Chapter 3

The Client Module

The 4PSA Spam Guardian client module can be accessed by logging in Plesk with a client account. To access the 4PSA Spam Guardian interface, go to the left navigation menu and in the "Custom" menu click the 4PSA Spam Guardian link.

Note

To be able to access and manage 4PSA Spam Guardian, the client must have permissions from the server administrator.

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

- Setup protection for entire domains and individual mailboxes
- View statistics for mailboxes and domains
- Change settings for domains and mailboxes
- Grant management permissions to domain administrators

1. Protecting Domains Globally

In the Domains area, the client can protect entire domains against spam messages. To access this area, the toolbar click the **Domains** tab 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. Next 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 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 client will be able to view the recorded statistics for the selected domain.
- **S** - By clicking the **Settings** icon, the client will be able to define settings for the selected domain.
- **Reset stats** – By clicking the **Reset statistics** icon, the client 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.

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, follow these steps:

1. In the Domains table, check the **Protect** checkbox of the chosen domain.
2. Click **Update**.

You can later disable domain protection by un-checking the same checkbox and clicking **Update**.

The domain protection can be enabled or disabled for several domains at the same time.

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 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 client 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 client 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 client 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.

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.

Tip

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 settings in the “Settings for mailbox” area.

Spam Detection Engine Settings for Domain

In this section, the client 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.
- **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.

- **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 dropdown list to select one of the available options:
    - Custom value – When this option is enabled, you must fill in the **Custom value** textbox.
    - 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 dropdown list to select one of the available options:
    - Custom value – When this option is enabled, you must fill in the **Custom value** textbox.
    - 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 textbox 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** textbox, 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 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 textbox 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** textbox, 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 dialog 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 textbox 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" textbox, 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 dialog opens.
2. Name the file and choose the location where you want to save the file.

Protecting Individual Mailboxes

The client can protect individual mailboxes against spam messages. The number of protected mailboxes for every hosted domain is available in the Protected Mailboxes column. For more details about the mailboxes, 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 client will be able to view the recorded statistics for the selected mailbox.
- **S** - By clicking the **Settings** icon, the client will be able to define settings for the corresponding mailbox.
- **Reset stats** – By clicking the **Reset statistics** icon, the client will reset the 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.

- **Protect** – When this option is enabled, 4PSA Spam Guardian protects the corresponding mailbox against spam messages.

Note

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

To protect a mailbox, check the "Protect" checkbox for the chosen mailbox and click **Update**. You can later disable mailbox protection by un-checking the same checkbox and clicking **Update**.

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

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

- **Start** and **End date** – The start and the end dates of the time interval for the graph. To select a date, the client must click the **Calendar** icon.
- **Tagged color** – The color of the curve that displays the number of email messages received by the protected mailbox 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 mailbox and dropped by the engine
- **Totals color** – The color for the curve that displays the total number of emails received by the protected mailbox
- **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)

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.

Settings for Mailbox

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

Tip

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

Spam Detection Engine Settings for Mailbox

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

- **Reset mailbox settings** – To reset mailbox settings, the client must enable this option and click **Update**. The mailbox settings will be reset to the global server settings or to the domain settings (if these exist).
- **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.
- **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 client 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.
- **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 client 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 in 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.
- **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 dropdown list to select one of the available options:
    - Custom value – When this option is enabled, you must fill in the **Custom value** textbox.
    - 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 dropdown list to select one of the available options:
    - Custom value – When this option is enabled, you must fill in the **Custom value** textbox.
    - 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 textbox 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** textbox, 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:

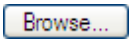
1. From the "Always accept mail from these addresses" select list, choose one or more addresses.
2. Click the **Remove** button.

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 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 textbox 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 

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** textbox, 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 dialog 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 textbox 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" textbox, 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 dialog opens.
2. Name the file and choose the location where you want to save the file.

2. Management Permissions

In the Permissions area, the client can grant 4PSA Spam Guardian management permissions to domain administrators. This means that domain administrators will be able to choose for themselves which mailboxes to protect from spam messages.

To access this area, click the **Permissions** tab in the toolbar on the top of the interface.

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

You can grant/revoke management permissions for several domain administrators at the same time.