages.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict

- Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

To save the changes click Update.

White List Settings for Domain

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.



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.

- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Black List Settings for Domain

Email messages originating from the addresses in the Black list will be considered spam by the engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.



Note

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

- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks for Domain

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - All the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the IP address text box, fill in the address you trust.
2. Click the Add button.



Note

You can select several IP addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the last address that you want to add.

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue appears.
2. Name the file and choose the location where you want to save the file.

Global Settings for Domains

You can make the same changes to several domains:

1. In the list of domains, select the respective domains.
2. Click Global changes
3. Make the desired changes. The following options are available:
 - Reset domain settings - To reset the settings of the spam detection engine for the domain, select the corresponding check box and click Update. Consequently, the domain settings will be reset to the global server settings.
 - Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option)
 - Spam message subject tag - When the previous option is enabled, this field contains the subject that will be used to tag spam messages.
 - Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
 - Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
 - IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
 - Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
 - Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
 - Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that

message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:

- Custom value - When this option is enabled, you must fill in the Custom value text box.
- Very permissive
- Permissive
- Moderate
- Strict
- Very strict
- Send daily statistics report - When you select this check box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

4. Click Update to save the changes.






Note

If you do not wish to modify a setting, select the **do not change** option.

Protecting Individual Mailboxes

The reseller 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, click the domain name link.

In the Mailbox protection section, the following columns are available for each mailbox:

- Dropped/Total - The number of dropped email messages that were not delivered because they were identified as spam out of the total number of email messages processed by the spam detection engine.
- Stats - By clicking the  Statistics icon, the reseller will be able to view the recorded statistics for the selected mailbox.
- S - By clicking the  Settings icon, the reseller will be able to define settings for the corresponding mailbox.
- Reset stats - By clicking the  Reset statistics icon, the reseller will reset the recorded statistics.



Note

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

- The Protected column, which can be found on the left of the mailbox name, comes with two clickable options describing whether the mailbox in question is protected or not. Here are the two options:
 1. Click the Enable link to enable mailbox protection. The Yes status under the Protected column confirms that mailbox protection is enabled.
 2. Click the Disable link to disable mailbox protection. The No status under the Protected column confirms that mailbox protection is disabled.



Note

When a domain is protected, all its mailboxes are protected.

To protect a mailbox, go to the Protected column and click the Enable option corresponding to the mailbox in question. To cancel mailbox protection, click the Disable option next to the mailbox name.

Protection can be enabled or disabled for several mailboxes at the same time.

Global Settings for Mailboxes

You can make the same changes to several mailboxes:

1. In the list of mailboxes, select the respective mailboxes.
2. Click Global changes
3. Make the desired changes. The following options are available:
 - Reset mailbox settings - To reset mailbox settings, the reseller 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).
 - 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. (see next option)
 - Spam message subject tag - When the previous option is enabled, the reseller can write in this field the subject that he wants to be used for spam messages tagging.

- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict

- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.


4. Click Update to save the changes



Note

If you do not wish to modify a setting, select the **do not change** option.

Mailbox Statistics

To view the statistics for a protected mailbox, click the  Stats icon corresponding to the chosen mailbox. A graphic with mailbox statistics is available in this area. Statistics take into consideration the total number of processed emails, the number of messages dropped, and the number of messages tagged by the spam detection 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 and processed by 4PSA Spam Guardian for the selected mailbox. The other two curves represent the number of email messages received and dropped by the spam detection engine and the number of email messages received and tagged. The reseller can modify the looks of the graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval, and the vertical oY axis the total number of emails received by the mailbox and processed by the spam detection engine.

Customize

In this section, the reseller 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 the graph. To select a date, the reseller must click the  Calendar icon.

- Tagged colour - The colour of the curve that displays the number of email messages received by the protected mailbox and tagged as spam by the engine.
- Dropped colour - The colour of the curve that displays the number of spam email messages received by the protected mailbox and dropped by the engine.
- Totals colour - The colour for the curve that displays the total number of emails received by the protected mailbox.
- Dots colour - The colour of the dotted lines across the graph.
- Label colour - The colour of the graph axis' labels.
- Axis colour - The colour of the oX and oY axes.
- Arrow colour - The colour of the arrows at the end of the axes.
- Graph background colour - The background colour for the plotted region.
- Canvas background colour - The background colour for the entire canvas (surrounding the plotted region).

Mailbox Statistics


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

- Total - The total number of emails received by the protected mailbox.
- Tagged - The number of spam email messages tagged by the spam detection engine.
- Dropped - The number of spam email messages dropped by the spam detection engine.
- Average processed - The average number of email messages received by the protect mailbox and processed every day.
- Average tagged - The average number of spam email messages tagged per day by the spam detection engine.
- Average dropped - The average number of spam email messages dropped per day by the spam detection engine.
- Minimum processed - The number of emails and the date when the minimum number of messages has been received by the protected mailbox.
- Minimum tagged - The number of spam emails and the date when the minimum number of spam messages has been tagged by the spam detection engine.
- Minimum dropped - The number of spam emails and the date when the minimum number of spam messages has been dropped by the spam detection engine.

- Maximum processed - The number of emails and the date when the maximum number of messages has been received by the protected mailbox.
- Maximum tagged - The number of spam emails and the date when the maximum number of spam messages has been tagged by the spam detection engine.
- Maximum dropped - The number of spam emails and the date when the maximum number of spam messages has been dropped by the spam detection engine.
- Percent dropped - The percentage of emails from the total number of emails received by the protected mailbox, dropped by the spam detection engine.
- Percent tagged - The percentage of emails from the total number of emails received by the protected mailbox, tagged by the spam detection engine.
- Best day - The percentage of spam emails and the date with the smallest percentage of spam emails received by the protected mailbox.
- Worst day - The percentage of spam emails and the date with the biggest percentage of spam emails received by the protected mailbox.

To clear statistics for the selected mailbox, click the Reset button. The global statistics available in the Settings area will be updated by this reset.

Mailbox Settings

To view the individual settings for the chosen mailbox, the reseller must click the  Settings icon on the chosen mailbox row. In this area, the reseller can modify the limits that apply to the selected mailbox.



Note

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

Spam Detection Engine Settings for Mailbox

In this section, the reseller can modify the following settings of the spam detection engine for the chosen mailbox:

- Reset mailbox settings - To reset mailbox settings, the reseller 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).

- 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. (see next option)
- Spam message subject tag - When the previous option is enabled, the reseller can write in this field the subject that he wants to be used for spam messages tagging.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- 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 - The reseller chooses from this field the address where spam messages are to be forwarded, after the option Enable spam forwarding has been enabled. The forward address must be on the same domain.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate

- Strict
- Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Send daily statistics report - When you select this check box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

To save the changes click Update.

White List Settings for Mailbox

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.
- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the mailbox White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.

2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the last address that you want to add.

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.
2. Click the Remove button

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue appears.
2. Name the file and choose the location where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list will be considered spam by the engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.
- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the mailbox Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the last address that you want to add.

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks for Mailbox

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - All the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the "IP address" text box, fill in the address you trust.
2. Click the Add button.



Note

You can select several IP addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Settings

In this area, the reseller can set the behaviour of 4PSA Spam Guardian with regard to the newly added domains.

To access this area, simply click the Settings button in the toolbar.



Note

This area will not be displayed unless the administrator has set at least one option under the **Allow resellers to manage the "Automatically protect new domain" permission for their customers** area.

Furthermore, the administrator can restrict the options available for the reseller.

Global Settings

If the administrator allows the reseller to manage the protection of newly created domains, according to the administrator settings, the reseller can use one of the following options for Automatically protect new domains:

- Use global value - With the help of this setting, the reseller delegates the administrator to manage the protection of their new domains against spam-infected messages.
- Never - According to this setting, the reseller's newly added domains (their own or their customers' domains or subscriptions) will not be automatically protected against spam-infected messages.
- If their service plan includes Spam Guardian - According to this setting, the reseller's newly added domains (their own or their customers' domains or subscriptions) will not be automatically protected against spam-infected messages unless they were created with Service Plans featuring an activated 4PSA Spam Guardian Additional Service.
- No matter their service plan - According to this setting, the reseller's newly added domains (their own or their customers' domains or subscriptions) will be automatically protected against spam-infected messages, even if they were created with Service Plans featuring an activated 4PSA Spam Guardian Additional Service.

Global value - This option is set by the administrator for the protection of all newly added domains.

Interface Settings



Note

This area will not be displayed unless the administrator has enabled the **Allow resellers to display their own message to their customers** option.

- Display message to customers - When enabled, this option will have the text written in the Message for customers field displayed under the form of an Info box in all the pages of the 4PSA Spam Guardian for the reseller's customers and users.
- Message for customers - When enabled, this option will display the text field in all the pages of 4PSA Spam Guardian at both customer and user level. Such messages can accept HTML tags and have an advertising or an informative role.

The value set for Message for customers will overwrite the administrator settings.



Note

Once the reseller decides to manage the customer's messages, the administrator will no longer be able to handle them. Therefore, any value the reseller sets for **Message for customers** will always overwrite the messages previously set by the administrator.

Reporting

In this area, the reseller can obtain and export statistics reports about the domains and mailboxes protected by 4PSA Spam Guardian.

This page displays detailed reports for each of the reseller's customers.

Use the Export to Excel link to save the selected report in a CSV (comma separated value) file.

The customer's report is displayed in a table containing the following data:

- Customer - The name of the customer.
- Total Domains - This column displays the total number of domains owned by the customer.
- Protected Domains - This column displays the total number of protected domains owned by the customer.
- Total Mailboxes - This column displays the total number of mailboxes created for all the domains owned by the customer.
- Protected Mailboxes - This column displays the total number of protected mailboxes created for all the domains owned by the customer.

The Customer or the Control Panel User Module

This chapter is dedicated to customers and Control Panel users with access to the Plesk Small Business Panel (smb). The 4PSA Spam Guardian can be accessed as soon as you log in to Plesk using a customer or a control panel user account. To open the 4PSA Spam Guardian interface, please select the Websites & Domains link from the toolbar and then click the [4PSA Spam Guardian](#) button.



Note

A Customer or a Control Panel user cannot access the 4PSA Spam Guardian interface unless the selected subscription is created based on a Hosting Service Plan and its 4PSA Spam Guardian additional service is enabled.

The 4PSA Spam Guardian toolbar is available on top of the application's interface. The toolbar makes it easy for the customer or the control panel user to perform the following operations:

- Set up protection for the entire domain and individual mailboxes.
- View statistics for mailboxes and the entire domain.
- Change and reset mailbox settings.

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 the Domains list, the customer will only be able to see the domains created under the current subscription. If the customer owns several subscriptions, they should switch between subscriptions in order to configure 4PSA Spam Guardian for all their domains.

In this area, the customer can view 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 - The number of dropped email messages that were not delivered because they were identified as spam out of the total number of email messages processed by the spam detection engine. This column is available only if statistics are enabled on the server.

Each domain has three columns displaying the following actions:

- Stats - By clicking the  Statistics icon, the customer or the control panel user will be able to view the recorded statistics for his domain.
- S - By clicking the  Settings icon, the customer or the control panel user will be able to define settings for his domain
- Reset stats - By clicking the  Reset statistics icon, the customer or the control panel user will reset the recorded statistics.



Note


These columns are visible if there is at least one protected mailbox on that domain and if statistics are enabled on the server.

The Protected column, which can be found on the left of the domain name, comes with two clickable options describing whether the domain in question is protected or not. Here are the two options:

1. Click the Enable link to enable domain protection. The Yes status under the Protected column confirms that domain protection is enabled.
2. Click the Disable link to disable domain protection. The No status under the Protected column confirms that domain protection is disabled.

To protect an entire domain, you need to go to the Protected column and click the Enable option corresponding to the domain in question. To cancel domain protection, click the Disable option next to the domain name.

Domain Statistics

To view the statistics for an entire domain, click the  Stats icon. A graphic with the domain statistics is available in this area. Statistics take into consideration the total number of processed emails, the number of messages dropped, and the number of messages tagged by the spam detection engine.



Note

The domain statistics are available if there is at least one protected mailbox on the domain and if statistics are enabled on the server.

Domain Statistics Graph


In this graph, one curve represents the total number of emails received and processed by 4PSA Spam Guardian for the selected domain. The other two

curves represent the number of email messages received and dropped by the spam detection engine and the number of email messages received and tagged. The domain user can modify the looks of the graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval while the vertical oY axis the total number of emails received by the selected domain and processed by the spam detection engine.

Customize

In this section, the customer or the control panel user can change the time interval displayed in the graph and the graph's look. These are the available options:

- Start and End date - The start and the end dates of the time interval for the graph. To select a date, the customer or the control panel user must click the  Calendar icon.
- Tagged colour - The colour of the curve that displays the number of email messages received by the protected mailboxes of the selected domain and tagged as spam by the engine.
- Dropped colour - The colour of the curve that displays the number of spam email messages received by the protected mailboxes of the selected domain and dropped by the engine.
- Totals colour - The colour for the curve that displays the total number of emails received by the protected mailboxes of the selected domain.
- Dots colour - The colour of the dotted lines across the graph.
- Label colour - The colour of the graph axis' labels.
- Axis colour - The colour of the oX and oY axes.
- Arrow colour - The colour of the arrows at the end of the axes.
- Graph background colour - The background colour for the plotted region.
- Canvas background colour - The background colour for the entire canvas (surrounding the plotted region).

Domain Statistics


In this section, 4PSA Spam Guardian displays the following information:

- Total - The total number of emails received by the protected mailboxes of the selected domain.
- Tagged - The number of spam email messages tagged by the spam detection engine.

- Dropped - The number of spam email messages dropped by the spam detection engine.
- Average processed - The average number of email messages received by the protected mailboxes of the domain and processed every day.
- Average tagged - The average number of spam email messages tagged per day by the spam detection engine.
- Average dropped - The average number of spam email messages dropped per day by the spam detection engine.
- Minimum processed - The number of emails and the date when the minimum number of messages has been received by the protected mailboxes of the domain.
- Minimum tagged - The number of spam emails and the date when the minimum number of spam messages has been tagged by the spam detection engine.
- Minimum dropped - The number of spam emails and the date when the minimum number of spam messages has been dropped by the spam detection engine.
- Maximum processed - The number of emails and the date when the maximum number of messages has been received by the protected mailboxes of the domain.
- Maximum tagged - The number of spam emails and the date when the maximum number of spam messages has been tagged by the spam detection engine.
- Maximum dropped - The number of spam emails and the date when the maximum number of spam messages has been dropped by the spam detection engine.
- Percent dropped - The percentage of emails from the total number of emails received by the protected mailboxes of the domain, dropped by the spam detection engine.
- Percent tagged - The percentage of emails from the total number of emails received by the protected mailboxes of the domain, tagged by the spam detection engine.
- Best day - The percentage of spam emails and the date with the smallest percentage of spam emails received by the protected mailboxes of the domain.
- Worst day - The percentage of spam emails and the date with the biggest percentage of spam emails received by the protected mailboxes of the domain.

To clear statistics for the domain, click the Reset button.

Domain Settings

In order to view the individual settings for his domain, the customer or the control panel user must click the  Settings icon. In this area, the customer or the control panel user can modify the available settings.



Note

he settings for mailboxes override the settings for the domain. The settings for domains override the global settings for server. If you want to enable higher or lower limits for a particular mailbox, change the corresponding individual settings.

Spam Detection Engine Settings for Domain

In this section, the customer or the control panel user can modify the settings of the spam detection engine for his domain.

- Reset domain settings - To reset the domain settings, the customer or the control panel user must enable this option and click Update.
- 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. (see next option)
- Spam message subject tag - When the previous option is enabled, the customer or the control panel user can write in this field the subject that he wants to be used for spam message tagging.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:

- Custom value - When this option is enabled, you must fill in the Custom value text box.
- Very permissive
- Permissive
- Moderate
- Strict
- Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

To save the changes, click Update.

White List Settings for Domain

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.



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.

- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.
2. Click the Remove button.



Note

You can select several email addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Black List Settings for Domain

Email messages originating from the addresses in the Black list will be considered spam by the engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.



Note

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

- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the next address that you want to add.

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks for Domain

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include on this list single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - All the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the IP address text box, fill in the address you trust.
2. Click the Add button.



Note

You can select several IP addresses at the same time by holding down the `Ctrl` key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the `Shift` key and then clicking the last address that you want to add.

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the "Always reject mail from these networks" select list, choose one or more addresses.
2. Click the Remove button.

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.

2. Name the file and choose the location where you want to save the file.

Global Settings for Domains

You can make the same changes to several domains:

1. In the list of domains, select the respective domains.
2. Click Global changes
3. Make the desired changes. The following options are available:
 - Reset domain settings - To reset the settings of the spam detection engine for the domain, select the corresponding box and click Update. Consequently, the domain settings will be reset to the global server settings.
 - Modify spam message subject - When this option is enabled, 4PSA Spam Guardian will change the subject of a spam message with the text available in the Spam message subject tag field. (see next option)
 - Spam message subject tag - When the previous option is enabled, this field contains the subject that will be used to tag spam messages.
 - Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
 - Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
 - IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
 - Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
 - Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive

- Moderate
- Strict
- Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

4. Click Update to save the changes.






Note

If you do not wish to modify a setting, select the **do not change** option.

Protecting Individual Mailboxes

The customer or the control panel 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 - The number of dropped email messages that were not delivered because they were identified as spam out of the total number of email messages processed by the spam detection engine.
- Stats - By clicking the  Statistics icon, the customer or the control panel user will be able to view the recorded statistics for the selected mailbox.

- S - By clicking the  Settings icon, the customer or the control panel user will be able to define settings for the selected mailbox.
- Reset stats - By clicking the  Reset statistics icon, the customer or the control panel user will reset the recorded statistics.



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.

- The Protected column, which can be found on the left of the mailbox name, comes with two clickable options describing whether the mailbox in question is protected or not. Here are the two options:
 1. Click the Enable link to enable mailbox protection. The Yes status under the Protected column confirms that mailbox protection is enabled.
 2. Click the Disable link to disable mailbox protection. The No status under the Protected column confirms that mailbox protection is disabled.



Note

When a domain is protected, all its mailboxes are protected.


To protect a mailbox, go to the Protected column and click the Enable option corresponding to the mailbox in question. To cancel mailbox protection, click the Disable option next to the mailbox name.

Protection can be enabled or disabled for several mailboxes at the same time. To do this, please follow the steps below:

1. Select the check boxes on the right corresponding to the respective mailboxes.
2. Click the Toggle protection button.

The mailboxes that were not protected will be protected and the mailboxes that were protected will be unprotected.

Mailbox Statistics

To view the statistics for a protected mailbox, the customer or the control panel 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 detection 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

In this graph, one curve represents the total number of emails received by the mailbox and processed by 4PSA Spam Guardian, while the other curve represents the number of email messages received by this specific mailbox and dropped by the spam detection engine. The customer or the control panel user can change the looks of this graph by making changes in the Customize area below.

The horizontal oX axis displays the selected time interval and the vertical oY axis the total number of emails received by the mailbox and processed by the spam detection engine.

Customize

In this section, the customer or the control panel 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 customer or the control panel user must click on the  Calendar icon.
- Tagged colour - The colour of the curve that displays the number of email messages received by the protected mailbox and considered spam by the engine.
- Dropped colour - The colour for the curve that displays the number of email messages received by this mailbox and dropped by the spam detection engine.
- Totals colour - The colour for the curve that displays the total number of emails received by this mailbox and processed by the spam detection engine.
- Dots colour - The colour of the dotted lines across the graph.
- Label colour - The colour of the graph axis' labels.

- Axis colour - The colour of the oX and oY axis.
- Arrow colour - The colour of the arrows at the end of the axis.
- Graph background colour - The background colour for the plotted region.
- Canvas background colour - The background colour for the entire canvas (surrounding the plotted region).

Mailbox Statistics


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

- Total - The total number of emails received by this mailbox and processed by the spam detection engine.
- Dropped - The number of email messages received by this mailbox and dropped by the spam detection engine.
- Average processed - The average number of email messages received by this mailbox and processed every day by the spam detection engine.
- Average dropped - The average number of email messages received every day by this mailbox and dropped by the spam detection engine.
- Minimum processed - The date when the spam detection engine processed the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages have been processed that day.
- Minimum dropped - The date when the spam detection engine dropped the lowest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages have been dropped that day.
- Maximum processed - The date when the spam detection engine processed the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages have been processed that day.
- Maximum dropped - The date when the spam detection engine dropped the highest number of email messages for this mailbox. 4PSA Spam Guardian also lets you know how many messages have been dropped that day.
- Percent dropped - The percentage of dropped emails from the total number of emails processed by the spam detection 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 the bottom right corner allows the customer or the control panel user to clear statistics for the selected mailbox. Both dropped and total statistics for the mailbox will be reset.

Mailbox Settings

To view the individual settings of a particular mailbox, the customer or the control panel user must click the  Settings icon corresponding to the chosen mailbox. In this area, the customer or the control panel user can modify the limits that apply to the chosen mailbox.



Note

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

Spam Detection Engine Settings for Mailbox

In this section, the customer or the control panel user can modify the following settings of the spam detection engine for the selected mailbox:

- Reset mailbox settings - To reset mailbox settings, the customer or the control panel 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).
- 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. (see next option)
- Spam message subject tag - When the previous option is enabled, the customer or the control panel user can write in this field the subject that he wants to be used for spam message tagging.
- Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
- Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.

- IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
- Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.
- 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 - The customer or the control panel user chooses from this field the address where spam messages are to be forwarded, after the option Enable spam forwarding has been enabled. The forward address must be on the same domain.
- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages with a score value higher than the value set in this field, will be dropped by the engine. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict

- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

To save the changes, click Update.

White List Settings for Mailbox

The spam protection engine will not process email messages originating from the addresses in the White List. In this section, you can edit the following settings for your White List:

- Email address - Use this text box to fill in a trusted email address.
- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the mailbox White List.

To add an email address to the White List, follow these steps:

1. In the Email address text box, fill in the trusted address.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the next address that you want to add.

To remove an email address from the White List, follow these steps:

1. From the Always accept mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The White List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Black List Settings for Mailbox

Email messages originating from the addresses in the Black list will be considered spam by the engine. In this section, you can edit the following settings for your Black list:

- Email address - Use this text box to fill in an email address that you do not trust.
- Import from file - Enter the name of the file that contains the email addresses you want 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 - This select list contains all the email addresses available in the domain's Black list.

To add an email address to the Black list, follow these steps:

1. In the Email address text box, fill in the address you do not trust.
2. Click the Add button.



Note

You can select several email addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive email addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the next address that you want to add

To remove an email address from the Black list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.

2. Click the Remove button.

The Black List can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Trusted Networks for Mailbox

The spam protection engine will not process email messages originating from the networks in this list. You can edit the following settings:

- IP address - Use this text box to fill in an IP address.

You can include single IP addresses or an entire network or sub-network. For example:

192.168.1.1 - Single IP address.

192.168. - All the IP addresses in the 192.168.0.0/16 sub-network.

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



Note

When both **IP 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 networks - These are the IP addresses currently available in the domain's trusted networks list.

To add an IP address to the Trusted Networks list, follow these steps:

1. In the IP address text box, fill in the address you trust.
2. Click the Add button.



Note

You can select several IP addresses at the same time by holding down the **Ctrl** key while clicking the addresses. You can select several consecutive IP addresses at the same time by clicking the first address, pressing the **Shift** key and then clicking the next address that you want to add.

To remove an IP address from the Trusted Networks list, follow these steps:

1. From the Always reject mail from these addresses select list, choose one or more addresses.
2. Click the Remove button.

The Trusted Networks list can be exported as a text file. To save it on your local computer:

1. Click the Export button. A file download dialogue opens.
2. Name the file and choose the location where you want to save the file.

Global Settings for Mailboxes

You can make the same changes to several mailboxes:

1. In the list of mailboxes, select the respective mailboxes.
2. Click Global changes
3. Make the desired changes. The following options are available:
 - Reset mailbox settings - To reset mailbox settings, the customer or the control panel 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).
 - 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. (see next option)
 - Spam message subject tag - When the previous option is enabled, the customer or the control panel user can write in this field the subject that he wants to be used for spam messages tagging.
 - Spam message as attachment - When this option is enabled, the messages detected to be spam are attached to emails and sent to the message recipients.
 - Save spam to IMAP folder - When this box is checked, emails identified as spam will be saved to a separate IMAP type folder.
 - IMAP folder to save spam in - This is the folder where emails identified as spam are kept, if the save option is enabled.
 - Delete mails after - The number of days the emails are stored in the IMAP folder. After this period of time, the emails in the IMAP folder are deleted.

- Tag engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. Messages that have scored a value higher than the value set in this field will be tagged as spam. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Drop engine sensitivity - Each message processed by the spam detection engine receives a score indicating the probability of that message being spam. A higher score means a higher probability that the message is spam. The engine will drop messages with a score value higher than the value set in this field. Use the drop-down list to select one of the available options:
 - Custom value - When this option is enabled, you must fill in the Custom value text box.
 - Very permissive
 - Permissive
 - Moderate
 - Strict
 - Very strict
- Send daily statistics report - When you check this box, the spam detection engine will send daily statistical reports on the number of emails tagged as spam or dropped, out of the total received messages.

4. Click Update to save the changes



Note

If you do not wish to modify a setting, select the **do not change** option.

Contact and Support

For online help and support please visit:

- Support Zone: <https://help.4psa.com>
- Knowledge Base: <http://kb.4psa.com>
- Documentation: <http://help.4psa.com/docs/>

For mailing addresses and phone numbers from our offices:

<http://www.4psa.com/contactus>

If you have any question, do not hesitate to contact us.