

**COMODO**  
CYBERSECURITY



# Comodo Secure Email Gateway MSP

Software Version 2.12

## User Guide

Guide Version 2.12.051920

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ, 07013

## Table of Contents

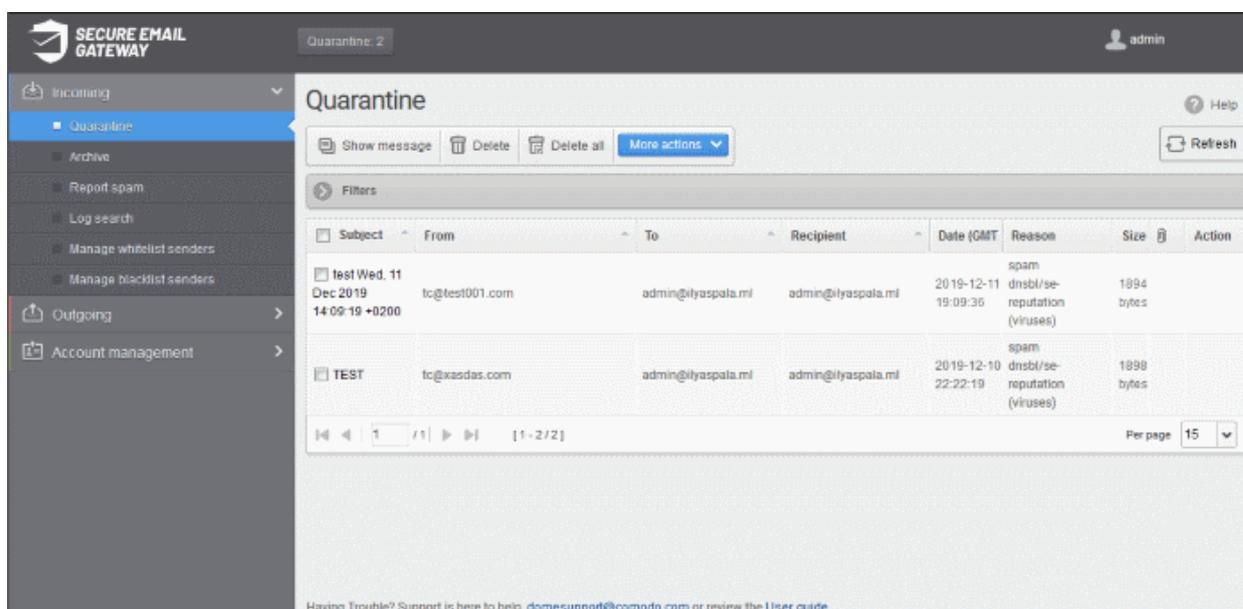
<b>1</b>	<b>Introduction to Comodo Secure Email Gateway - MSP.....</b>	<b>3</b>
<b>2</b>	<b>How to...Tutorials.....</b>	<b>4</b>
2.1	How to Login to CSEG.....	4
2.2	How to Get a New Password.....	6
2.3	How to Manage your Quarantined Mails.....	8
2.4	How to Use Filter Options in the Quarantined Emails Interface.....	17
2.5	How to Check when an Expected Email is not Received.....	17
2.6	How to Retrieve an Email which had a Virus Attachment.....	20
2.7	How to Restore Deleted Mails.....	23
2.8	How to Reply to Archive Mails.....	25
2.9	How to Subscribe for Quarantine Reports.....	27
2.10	How to Perform a Log Search of your Incoming Emails.....	28
2.11	How to Add or Remove yourself from Recipient Whitelist.....	30
2.12	How to Report Spam Emails.....	31
2.13	How to Perform a Log Search of your Outgoing Emails.....	34
2.14	How to Manage Whitelisted Senders.....	37
2.15	How to Manage Blacklisted Senders.....	39
<b>3</b>	<b>The CSEG User Console.....</b>	<b>42</b>
3.1	Login to the User Interface.....	42
3.2	The User Interface.....	45
3.2.1	Incoming.....	46
3.2.1.1	Quarantine.....	46
3.2.1.2	Mail Archive.....	57
3.2.1.3	Report Spam.....	70
3.2.1.4	Log Search.....	71
3.2.1.5	Manage Whitelist Senders.....	73
3.2.1.6	Manage Blacklisted Senders.....	76
3.2.2	Outgoing.....	79
3.2.2.1	Log Search.....	79
3.2.3	User Account Management.....	82
3.2.3.1	Manage Profile Settings.....	82
3.2.3.2	Manage Subscriptions to Summary Reports.....	86
<b>4</b>	<b>CSEG Reports.....</b>	<b>88</b>
	<b>Appendix - CSEG Feature List.....</b>	<b>89</b>
	<b>About Comodo Security Solutions.....</b>	<b>90</b>

# 1 Introduction to Comodo Secure Email Gateway - MSP

Comodo Secure Email Gateway - MSP (CSEG) is an email filtering solution that blocks spam, email-borne viruses and other unwanted mail from reaching your inbox. It helps protect you from phishing and malware emails, and saves you the daily hassle of deleting spam. You can log into your CSEG user account to quickly check/release quarantined mails and search log files. You can also modify your account settings and change your password from this interface.

Features and benefits include:

- Complete Antispam protection for incoming mails
- Complete Antispam protection for outgoing mails
- Easy to use and configure
- Easy to manage quarantine
- Easy to manage recipient whitelist
- Easy to manage sender blacklist



## Guide Structure

This guide is intended to take you through the use of Comodo Secure Email Gateway - MSP and is broken down to the following main sections.

- **How to...** - How to use specific features.
- **The User Interface** - A snapshot of the main functional areas of CSEG.
  - **Login to the User Interface** - How to login to the CSEG interface.
  - **The Dashboard Area** - Describes briefly about Quarantine management and Account management.
    - **Incoming** - How to manage quarantined mails and perform log searches of incoming emails.
    - **Outgoing** - How to perform log searches of outgoing emails.
    - **Account Management** - How to change your password, update the recipient whitelist, manage subscriptions to quarantine reports and configure notification language.
- **CSEG Reports** - An overview of quarantine reports generated and sent by CSEG.
- **Appendix** - List of CSEG Features

## Quick Link to Online Help Guide

Various interfaces will display a help button  at the top-right of the interface. Click the help button to visit the help page for the interface you have open.

Access to various interfaces in the application depends on the permission levels set for you by your administrator. Contact your administrator if you need to access to features that have been blocked to you.

## 2 How to...Tutorials

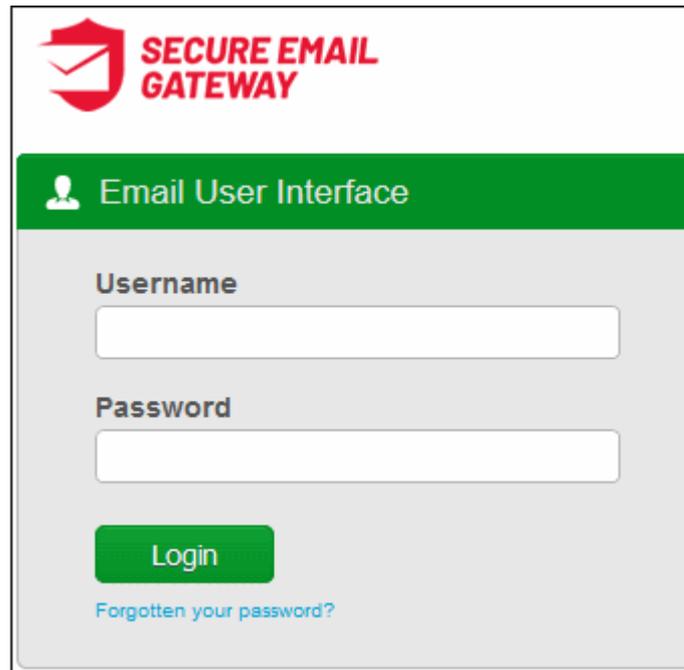
This section contains quick guides to help you use CSEG effectively:

- [How to login to CSEG](#)
- [How to get a new password](#)
- [How to manage your quarantined mails](#)
- [How to use filter options in the Quarantined emails interface](#)
- [How to check when an expected email is not received](#)
- [How to retrieve an email which had virus attachment](#)
- [How to restore deleted mails](#)
- [How to reply to archive mails](#)
- [How to subscribe for Quarantine Reports](#)
- [How to perform a log search of your incoming emails](#)
- [How to add or remove a user from recipient whitelist](#)
- [How to report spam emails](#)
- [How to perform a log search of your outgoing emails](#)
- [How to manage whitelisted senders](#)
- [How to manage blacklisted senders](#)

### 2.1 How to Login to CSEG

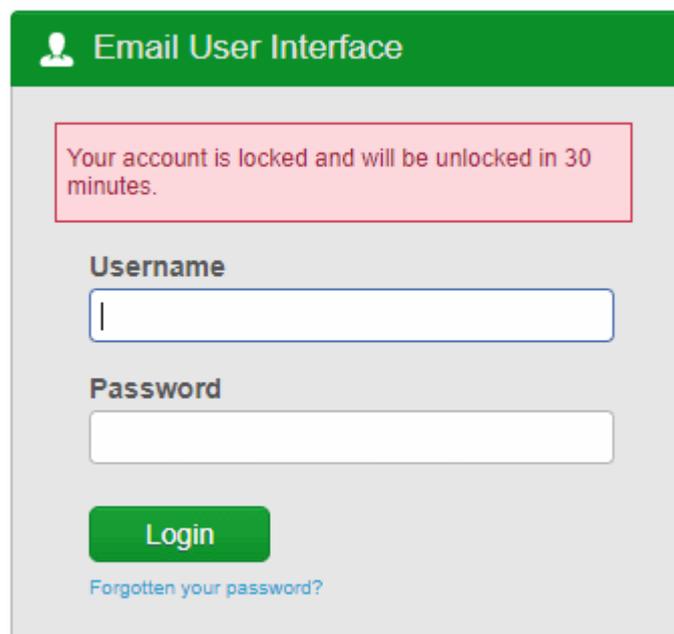
You can login into your account at one of the following URLs using any internet browser. Your admin should tell you which one to use:

- USA users - <https://us-domeasmsp.cdome.net/user/login.zul>
- EU users - <https://domeasmsp.cdome.net/user/login.zul>



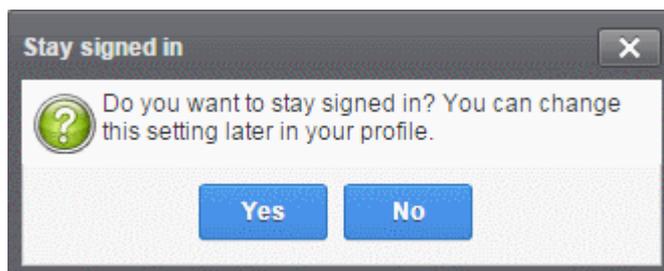
- Login to your account with the username and password that were sent to you via email after your CSEG account was created.

For security, CSEG will lock the account for 30 minutes after three failed login attempts. Please contact your administrator if you want to unlock the account immediately.



- Click 'Forgotten your password?' if you can't remember your password. [Click here](#) if you want help with the password retrieval process.

After first login, you might be offered the opportunity to stay signed-in if so configured your administrator:



- Click 'Yes' to enable the feature.

You can change these settings anytime in 'My Profile' > 'Change settings'. The 'Stay signed in' check-box is only available if your administrator has enabled the option for the domain.

## 2.2 How to Get a New Password

If you have forgotten your password, you can reset it using one of the following methods:

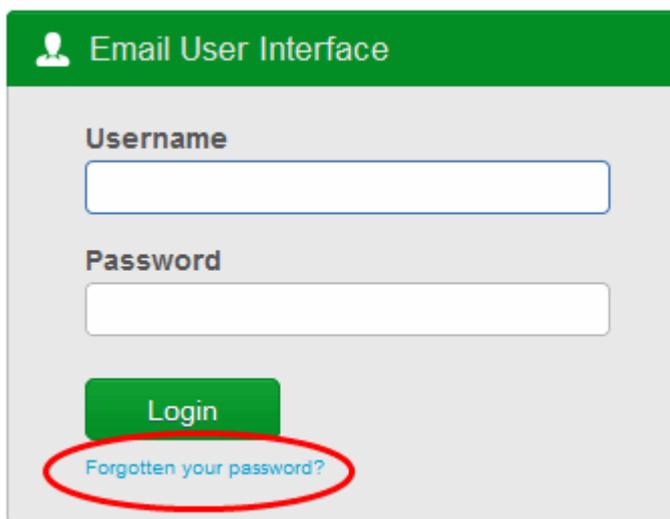
- Click the 'Forgotten your password?' link under the login button
- Request your administrator to generate a new password for you.

If you want to change your password for other reasons than login, click 'My Profile' then 'Change Password'.

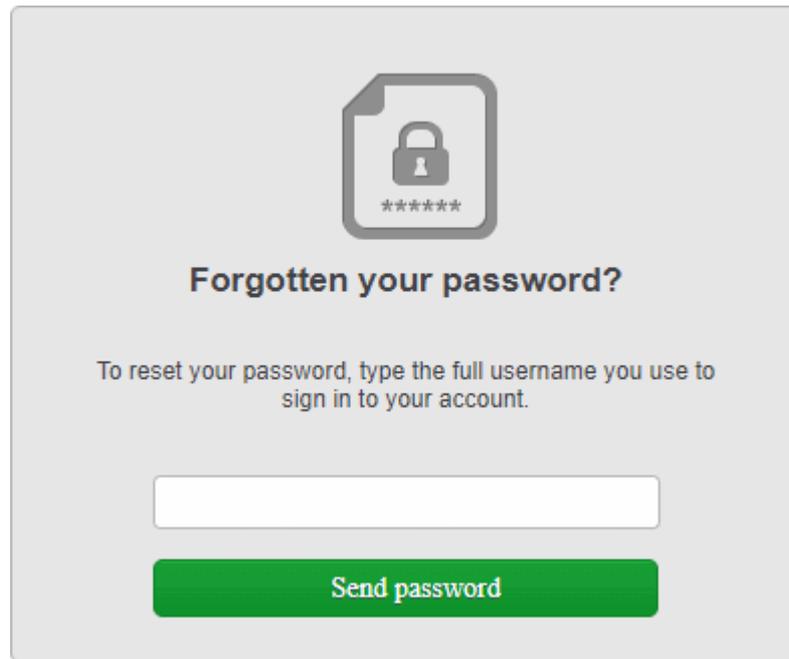
Note. Only users that have successfully logged in at least once can reset their password using the 'Forgotten your password?' link. If you are a new user, contact your admin.

### Generate a new password from CSEG login interface

- Visit <https://domeasmsp.cdome.net/user/login.zul> or <https://us-domeasmsp.cdome.net/user/login.zul> as appropriate
- Click the 'Forgotten your password?' link to reset your password:



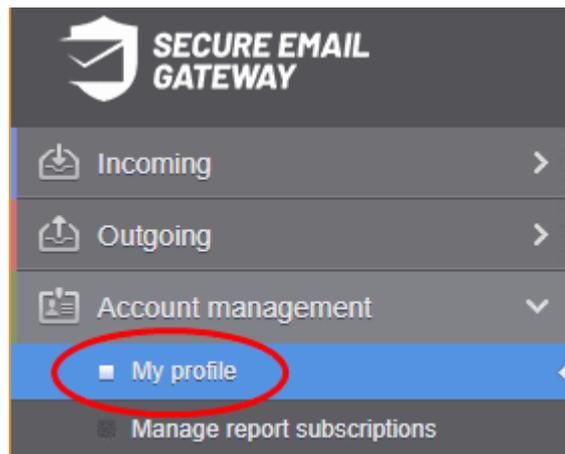
- Enter your full username, including domain address. For example, **johnsmith@example.com**. Click the 'Send password' button.



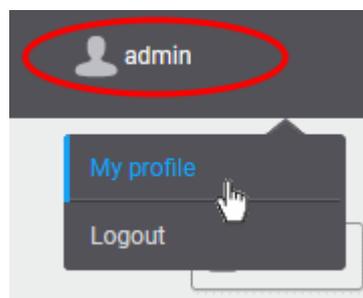
A new password is generated and sent to your email address.

### Change your current password

- Login to the CSEG interface.
- Click 'Account management' on the left then select 'My profile'.



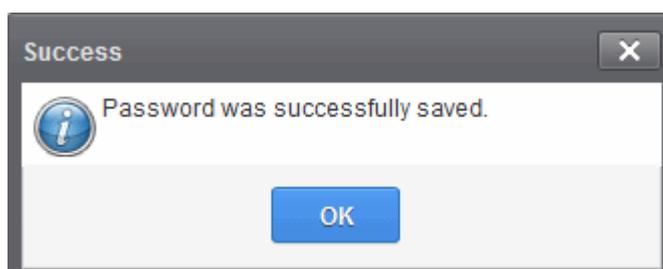
Alternatively, click your username at top-right then select 'My Profile'.



This opens the 'My Profile' page:

- In the 'Change password' section, enter and confirm your new password then click 'Save'.

You will see a confirmation as follows:



- Click 'OK'.

You can now access the CSEG interface with your new password.

## 2.3 How to Manage your Quarantined Mails

All spam, phishing and suspicious emails sent to your mailbox are quarantined by Comodo Secure Email Gateway. The quarantine interface allows you to manage those mails. You can read and even download attachments from them if you are sure they are safe.

There are two ways you can view quarantined mails:

- **From the Notification email**
- **From the CSEG User Interface**

### Quarantine Notification Email

All spam or mails containing malicious content or attachments are moved to quarantine. You will receive a notification when we quarantine one of your emails. The notification mail has a link that allows you to view the message.



## New quarantined message for [admin@bulut.ml](mailto:admin@bulut.ml)

Sender: [muratti66@hotmail.com](mailto:muratti66@hotmail.com)  
Date: Dec 05, 2019 07:04  
Subject: püff  
Reason: spam Combined (0.99)

For help, see the User guide: <https://help.comodo.com/topic-445-1-917-12240-Introduction-to-Comodo-Dome-Antispam---MSP.html>

Having Trouble? Support is here to help, [domesupport@comodo.com](mailto:domesupport@comodo.com) or review the [Users Guide](#)

- Click the shield logo at the top of the mail to open the CSEG login page.
- If your admin has enabled auto-login for your domain, the mail will also contain links to request release, whitelist/blacklist the sender, or delete the mail from quarantine.

## CSEG Quarantine Interface

The quarantine area lets you view all your quarantined emails. From this interface you can::

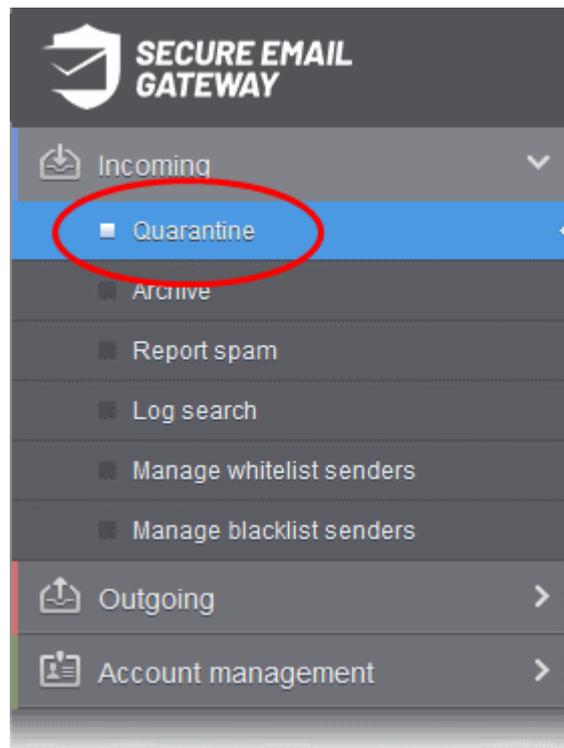
- Request your administrator to release quarantined emails.
- Add senders to the whitelist or blacklist.
- Delete spam mails as required.

**Note:** Please contact your administrator if you are not able to view your mails.

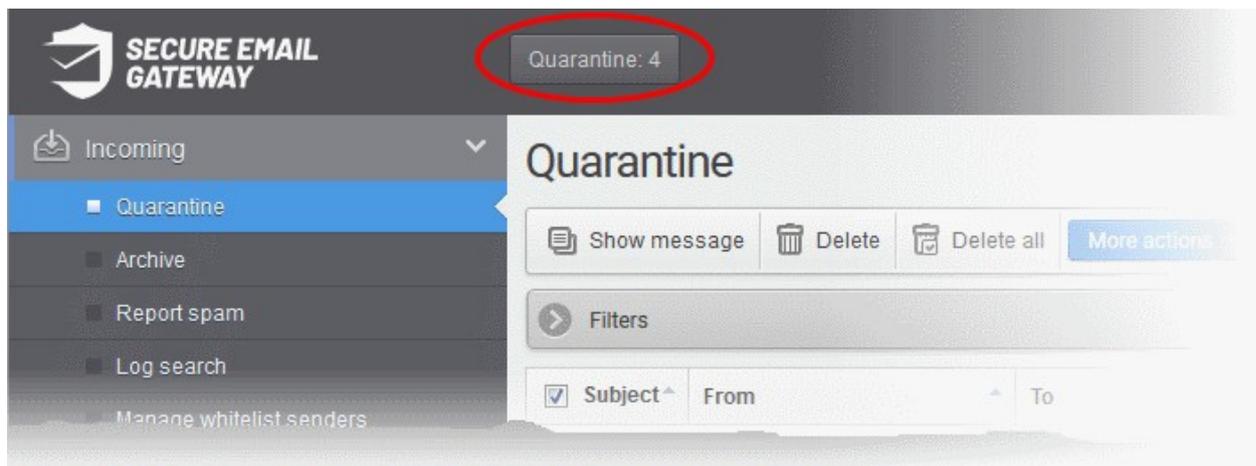
**Tip:** You can configure CSEG to send you regular reports of all your quarantined emails. See [How to Subscribe for Periodical Quarantine Report Summary](#) for help with this.

## Open the quarantine interface

- [Login](#) to CSEG
- Click 'Incoming' on the left then 'Quarantine'



- Alternatively, click the 'Quarantine' button at the top.



The quarantine interface contains details about each mail:

The screenshot shows the 'Quarantine' interface with the following elements:

- Buttons: Show message, Delete, Delete all, More actions (dropdown), Show messages for all aliases (checkbox), Refresh.
- Filters: A search bar for filtering messages.
- Table of Quarantined Messages:
 

Subject	From	To	Recipient	Date (GMT)	Reason	Size	Action
<input type="checkbox"/> Fw: Become a certified cloud computing professional	Stealing Talent <teacher@stealingtalent.com>	robin@democasg.com	robin@democasg.com	2016-02-2 09:04:25	spam Combined (0.15)	20.89 KB	[Action]
<input type="checkbox"/> Fw: Make your journey more exciting with 0 first year fee and rewards	Bullock Travels <marketing@yaktouring.org>	bob@democasg.com	bob@democasg.com	2016-02-2 08:43:01	spam Combined (0.15)	14.42 KB	[Action]
<input type="checkbox"/> Fw: Investment with lasting returns	Money Swindlers <campaign@mswindlers.org>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:47	spam Combined (0.14)	5.91 KB	[Action]
<input checked="" type="checkbox"/> Fw: Get upto 90% off on household items.	Brokenpot Sellers <offers@brokenpotsellers.co.uk>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:03	spam Combined (0.19)	6.1 KB	[Action]
- Navigation: Page 1 of 1, [ 1 - 4 / 4 ], Per page 15.

- **More Actions** - Request that the mail is released from quarantine, or that the sender is added to the blacklist or whitelist.
- **Show messages for all aliases** - By default, the list only shows mails sent to your primary email address. Select this option to view messages sent to all your mailboxes.

From this interface you can:

- **View quarantined mails**
- **Request administrator to release quarantined mails**
- **Request administrator to add sender to blacklist**
- **Request administrator to add sender to whitelist**

Click 'Filters' to search for particular email. See '**How to use filters**' topic for more details.

### View Quarantined Mails

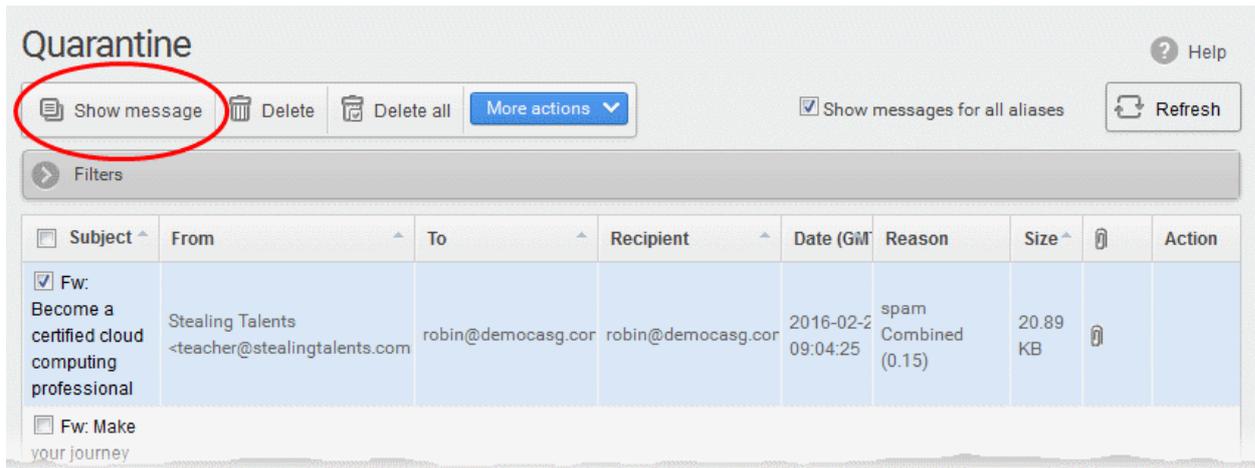
The mails added to the Quarantine can be viewed in two ways:

- **In the same CSEG window**
- **In a new CSEG window**

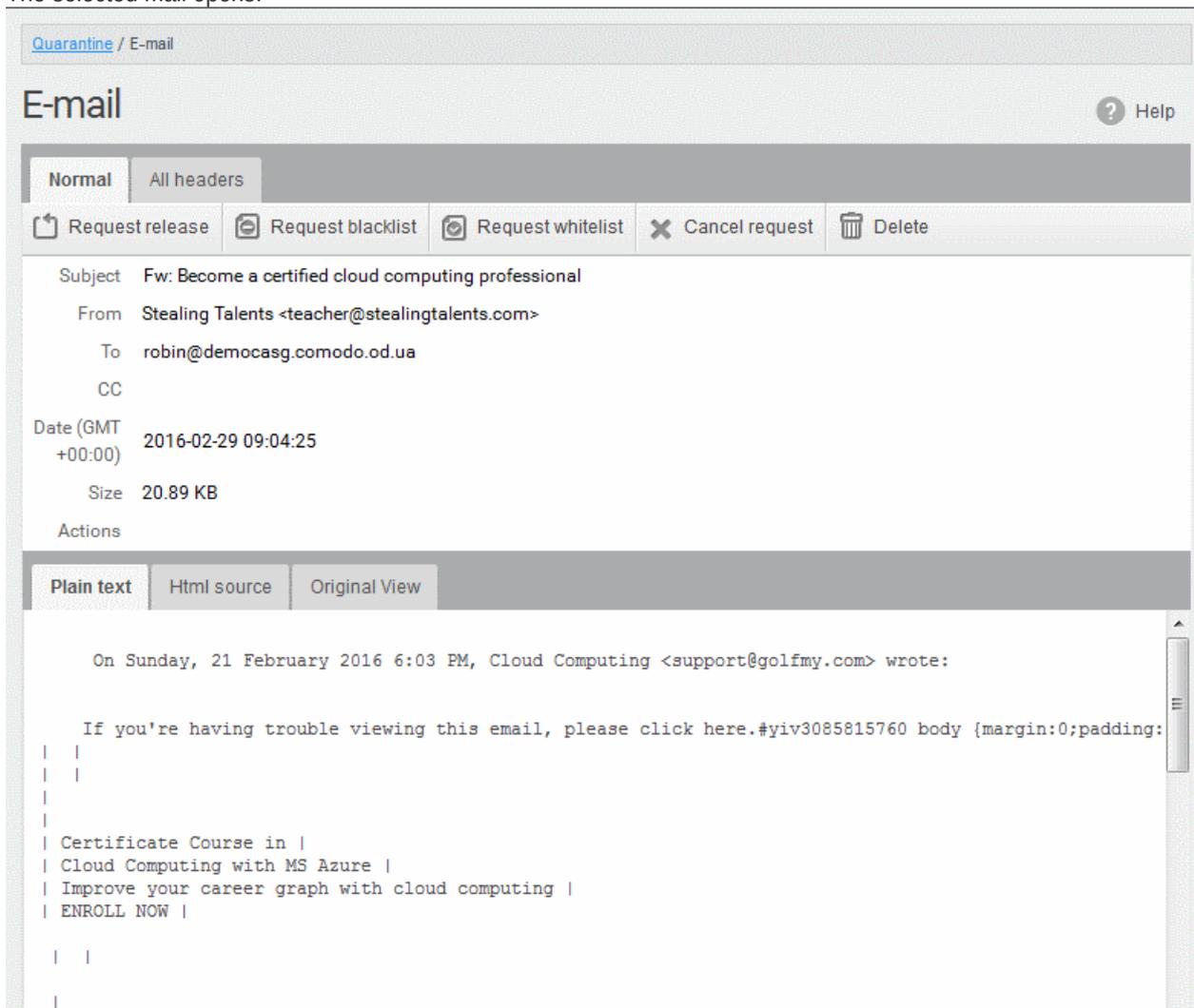
**Note:** The administrator of your email account should have enabled this feature for you. If this is enabled, the 'Show message' button will be available in the interface.

### View quarantined mails in the same CSEG window

- Select the mail that you want to view and click the 'Show Message' button.
- OR
- Click on the email link in the subject column that you want to view its details.

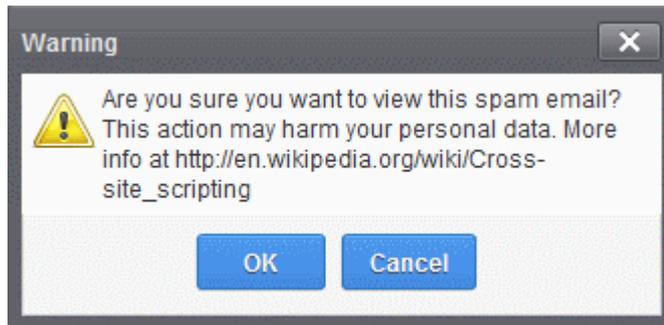


The selected mail opens:



By default, the email opens in plain text, so images, banners and links are not be displayed.

- Click 'Html source' to view the source code of the mail.
- Click the 'Original View' tab. to view the mail with images and links

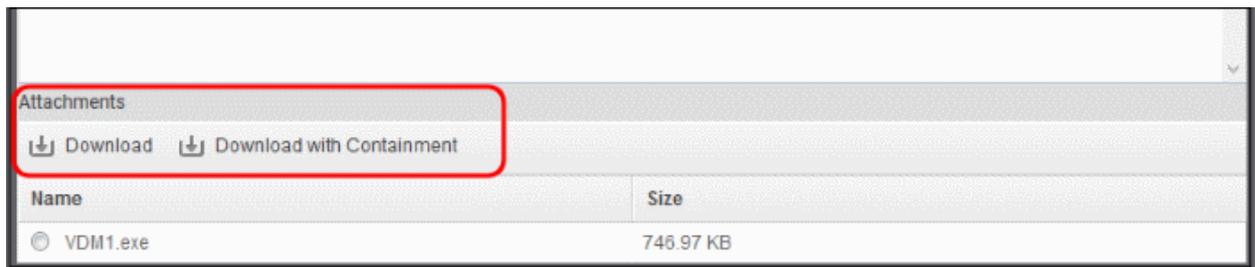


A warning is displayed before you view the selected email in original.

- Click 'OK' to view the email.

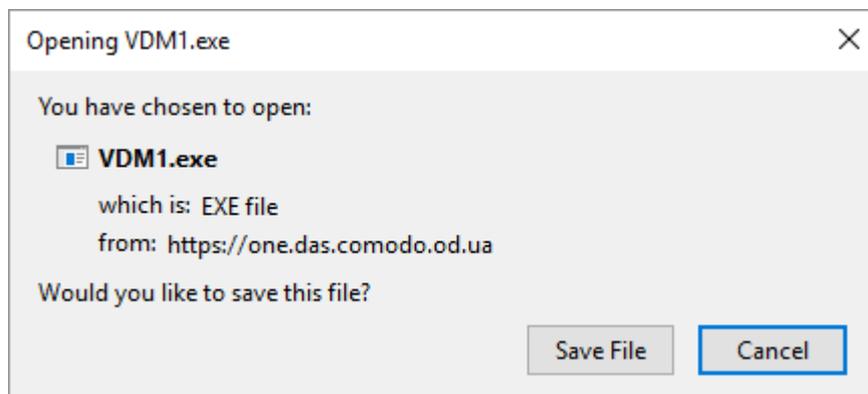
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **release** the email or to add the sender to **whitelist** or **blacklist**.

If there is an attachment, you can download it from this dialog.



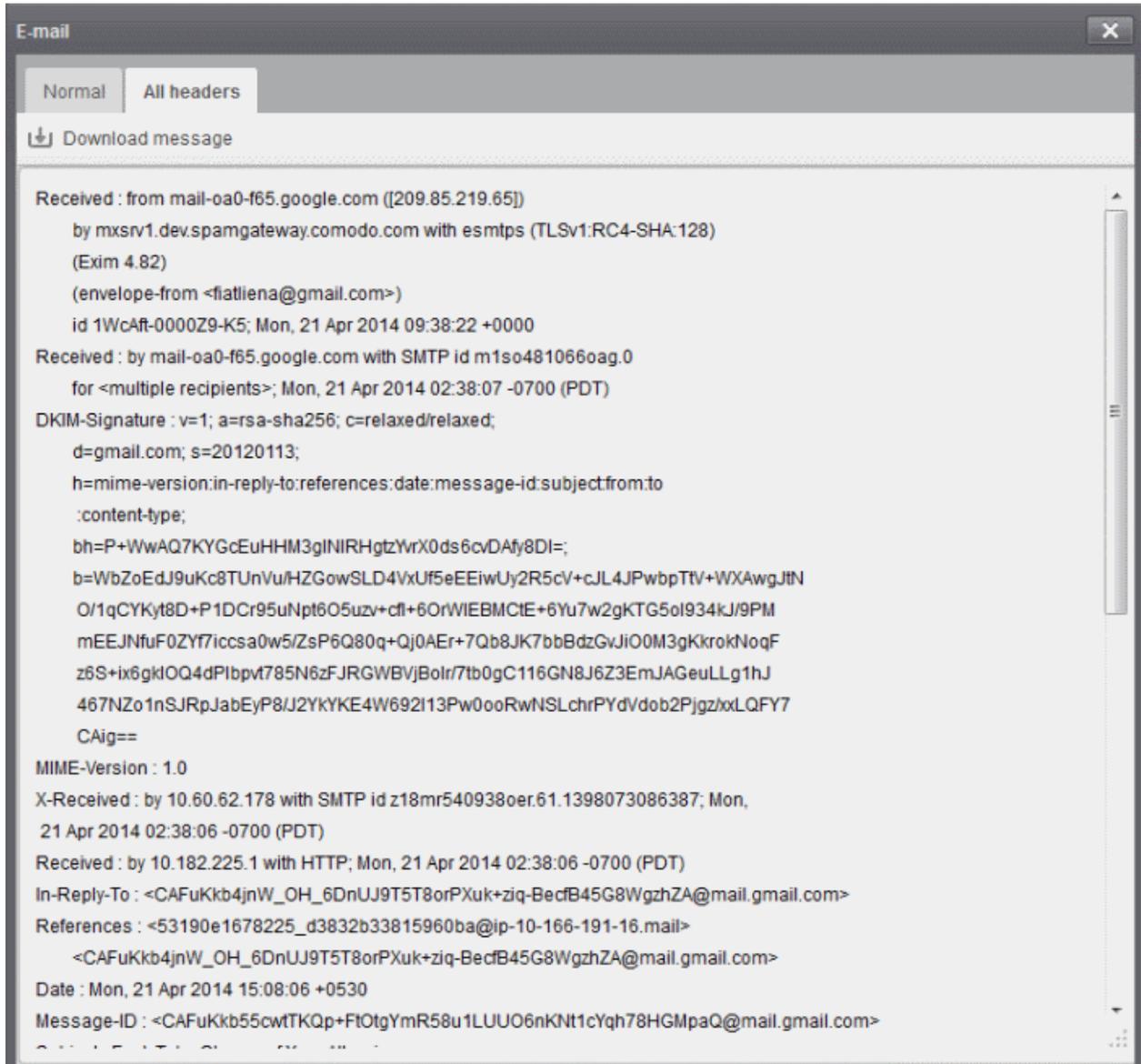
- Select the attachment and click 'Download' or 'Download with Containment'
  - **Download** – You can save the file / attachment as original.
  - **Download with Containment** – Containment is a technology whereby attachments with an 'unknown' trust rating are run inside a secure, sandbox environment. You can open and run the file as normal, but it is prevented from making potentially damaging changes to your computer.

'Download with containment' is only available if enabled by your administrator.



You can open the attachment with an appropriate application or save to a desired location in your computer.

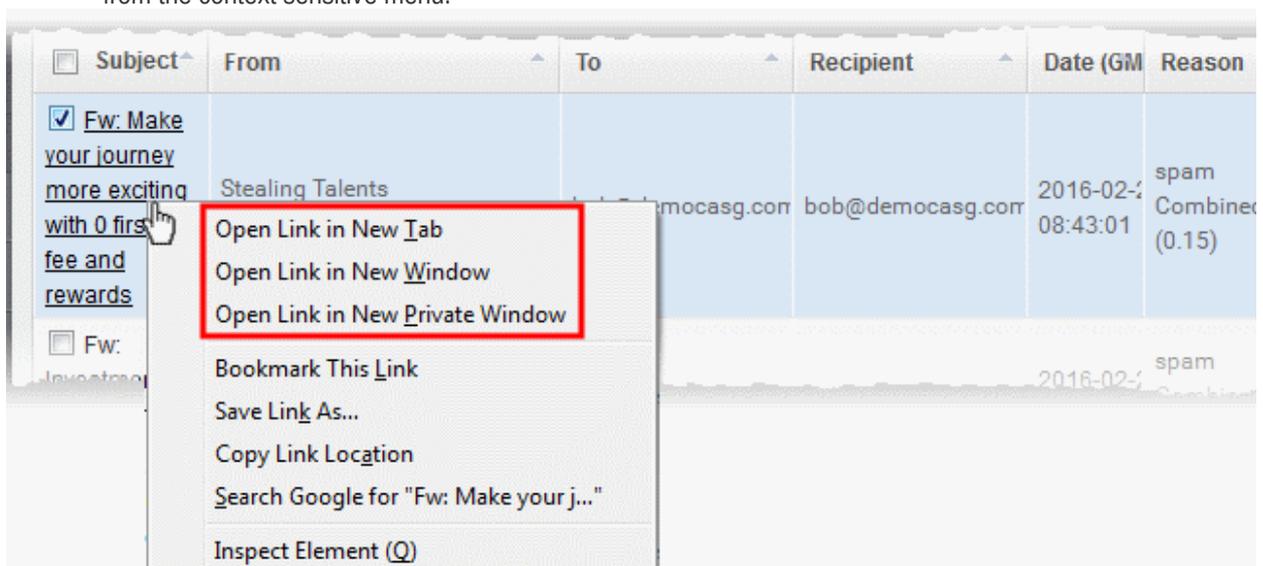
- **'All headers' tab** – Email headers contain information about the route taken by the mail before it reached your mailbox. This lets you check the authenticity of the mail:



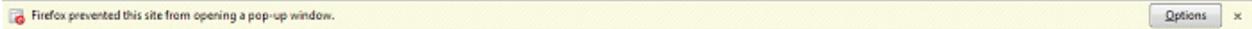
- To download the email as a HTML file, click 'Download' message.

### View a quarantined mail in a new window

- Right-click on the subject line of the mail you want to view and choose to open in a new tab or new window from the context sensitive menu.



Your browser may display a warning pop-up window notification. Click 'Options'> then select 'Allow pop-ups for...' to allow the message to open in a new window. Click 'Show message in new window' again.



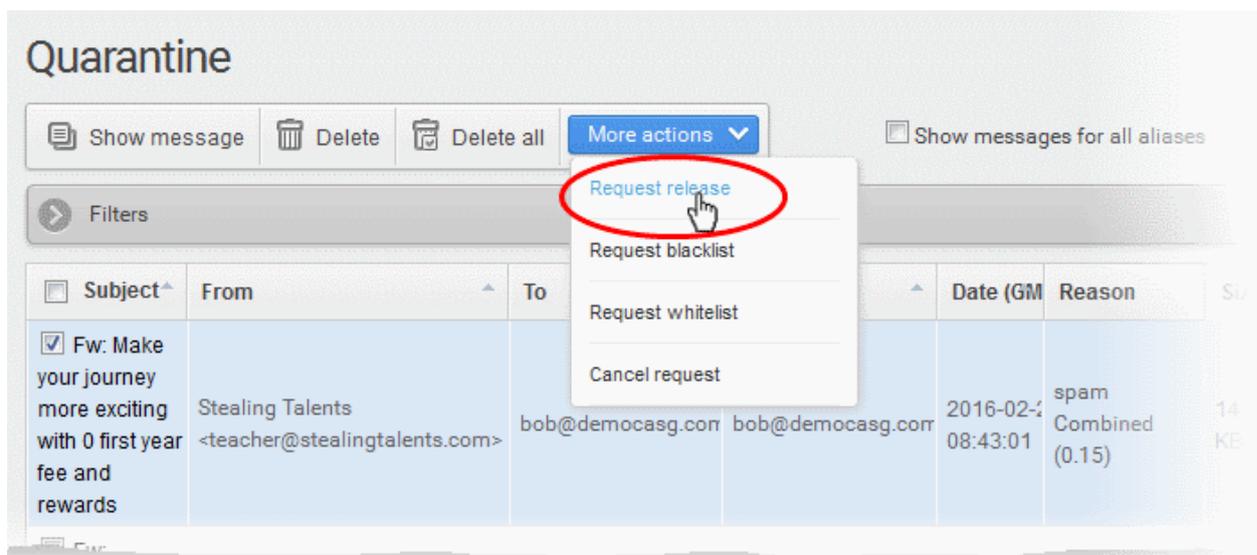
The details of the selected mail will be displayed in a new CSEG window

## Request administrator for releasing quarantined mails

After checking that the selected email is not spam, you can request your admin release the email.

**Note:** Depending on the permission level configured for your email account by your administrator, the button for releasing quarantined email will be either 'Release' or 'Request release' in the 'More actions' drop-down button. If the interface displays 'Release' button, you can release the selected email from the list without approval from your administrator.

- Select the mail that you want to release and click 'More actions' > 'Request Release'



An email notification is sent to your administrator for your request and you will also receive the request email. This request is also displayed in the 'Action' column of the users' Quarantined interface. If the administrator accepts the request, the user receives the email and if it is rejected, 'Release' icon in the action column is no longer displayed.

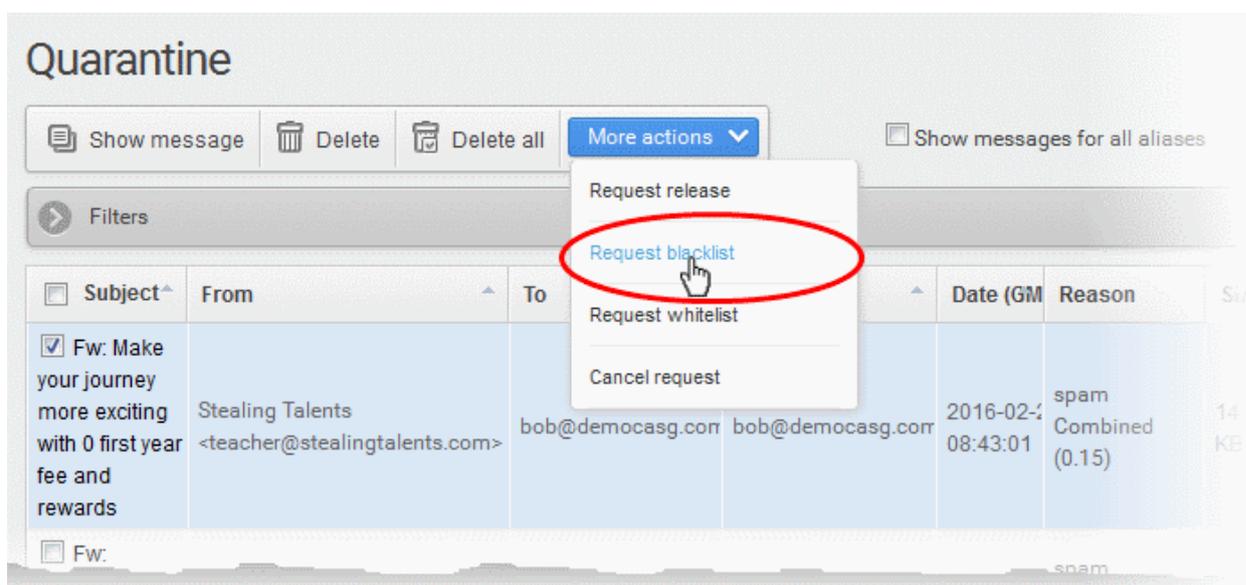
- Click 'More actions' then 'Cancel request' to cancel the request.

## Request administrator to add senders to blacklist

To avoid receiving spam emails, you can request the administrator to add the senders of these emails to blacklist.

**Note:** Depending on the permission level configured for your email account by your administrator, the button for adding senders to blacklist will be 'Blacklist this Sender' or 'Request blacklist' in the 'More actions' drop-down button. If the interface displays 'Blacklist this Sender' button, you can add the sender to blacklist without approval from your administrator.

- Select the mail whose sender you want to add to the blacklist and click 'More actions' > 'Request Blacklist'



A notification is sent to your administrator for your request and you will also receive the request email. This request is also displayed in the 'Action' column of the users' Quarantined interface.

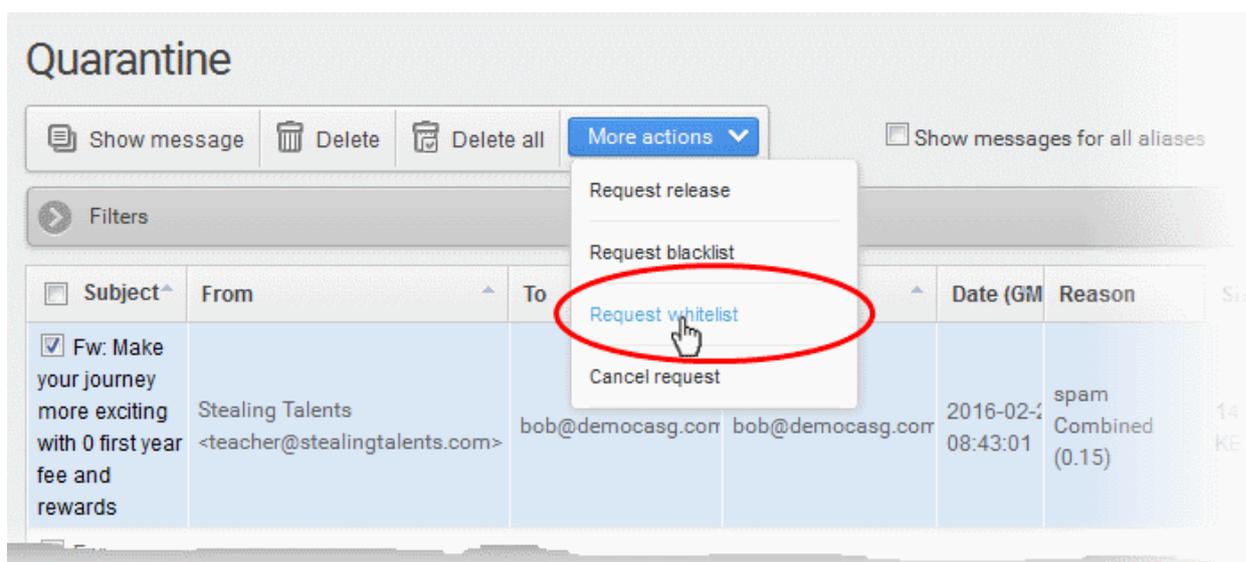
- If your administrator accepts the request, the sender is added to blacklist and you will no longer receive any mail from that sender.
- If the request is rejected, the 'Blacklist this Sender' icon in the 'Action' column will no longer be displayed.
- Senders added to blacklist are displayed in the 'Manage blacklist senders' interface. See **Managing Blacklisted Senders** for more details.
- To cancel the request before the administrator accept the request, choose the mail > click 'More actions' then 'Cancel request'.

### Request administrator to add senders to whitelist

If mail from a sender that you trust gets quarantined, you can request your administrator to add the sender to the whitelist.

**Note:** Depending on permissions set by your administrator, the link in the 'More Actions' drop-down will either be 'Whitelist this Sender' or 'Request whitelist'. If the interface displays 'Whitelist this Sender' button, you can add the sender to whitelist without approval from your administrator.

- Select the mail that you want its sender to be added to whitelist and click 'More actions' > 'Request Whitelist'



Your request is sent to your administrator. You also will also receive the request email.

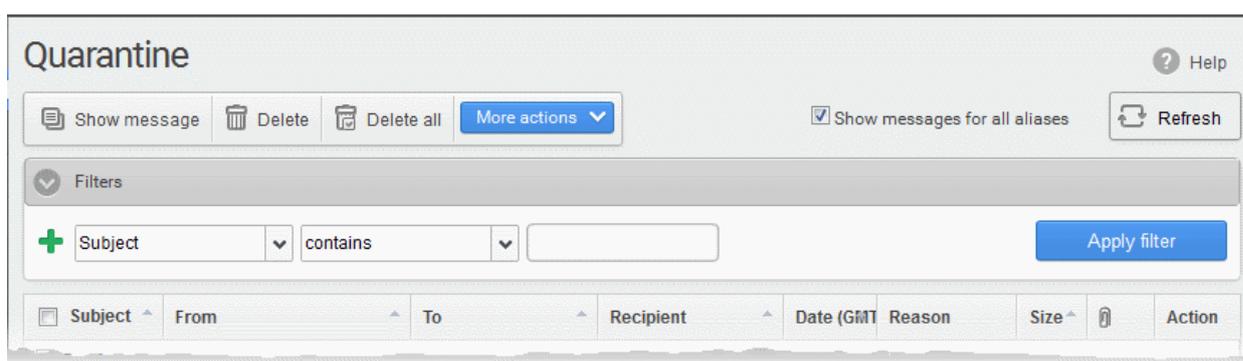
This request is also shown in the 'Action' column of the users' 'Quarantined' interface.

- If the administrator accepts the request, the sender is added to whitelist and the mails from them are no longer quarantined.
- If the request is rejected, 'Whitelist this Sender' icon in the action column is no longer displayed.
- Click 'More actions' then 'Cancel request' to cancel the request.

## 2.4 How to Use Filter Options in the Quarantined Emails Interface

You can use the filtering option in the quarantine interface to optimize your search.

- Click anywhere on the 'Filters' stripe to open (or close) the filters area.



- Choose the filter by which you want to search from the first drop-down, then a condition in the 2nd text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the mail subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Reason:** Enter the quarantined reason in the text box (column 3) and select a condition 2.
- **Recipient:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

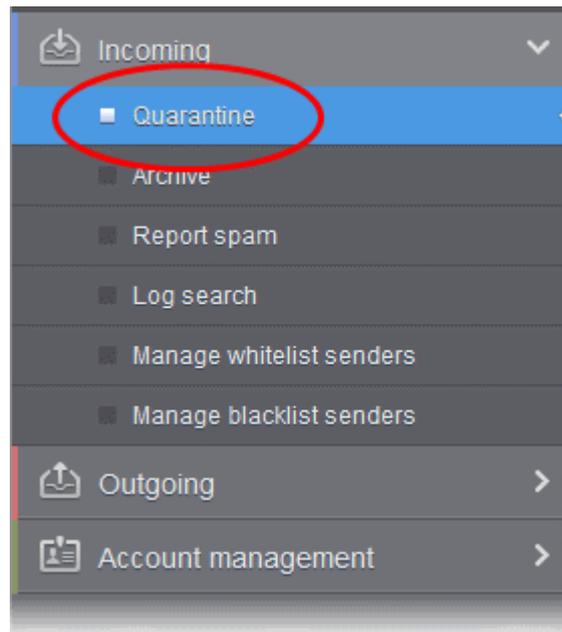
## 2.5 How to Check when an Expected Email is not Received

You are expecting an important email, but it is not in your inbox. The CSEG filtering engine would have most probably classified it as spam and quarantined. Search for it in the 'email quarantined' area.

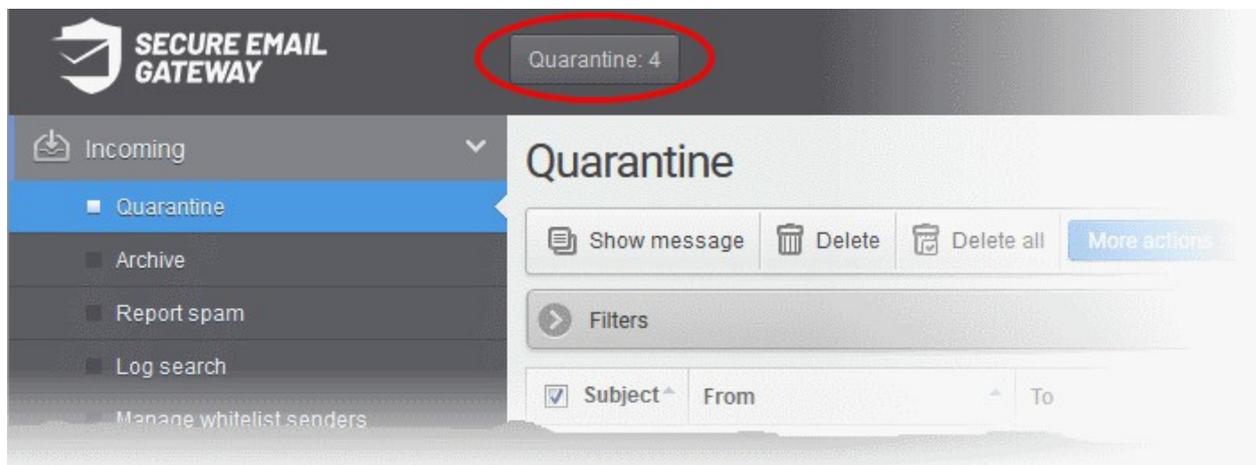
### Search for a particular email in the quarantine interface

- **Login** to the CSEG interface.

- Click 'Incoming' on the left then choose 'Quarantine'



- Alternatively, click the 'Quarantine' button at the top.



All your quarantined emails are listed with their details.

## Quarantine ? Help

Show message
Delete
Delete all
More actions ▾

Show messages for all aliases
 Refresh

Filters

Subject	From	To	Recipient	Date (GMT)	Reason	Size	🗑️	Action
<input type="checkbox"/> Fw: Become a certified cloud computing professional	Stealing Talent <teacher@stealingtalent.com>	robin@democasg.com	robin@democasg.com	2016-02-2 09:04:25	spam Combined (0.15)	20.89 KB	🗑️	
<input type="checkbox"/> Fw: Make your journey more exciting with 0 first year fee and rewards	Bullock Travels <marketing@yaktouring.org>	bob@democasg.com	bob@democasg.com	2016-02-2 08:43:01	spam Combined (0.15)	14.42 KB	🗑️	
<input type="checkbox"/> Fw: Investment with lasting returns	Money Swindlers <campaign@mswindlers.org>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:47	spam Combined (0.14)	5.91 KB	🗑️	
<input checked="" type="checkbox"/> Fw: Get upto 90% off on household items.	Brokenpot Sellers <offers@brokenpotsellers.co.uk>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:03	spam Combined (0.19)	6.1 KB	🗑️	

⏪ ⏩
1 / 1
▶ ▶
[ 1 - 4 / 4 ]

Per page 15

- More Actions** - Request that the mail is released from quarantine, or that the sender is added to the blacklist or whitelist.
- Show messages for all aliases** - By default, the list only shows mails sent to your primary email address. Select this option to view messages sent to all your mailboxes.
- Click 'Filters' to search for particular email. See ['How to use filters'](#) for more on this.
- [Click here](#) to know how to manage your quarantined mails.

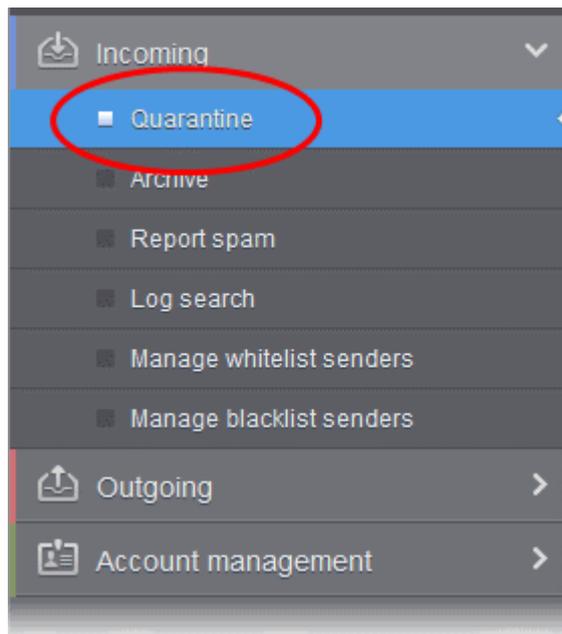
**Tip:** You can configure CSEG to send Quarantine summary reports periodically to your email. The report contains a list of mails identified as spam and moved to Quarantine automatically by CSEG. See [How to Subscribe for Periodical Quarantine Report Summary](#).

## 2.6 How to Retrieve an Email which had a Virus Attachment

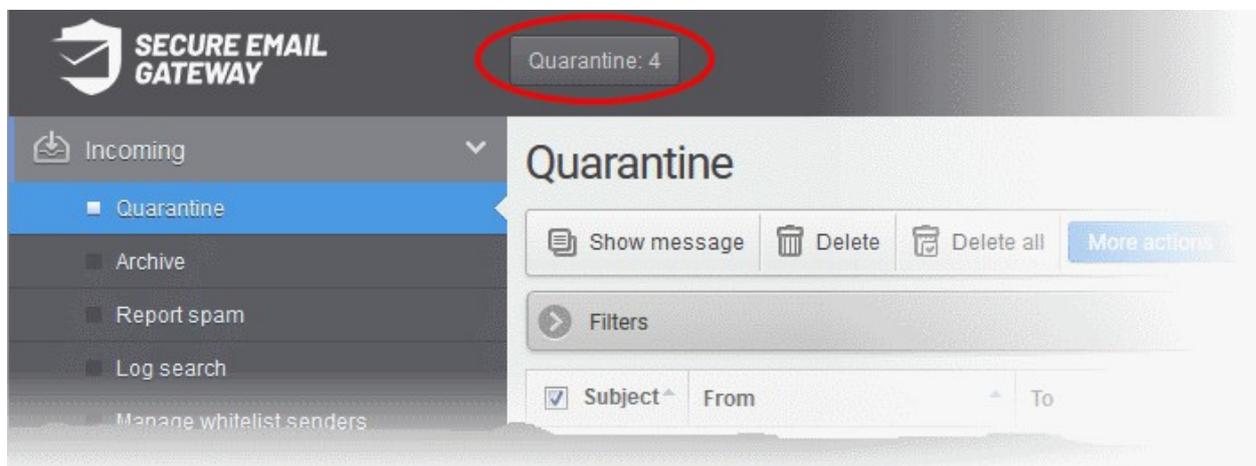
- CSEG quarantines any email that contains malicious links or attachments
- You will receive a notification whenever a mail addressed to you is quarantined.
- You can retrieve these message as follows:

### Retrieve quarantined mails

- **Login** to the CSEG interface.
- Click the 'Incoming' tab from the left and choose 'Quarantine'



- Alternatively, click the 'Quarantine' button at the top.



All your quarantined mails are listed in the interface:

**Quarantine** ? Help

Show messages for all aliases

Filters

<input type="checkbox"/>	Subject ^	From ^	To ^	Recipient ^	Date (GMT)	Reason	Size ^		Action
<input type="checkbox"/>	Fw: Become a certified cloud computing professional	Stealing Talent <teacher@stealingtalent.com>	robin@democasg.com	robin@democasg.com	2016-02-2 09:04:25	spam Combined (0.15)	20.89 KB		
<input type="checkbox"/>	Fw: Make your journey more exciting with 0 first year fee and rewards	Bullock Travels <marketing@yaktouring.org>	bob@democasg.com	bob@democasg.com	2016-02-2 08:43:01	spam Combined (0.15)	14.42 KB		
<input type="checkbox"/>	Fw: Investment with lasting returns	Money Swindlers <campaign@mswindlers.org>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:47	spam Combined (0.14)	5.91 KB		
<input checked="" type="checkbox"/>	Fw: Get upto 90% off on household items.	Brokenpot Sellers <offers@brokenpotsellers.co.uk>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:03	spam Combined (0.19)	6.1 KB		

1 / 1
[ 1 - 4 / 4 ]
Per page 15

- **More Actions** - Request that the mail is released from quarantine, or that the sender is added to the blacklist or whitelist.
- **Show messages for all aliases** - By default, the list only shows mails sent to your primary email address. Select this option to view messages sent to all your mailboxes.

## Read the Email

- After identifying the email with attachment that you suspect to be virus, select it and click the 'Show Message' button or click the email link in the 'Subject' column to view its details. To open the mail in a new CSEG window or tab, right-click the email link in the 'Subject' column and select from the context sensitive menu options.

**Note:** The administrator of your email account should have enabled this feature for you. If this is enabled, the 'Show message' button will be available in the interface.

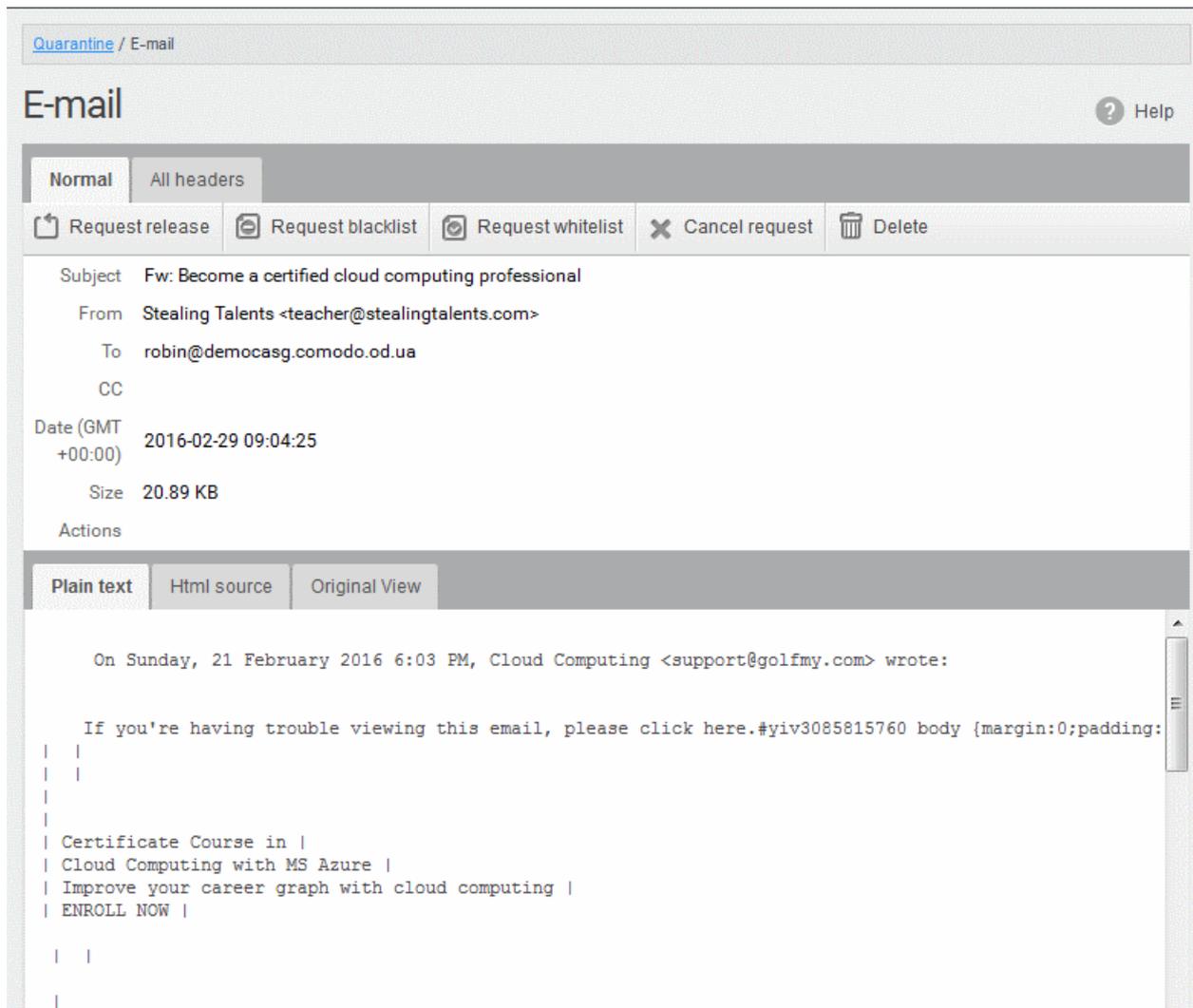
**Quarantine** ? Help

Show messages for all aliases

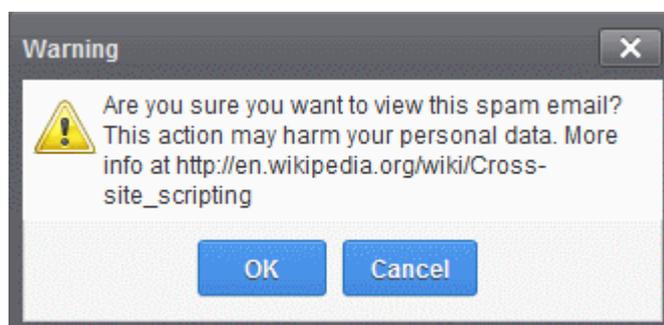
Filters

<input type="checkbox"/>	Subject ^	From ^	To ^	Recipient ^	Date (GMT)	Reason	Size ^		Action
<input checked="" type="checkbox"/>	Fw: Become a certified cloud computing professional	Stealing Talents <teacher@stealingtalents.com>	robin@democasg.com	robin@democasg.com	2016-02-2 09:04:25	spam Combined (0.15)	20.89 KB		
<input type="checkbox"/>	Fw: Make your journey								

This opens selected email:



By default, the email opens in normal view and is displayed in plain text, where the images, banners and links are not displayed. Click 'Html source' to view the source code of the mail. To view images and links, click the 'Original View' tab. A warning is displayed before you want to view the selected email in original.

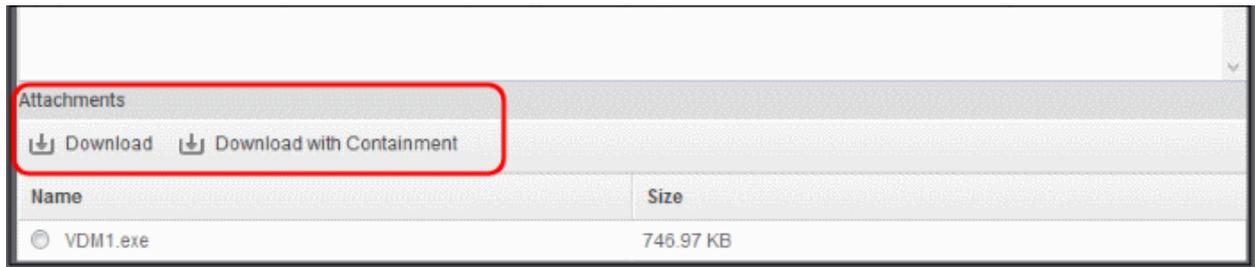


- Click 'OK' to view the email.

Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either release the email or to add the sender to **whitelist** or **blacklist**.

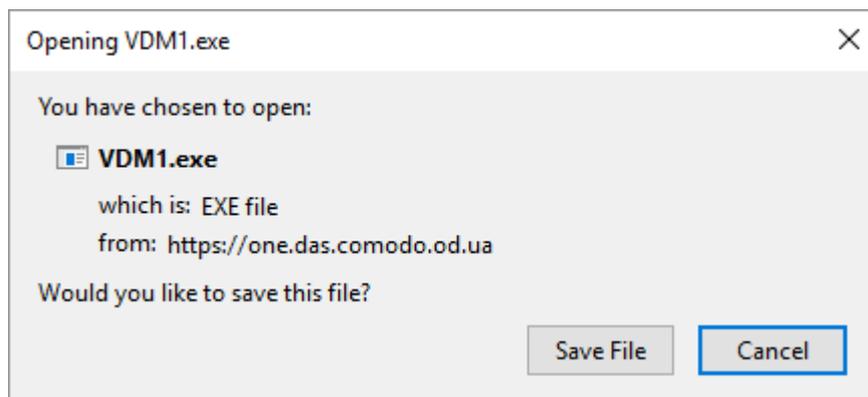
**Note:** Depending on the permission level configured for your email account by your administrator, the buttons in the 'E-mail' may vary. The 'Request release', 'Request blacklist' and 'Request whitelist' buttons may appear as 'Release', 'Blacklist this sender' and 'Whitelist this sender' buttons respectively enabling you to perform the desired action without approval from the administrator.

- Select the attachment and click 'Download' or 'Download with Containment'



- **Download** – You can save the file / attachment as original.
- **Download with Containment** – Containment is a technology whereby attachments with an 'unknown' trust rating are run inside a secure, sandbox environment. You can open and run the file as normal, but it is prevented from making potentially damaging changes to your computer.

'Download with containment' is only available if enabled by your administrator.



You can open the attachment with an appropriate application or save to a desired location in your computer.

The selected email is delivered to your inbox only when the administrator has accepted your request for releasing it.

**Note:** Antivirus application in your computer may prevent an attachment that contains virus from downloading. To download the attachment, disable the antivirus option in your computer.

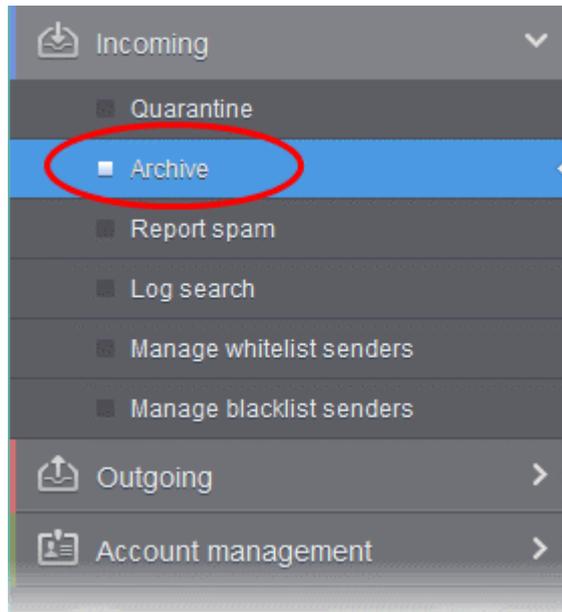
## 2.7 How to Restore Deleted Mails

CSEG keeps a copy of your emails in the archive.

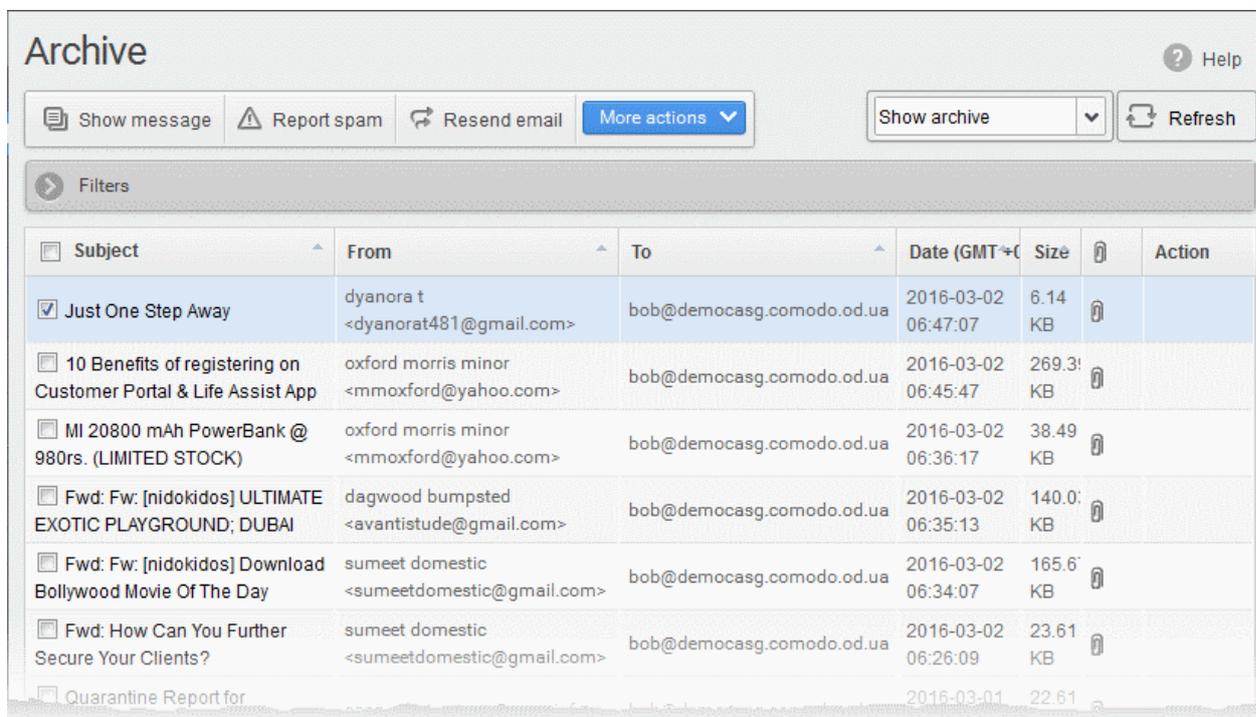
- The period for which mails are retained in the archive depends on the retention period configured by your administrator.
- The 'Archive' interface allows you to view the list of emails received at your email address.
- You can view stored messages, reply to mails, report spam, and resend mail to yourself from this interface.

### Retrieve a deleted mail

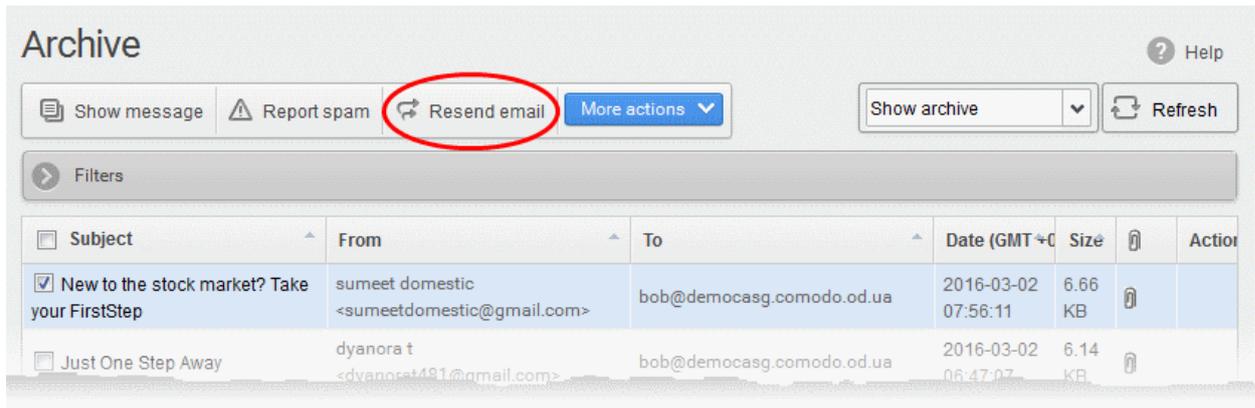
- **Login** to the CSEG interface.
- Click 'Incoming' on the left then choose 'Archive'



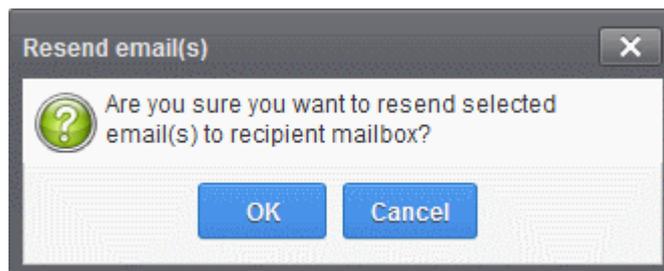
Your stored mails are listed in the interface:



- Locate the mail you wish to restore and click 'Resend Mail'. This sends the mail to your mailbox only, and not to any other recipients in the 'To', 'CC' and 'BCC' fields.



A confirmation dialog is shown:



- Click 'OK' to receive the mail(s) at your mail box

You can search for specific mails by clicking the 'Filters' bar. You can search by subject line, sender, date received or file size.

If you would like to know more about the mail archive area, see [Mail Archive](#).

## 2.8 How to Reply to Archive Mails

CSEG allows you to reply to archived mails. This is useful if you have accidentally deleted a mail from your mail box but wish to send a reply to the sender. You can choose to send the reply only to the sender or to all for which the email was addressed.

### Send a reply to a mail from archive

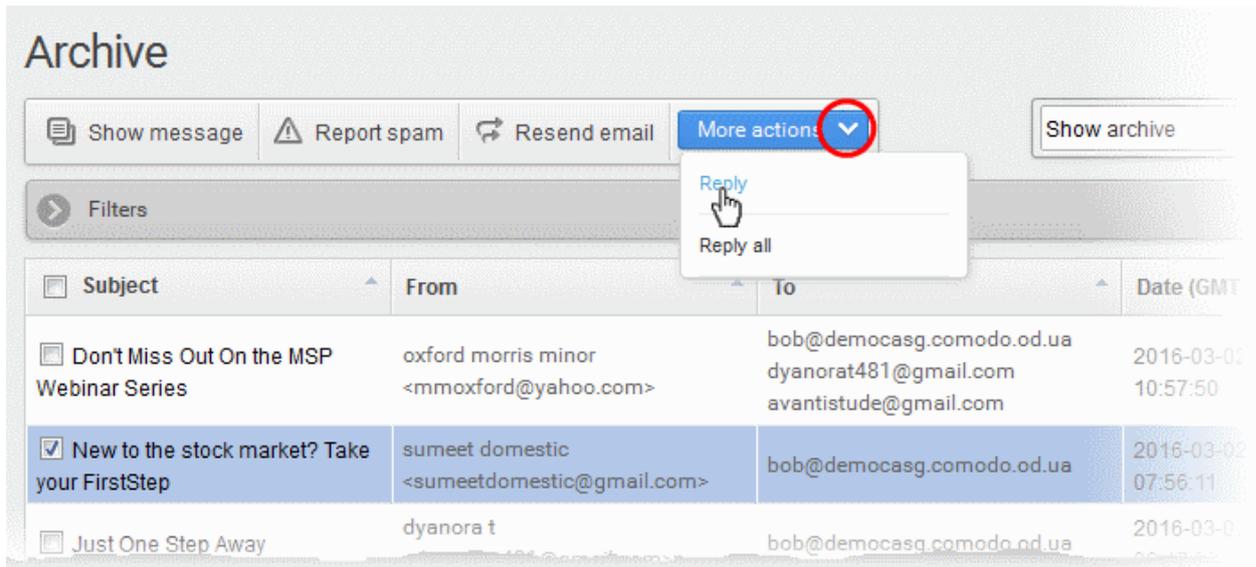
- **Login** to CSEG
- Click 'Incoming' on the left then choose 'Archive'

The 'Archive' interface opens with the list of your emails.

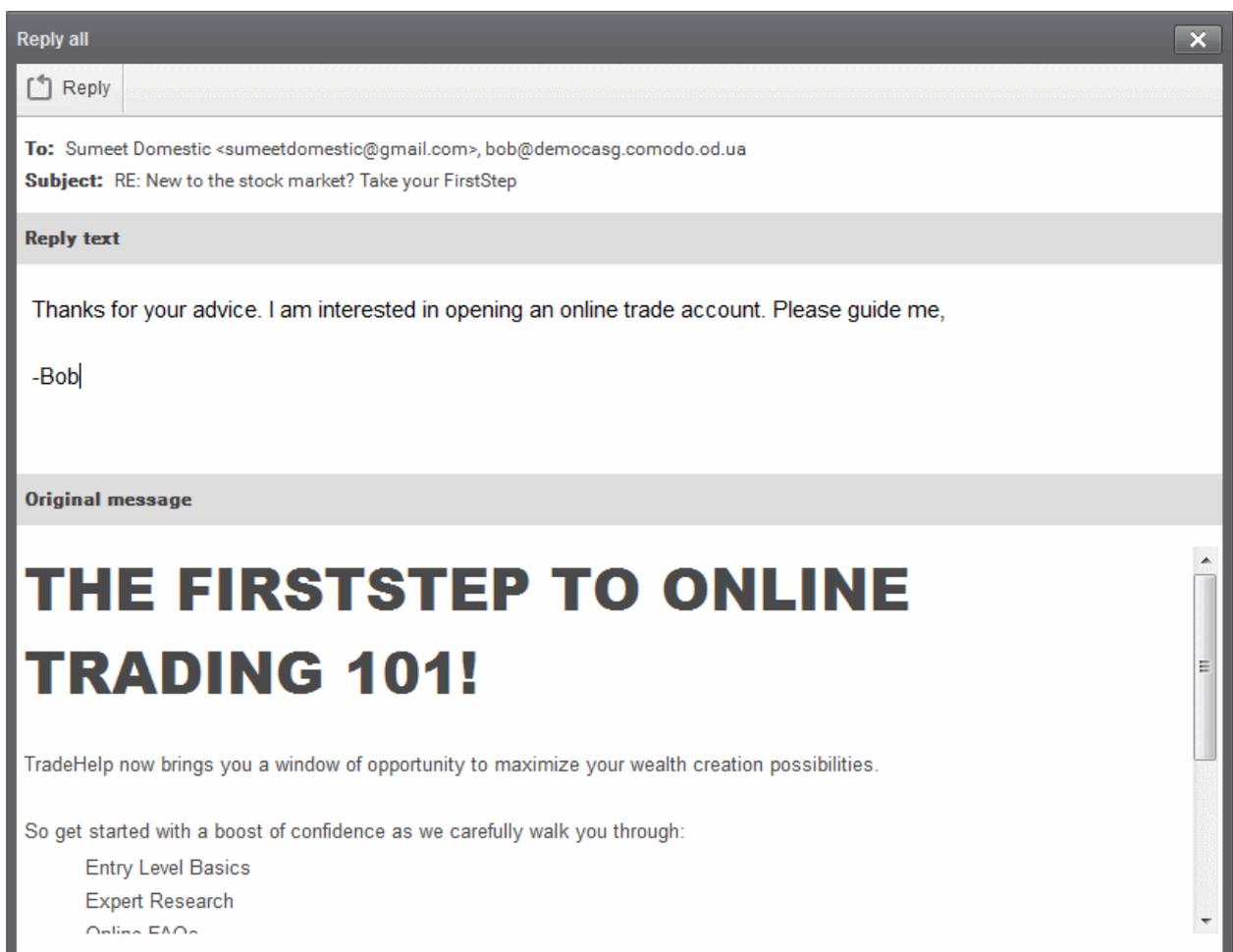
- Select the mail from the Archive interface

You can use sorting and search options to search for specific mails.

- Click 'More actions' and choose the option
  - Reply - The reply mail is sent only to the sender email address
  - Reply all - The reply mail is sent to all email addresses in the 'To' and 'CC' fields of the selected mail



The Reply/Reply all interface opens.



- Enter your reply message in the 'Reply text' field and click Reply from the top left

The message will be sent to the selected email addresses.



## 2.9 How to Subscribe for Quarantine Reports

Comodo Secure Email Gateway MSP can periodically generate quarantine reports. These reports contain the details of emails addressed to you but moved to quarantine.

- Subscribe for these reports in the 'Manage report subscriptions' interface so these are sent to you periodically

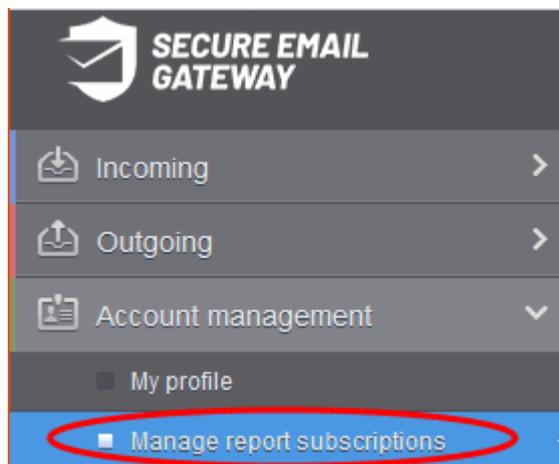
**Note:** The report subscription feature is available for you only if the administrator has enabled this feature. If enabled, the 'Manage report subscriptions' sub tab is available on the left under the 'Account management' tab.

The quarantine report contains a statistical breakdown of the mails that were identified as spam or containing malicious content and were moved to quarantine automatically by CSEG, with the details of sender, receiver, date and attachments. Clicking the subject line in the list will open the respective mail in a new CSEG window. See **CSEG Reports** for more details.

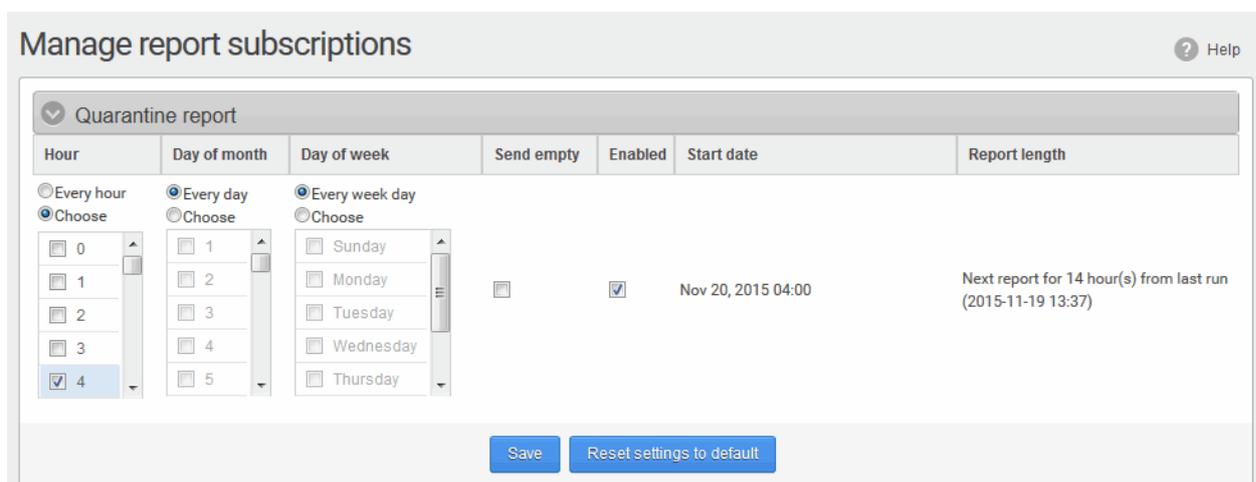
You can subscribe to receive the reports daily, weekly or monthly.

### Configure report subscription

- **Login** to CSEG
- Click 'Account management' on the left then select 'Manage report subscriptions'.



The 'Manage report subscriptions' interface opens:



- If you want to receive the periodical quarantine summary reports, ensure that the 'Enabled' check box is selected.

- Leave the 'Send empty' checkbox unchecked if you do not want to receive empty reports.
- Select the frequency of the report to be sent to you from the 'Hour', 'Day of month' or 'Day of week' columns.
  - **Hour** - The reports are generated and sent at the selected hour of the day or date chosen from 'Day of month' or 'Day of week' columns.
  - **Day of month** - The reports are generated and sent every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
  - **Day of week** - The reports are generated and sent every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
  - **Start date** - Shows the begin date of the report generation depending on the options chosen.
  - **Report length** - Shows the period of the report that are generated depending on the options chosen.
- Click 'Save' for your settings to take effect.
- Click 'Reset settings to default' button to configure default report generation period. The reports are generated every 24 hours starting from last report generated time or from 00:00 hours.

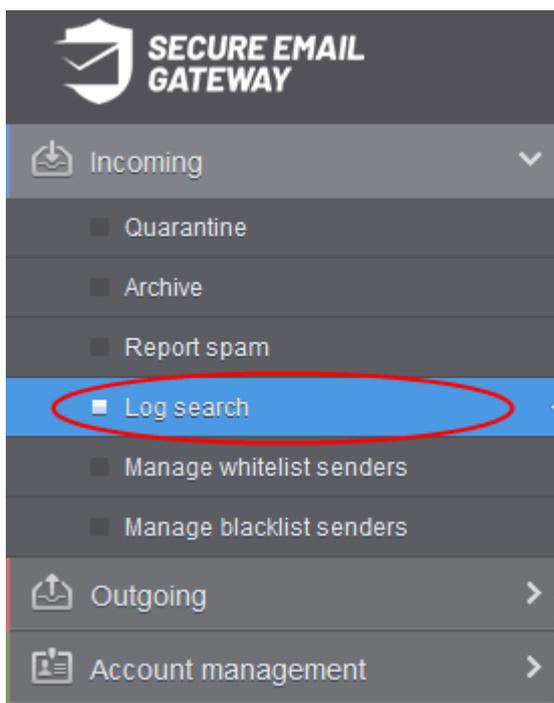
## 2.10 How to Perform a Log Search of your Incoming Emails

The 'Log search' area lets you search for specific email messages. You can modify your search according to multiple criteria, including date range, sender, recipient and IP address.

**Note:** The administrator of your email account should have enabled this feature for you. If enabled, the 'Log search' is available on the left under 'Incoming'.

### Search your incoming emails in logs

- **Login** to the CSEG interface.
- Click 'Incoming' on the left then click the 'Log search'.



The 'Log search (incoming)' interface opens:

## Log search (incoming) ? Help

Date range:  -

Message ID:

Sender:

Recipient:  @demo.das.comodo.od.ua

Sender IP:

Sender host:

Include results from the last minutes:

[Search](#)

- **Date range:** The date range for which you want to search the log file.
- **Message ID:** A unique message identifier (*optional*).
- **Sender:** The sender email address in this field.
- **Recipient:** The currently logged in user name is displayed in this field.
- **Sender IP:** The IP address of the sender.
- **Sender Host:** The sender host name.
- **Include results from the last minutes:** If selected, CSEG includes messages that are currently being migrated from the filtering server to the logging server in the search results.

The option "Include results from the last minutes" will slow down the search result retrieval ✕

- Click the 'Search' button.

CSEG searches for the entered terms and shows the results.

Date and time <sup>^</sup>	Host (Exim id) <sup>^</sup>	Sender host <sup>na</sup>	Sender <sup>^</sup>	Recipient <sup>^</sup>	Subject <sup>^</sup>	Classification <sup>^</sup>
2014-10-29 14:53:43	mxsrv3.spamgat 1XjUd0-0006V6-\	mxsrv3.spamgat 178.33.199.69	admin@csg.com	john	demo spam email 1	Rejected External pattern match
2014-10-29 14:45:07	mxsrv2.spamgat 1XjUUF- 0001RZ-B8	mxsrv2.spamgat 178.33.199.66	demo@csg.com	john	Spam email 1	Rejected Rejected by relay restriction for this recipient
2014-10-29 14:44:59	mxsrv1.spamgat 1XjUUX- 0006NV-Bj	mxsrv2.spamgat 178.33.199.66	demo@csg.com	john	Spam email 2	Rejected Rejected by relay restriction for this recipient

⏪ ⏩ |  / 1 | ⏪ ⏩ | [ 1 - 3 / 3 ] Per page  ▼

- Click any column header to sort the entries based on the ascending/descending order

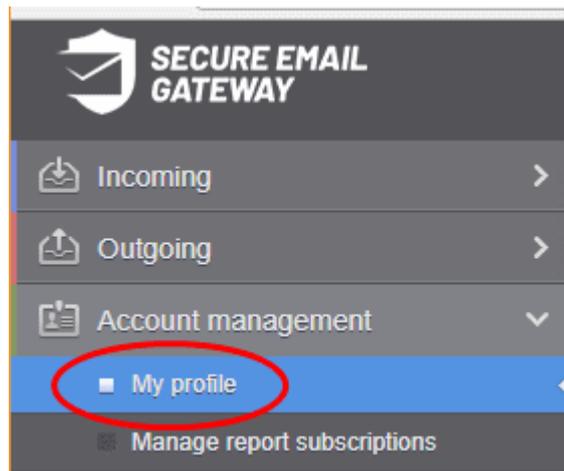
## 2.11 How to Add or Remove yourself from Recipient Whitelist

All filtering checks in CSEG are disabled for whitelisted recipients. You have the option to add or remove yourself from the recipient whitelist.

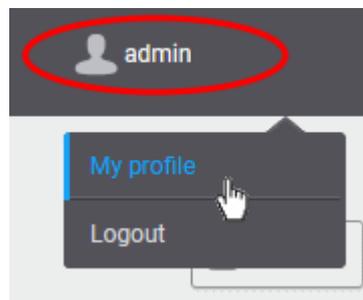
**Note:** The administrator of your email account should have enabled this feature for you. The 'Change settings' section will only be available in the 'My profile' interface if the feature is enabled.

### Add or remove yourself from recipient whitelist

- **Login** to CSEG.
- Click 'Account management' on the left then select 'My profile'.



Alternatively, click your username at top-right then select 'My Profile'.



The 'My Profile' interface opens.

The screenshot shows the 'My profile' page with two main sections: 'Change password' and 'Change settings'. The 'Change password' section has two input fields for 'New password' and 'Confirm password', and a 'Save' button. The 'Change settings' section has several options: 'Whitelist my email' (checkbox), 'Enable quarantine alert' (dropdown menu with 'Use domain settings (Enabl' selected), 'Enable Containment' (dropdown menu with 'Enable' selected), 'Stay signed in' (checkbox), 'Non human' (checkbox), and 'Public email' (checkbox). There is also a 'Save' button at the bottom of the settings section.

- In the 'Change settings' section, select or deselect the 'Whitelist my email' checkbox to add or remove yourself from the recipient whitelist.
- Click 'Save' to confirm your changes.

## 2.12 How to Report Spam Emails

You can upload and submit suspected junk emails that have got through our spam filters. Comodo will analyze reported mails and, if we confirm them as spam, will update our filters to quarantine similar mails in future.

You can report spam emails in two ways:

- **Submit mails from your mail archive**
- **Manually upload emails in .eml and .msg.files**

Users can also report spam by sending it to [spam@antispamgateway.comodo.com](mailto:spam@antispamgateway.comodo.com). Add the spam email as an attachment in .eml or .msg format.

### Submit mails from your mail archive

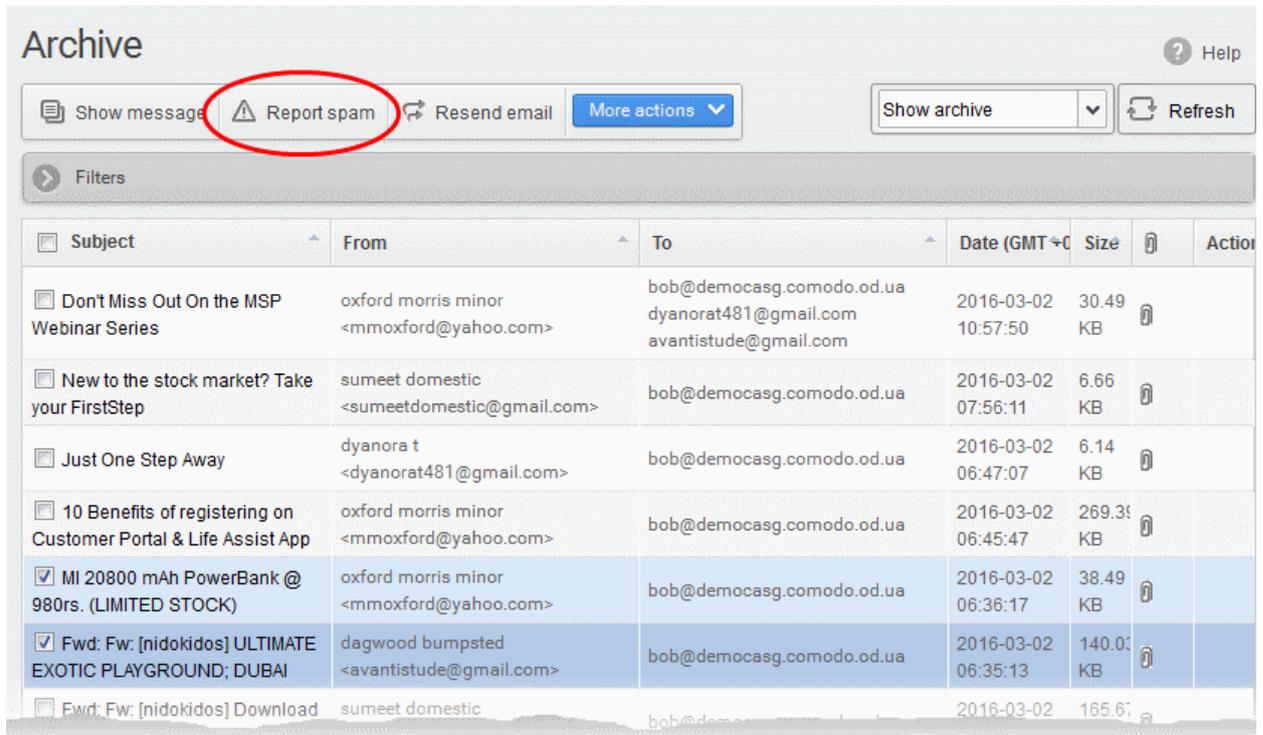
- **Login** to CSEG.
- Click 'Incoming' on the left then choose 'Archive'

The 'Archive' interface will open with the list of your emails.

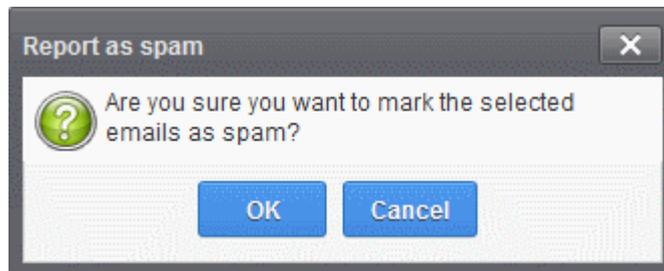
- Select the mail from the 'Archive' interface

You can use sorting and search options to search for specific mails.

- Click the 'Report Spam' button from the top



A confirmation dialog is shown:

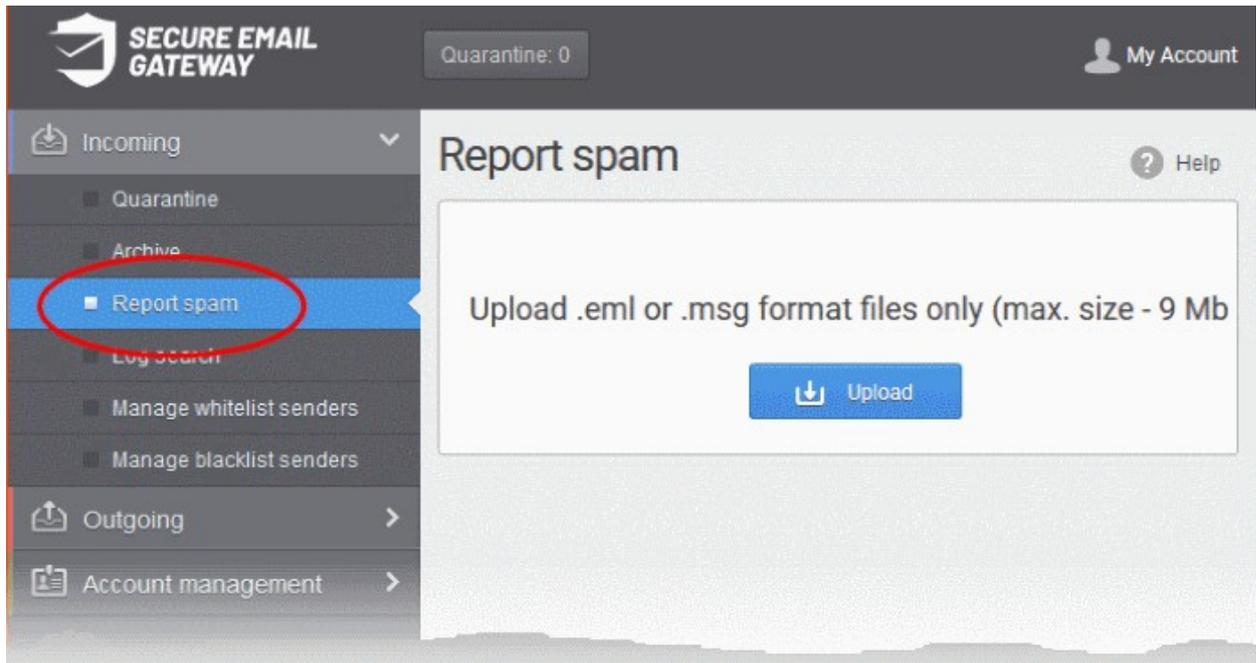


- Click 'OK' to upload the mails for analysis

### Manually upload an email

- **Login** to CSEG.
- Click 'Incoming' on the left then select 'Report spam'.

**Note:** The administrator of your email account should have enabled this feature for you. If enabled, the 'Report spam' sub tab will be available on the left under the 'Incoming' tab.

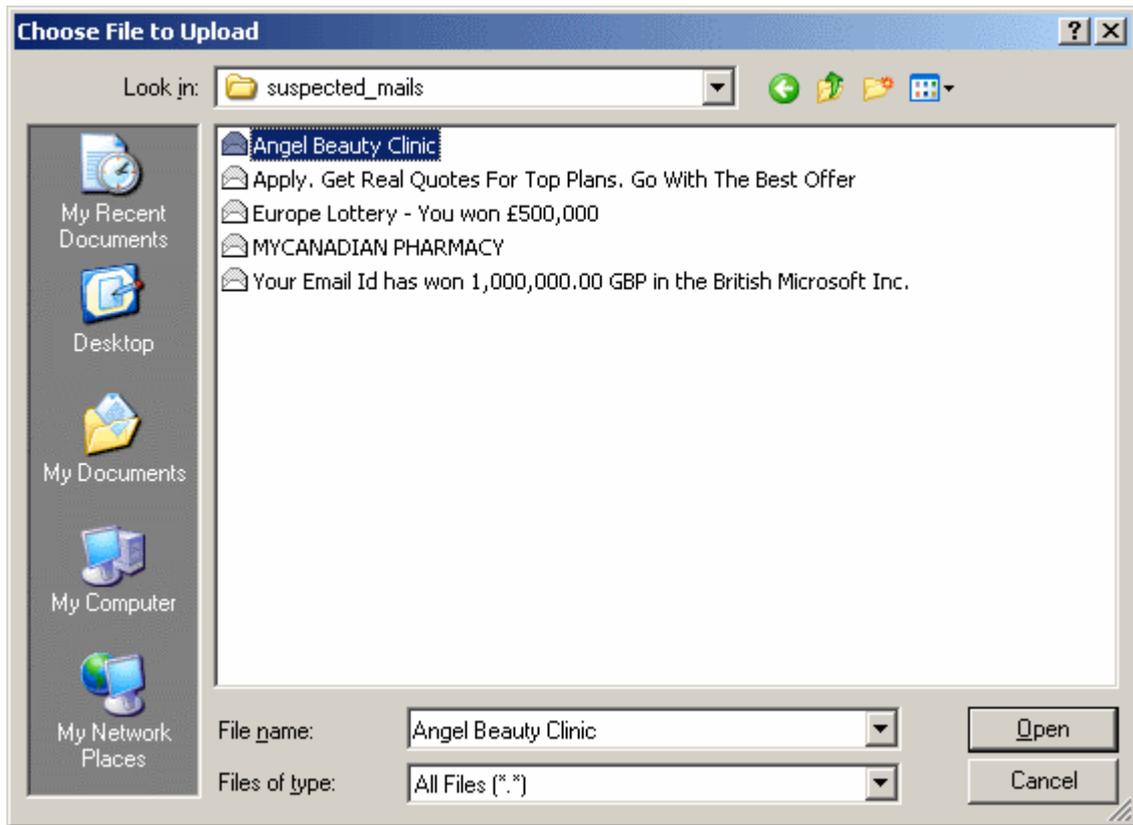


The 'Report Spam' interface will open.

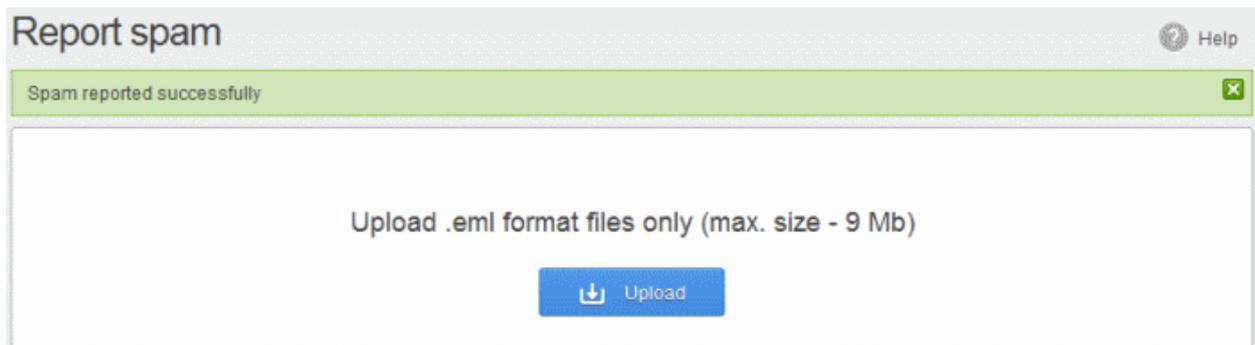
- Click the 'Upload' button.
- Navigate to the location where the suspected email(s) is/are stored in your system. Select the mail that you want to report as spam and click 'Open'. The maximum size of the file that can be uploaded is 9 MB.

**Note:** The files should be email format (with .eml extension) and its size should not exceed 9 MB. The following error message will be displayed if any of the above is not complied with.

Perhaps the body of the file is damaged or it is not \*.eml format or it size greater than 9Mb (outgoing\_users.csv) ✕



- The mail is processed for uploading and success message displayed after the process is completed.



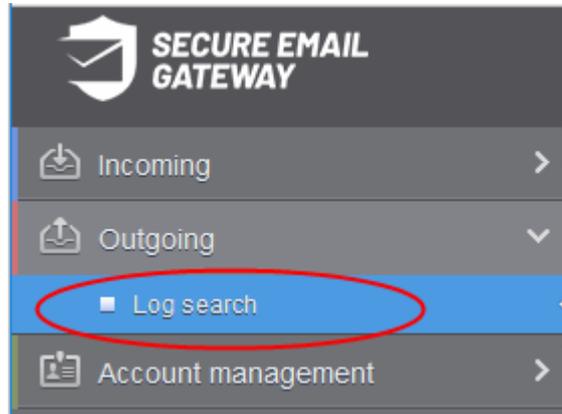
## 2.13 How to Perform a Log Search of your Outgoing Emails

The 'Log search' area lets you search sent emails based on filters such as date range, recipient email address, sender IP and classification.

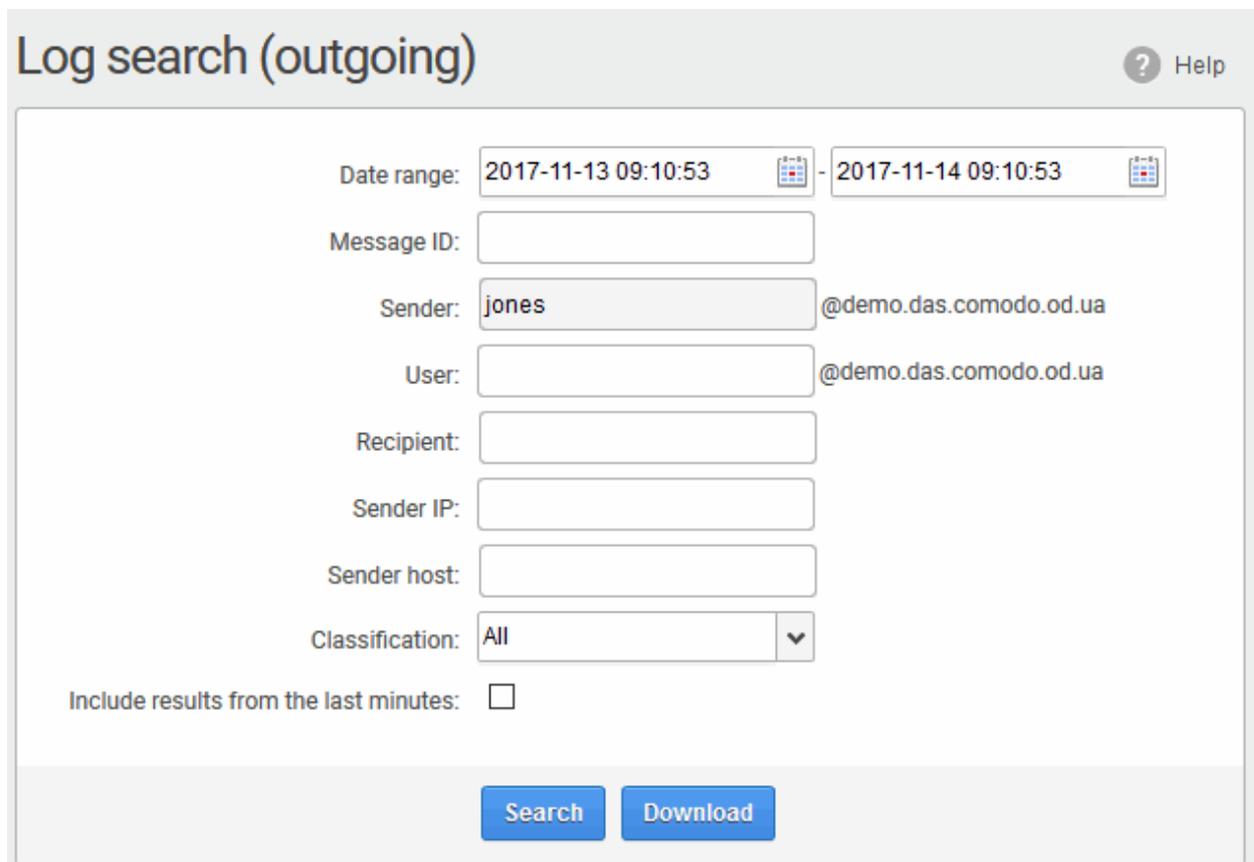
**Note:** The administrator of your email account should have enabled this feature for you. If this is enabled, the 'Log search' will be available in the under the 'Outgoing'.

## Search your outgoing emails in logs

- **Login** to the CSEG interface.
- Click 'Outgoing' on the left then 'Log search'.



The 'Log search (Outgoing)' interface opens:

The screenshot shows the 'Log search (outgoing)' interface. It features a search form with the following fields: 'Date range' (with two date pickers showing '2017-11-13 09:10:53' and '2017-11-14 09:10:53'), 'Message ID', 'Sender' (with 'jones' and '@demo.das.comodo.od.ua'), 'User' (with '@demo.das.comodo.od.ua'), 'Recipient', 'Sender IP', 'Sender host', and 'Classification' (a dropdown menu set to 'All'). There is also a checkbox for 'Include results from the last minutes' which is currently unchecked. At the bottom of the form are two blue buttons: 'Search' and 'Download'. A 'Help' icon is visible in the top right corner of the interface.

- **Date range:** The date range for which you want to search for the sent mails.
- **Message ID:** Enter a unique message identifier (*optional*)
- **Sender:** The currently logged in user name is displayed in this field.
- **User:** The username of the outgoing email address that was used for your outgoing mails. Please note that even though many users may be configured with the same username for their outgoing mails, only the mails sent by you are displayed for the search.
- **Recipient:** The email address of the recipient (for example, 'testuser1@domain.in') that you want to search

for sent mails.

- **Sender IP:** The IP address of the sender.
- **Sender host:** The sender host name.
- **Classification:** The type of email that you want to search from the drop-down options.
- **Include results from the last minutes:** If selected, CSEG will include messages that are currently being migrated from the filtering server to the logging server in the search results.

The option "Include results from the last minutes" will slow down the search result retrieval

- Click the 'Search' button.

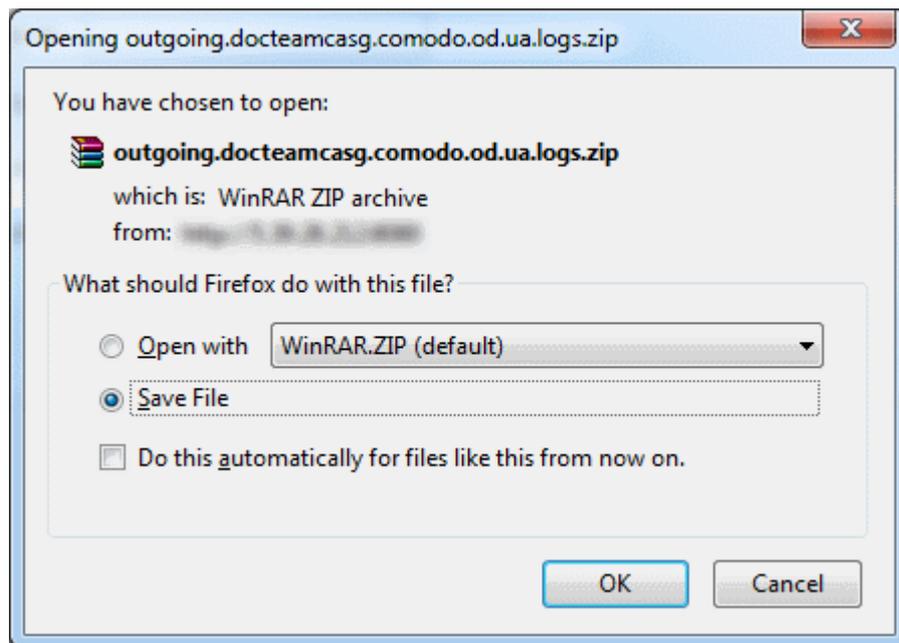
CSEG will search for the sent mails based on the filters entered and / or selected and display the results.

Date and time	Host (Exim id)	Sender host	User	Sender	Recipient	Subject	Classification
2014-10-29 14:49:16	mxsrv3.spamg 1XjUYS- 0005Ws-OH	mail2.comodo. 91.196.95.33	john	john@doctean	demo2@docte	outgoing subject 2	Accepted
2014-10-29 14:48:43	mxsrv2.spamg 1XjUYF- 0002Do-AU	mail2.comodo. 91.196.95.33	john	john@doctean	demo1@docte	outgoing subject	Accepted

Navigation: 1 / 1 [ 1 - 2 / 2 ] Per page 15

- Click the 'Download' button to download the log report of sent mails for the filters entered and/or selected.

The download dialog is shown.



You can open the file by using the browse option or save the file in your system. The compressed log file will be saved in the folder that you have configured for saving download files. The values in the log report will be separated by commas and this file can be opened with application such as Excel or Openoffice Calc.

## 2.14 How to Manage Whitelisted Senders

CSEG lets you define a list of trusted senders known as a 'whitelist'.

- Mails from whitelisted senders are delivered and not blocked by the antispam engine.
- Comodo strongly recommends you use this option only after ascertaining the authenticity of the senders.

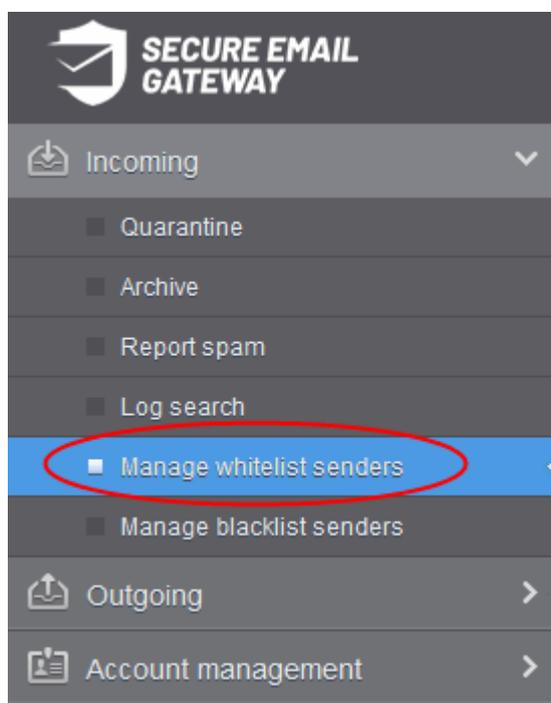
You can add senders to the whitelist in two ways:

- From the Quarantine interface
  - Request the administrator of your account to whitelist senders
  - OR
  - Add sender yourself to whitelist without approval from the administrator depending on the permissions configured. See **Quarantine** section.
- From the Manage whitelist senders interface
  - Manually add or delete senders to whitelist, depending on the permissions assigned to you by the administrator.

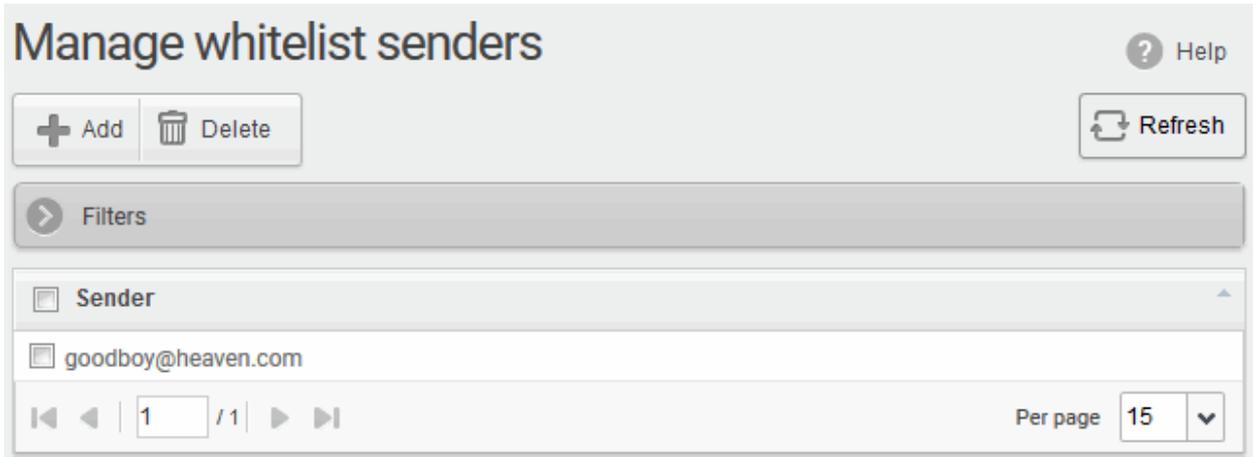
This section explains viewing the list of Whitelisted senders and adding/removing senders to the list.

### Manage whitelist senders

- Click 'Incoming' on the left and choose 'Manage whitelist senders'



Whitelisted senders for your mail account are listed in the interface:

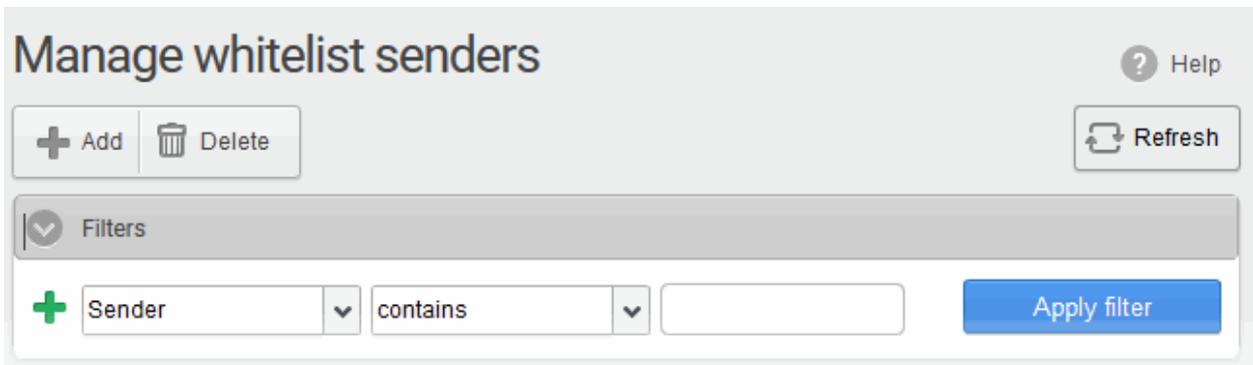


From this interface you can:

- **Add senders to whitelist manually**
- **Remove senders from whitelist**

**Note:** The 'Add' and 'Delete' buttons are available only if the administrator of your account has enabled this for you. If this is not enabled, you can just view the whitelisted senders in this interface.

- Click the 'Sender' header to sort the entries in ascending or descending order of senders' names.
- Click anywhere on the 'Filters' stripe to open (or close) the filters area.



- You can filter results by sender
  - **Sender:** Type a sender's mail address in the text box (column 3) and select a condition in column 2.

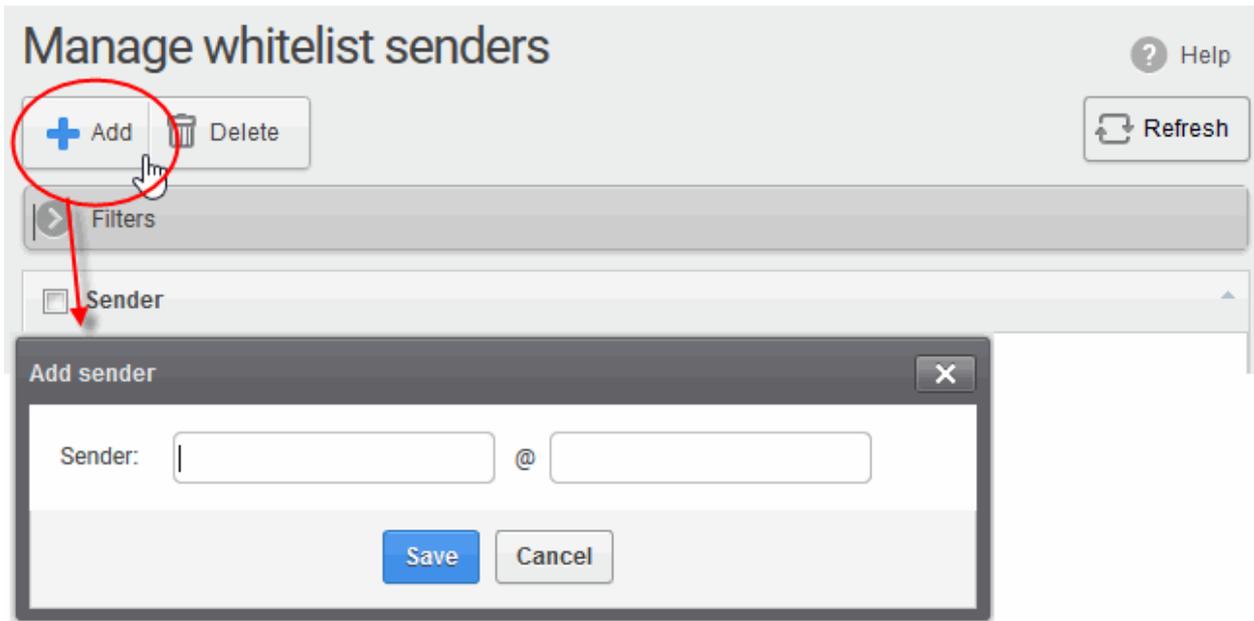
Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

### Manually add senders to whitelist

- Click the 'Add' button at the top.

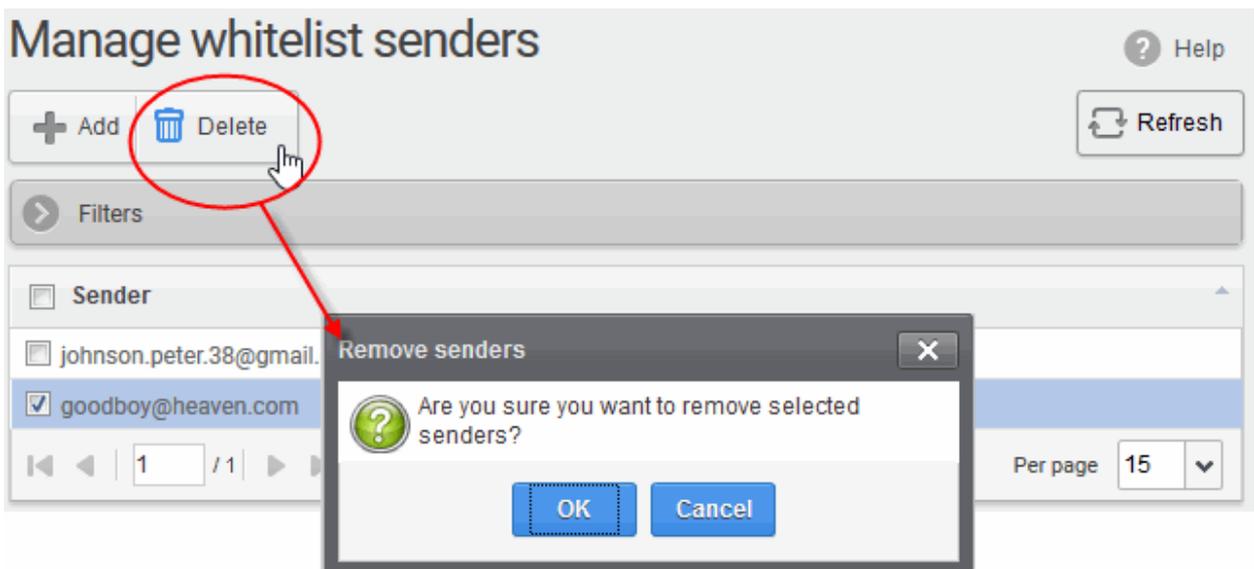
The 'Add sender' dialog opens:



- Enter the sender's username in the first text box and sender's email domain name in the second text box after the @ symbol.
- Click the 'Save' button. Repeat the process to add more senders to whitelist.

### Remove senders from whitelist

- Select the sender(s) from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.

## 2.15 How to Manage Blacklisted Senders

- CSEG allows you to blacklist senders who frequently send unsolicited emails to you.
- The sender is blocked only for you and not for other users in the domain.
- Messages from blacklisted senders are not quarantined.

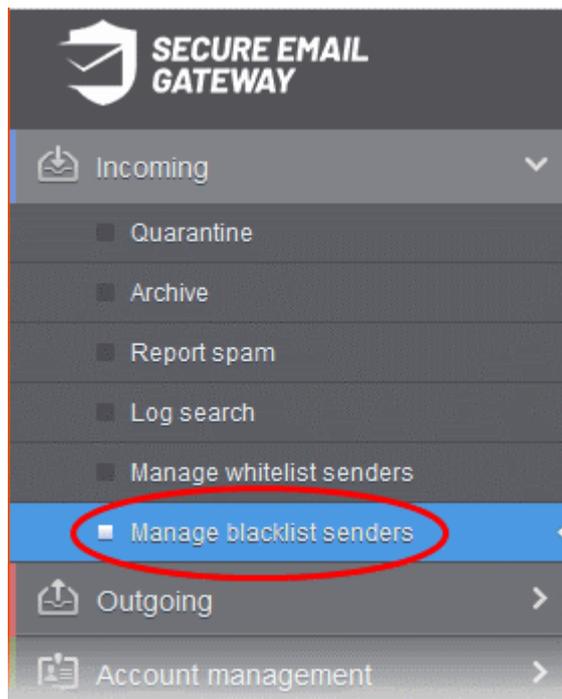
- The sending SMTP server will send a 'bounce' message to the sender.

You can add senders to the blacklist in three ways:

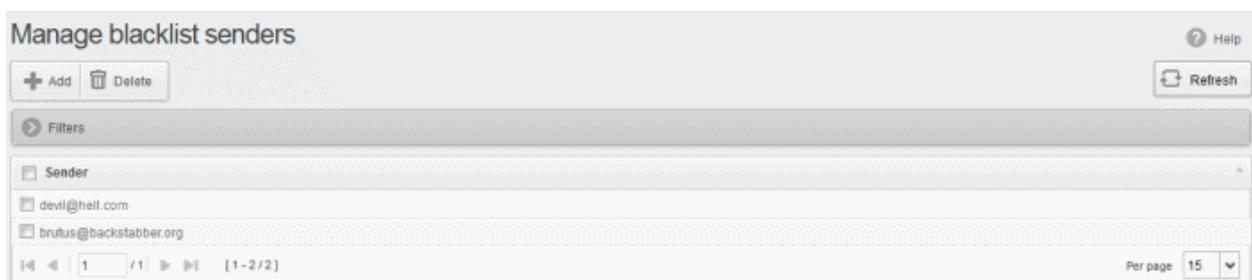
- From the **Quarantine** interface - By requesting your administrator to blacklist senders of selected quarantined emails. For more details see the **Quarantine** section.
- From the **Archive** interface - By requesting your administrator to blacklist the senders of selected mails. For more details see the **Mail Archive** section.
- From the 'Manage blacklist senders' interface - You can manually add or delete senders to blacklist, depending on the permissions assigned to you by the administrator.

## Manage blacklist senders

- Click 'Incoming' on the left then choose 'Manage blacklist senders'



The 'Manage blacklist senders' interface is shown with a list of senders blacklisted for your mail account.



From this interface users can:

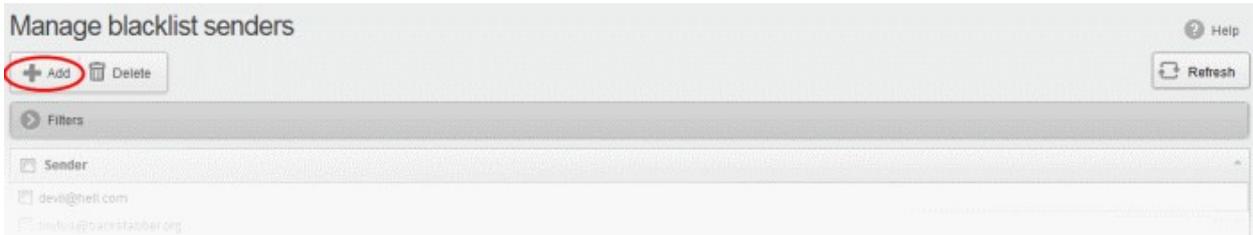
- **Add senders to blacklist manually**
- **Remove senders from blacklist**

**Note:** The 'Add' and 'Delete' buttons are available only if the administrator of your account has enabled this for you. If this is not enabled, you can just view the blacklisted senders in this interface.

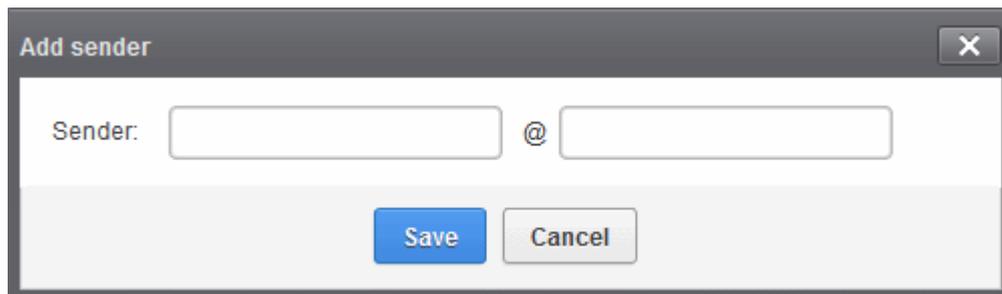
- Click on the 'Sender' column header to sort the entries in ascending or descending order of sender names.
- You can use the filter options to search for specific sender from this interface.

## Manually add senders to blacklist

- Click the 'Add' button at the top.



The 'Add sender' dialog will be displayed.



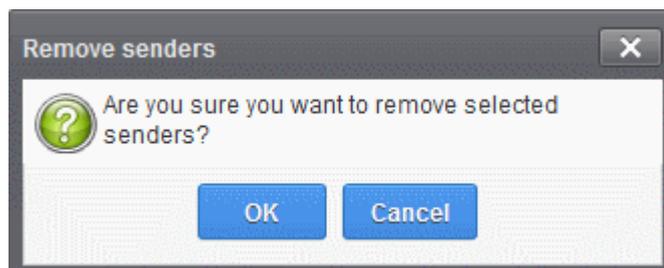
- Enter the sender's username in the first text box and sender's email domain name in the second text box after the @ symbol.
- Click the 'Save' button. Repeat the process to add more senders to blacklist.

## Remove senders from blacklist

- Select the sender(s) from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog for your changes to take effect.

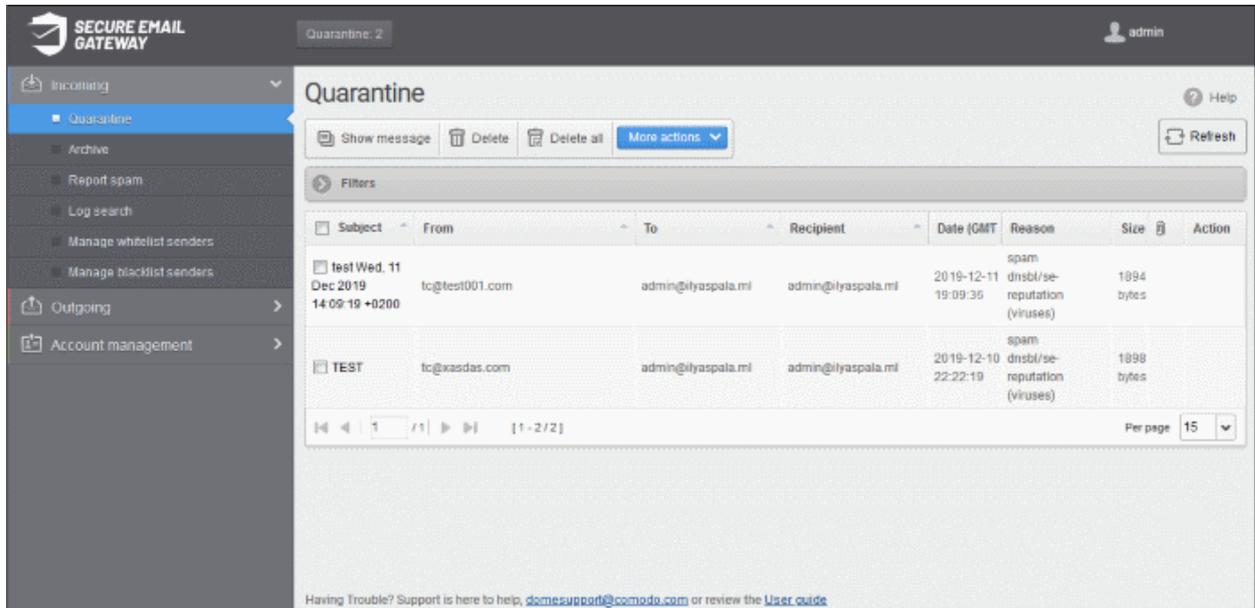


## 3 The CSEG User Console

The user console of Comodo Secure Email Gateway (CSEG) allows you to manage your incoming mails and account settings.

- The CSEG web interface is divided into three main areas - Incoming, Outgoing and Account Management. These can be accessed in the menu on the left.
- Each area has several sub-sections. The exact number of features available to you depends on the permissions set by your administrator.

The image below shows the user interface after logging in.



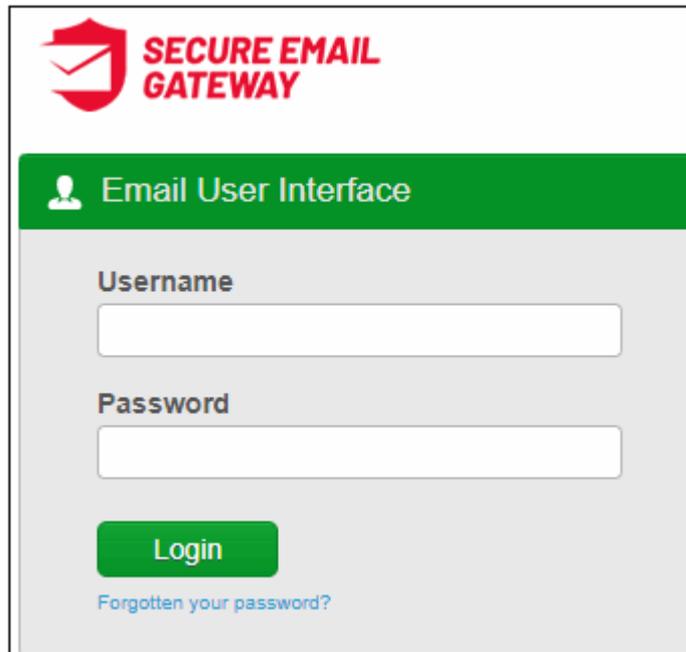
### Main Functional Areas

- **Incoming** - In this area, a user can manage his/her quarantined mails, perform log search of incoming mails, report spam, manage whitelist and blacklist senders. See the **Incoming** section for more details.
- **Outgoing** - In this area, a user can perform log search of outgoing mails. See the **Outgoing** section for more details.
- **Account Management** - In this interface, a user can change his/her CSEG login password and choose to add or remove in Recipient Whitelist and managing subscription to periodical quarantine summary reports. See the **Account Management** section for more details.

### 3.1 Login to the User Interface

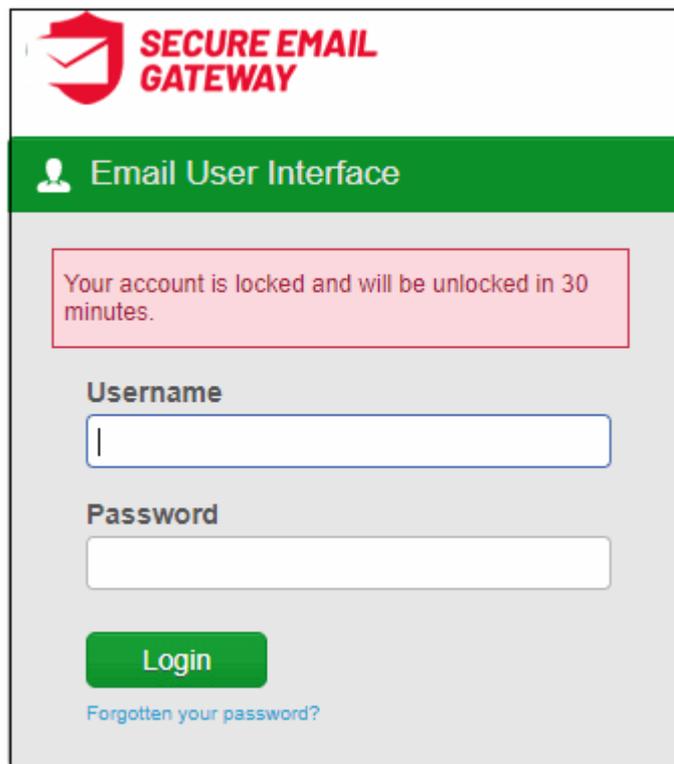
You can login into your account using any internet browser. Your admin should let you know which to use.

- USA users - <https://us-domeasmsp.cdome.net/user/login.zul>
- EU users - <https://domeasmsp.cdome.net/user/login.zul>



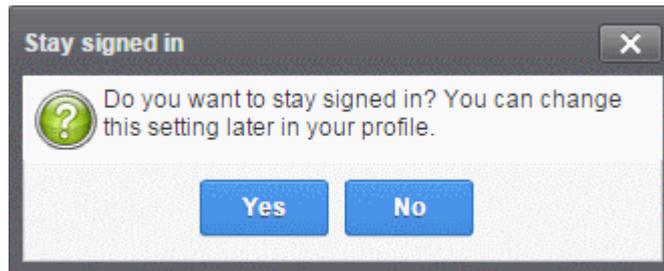
- Login to your account with the username and password that were sent to you via email after your CSEG account was created.

For safety reasons, CSEG will lock the account for 30 minutes after three failed login attempts. Please contact your administrator if you want to unlock the account immediately.



- The length of time that accounts are locked for can be customized by contacting your Comodo account Manager.
- If you have forgotten your login password, click 'Forgotten your password?' to generate a new password. [Click here](#) for more details.

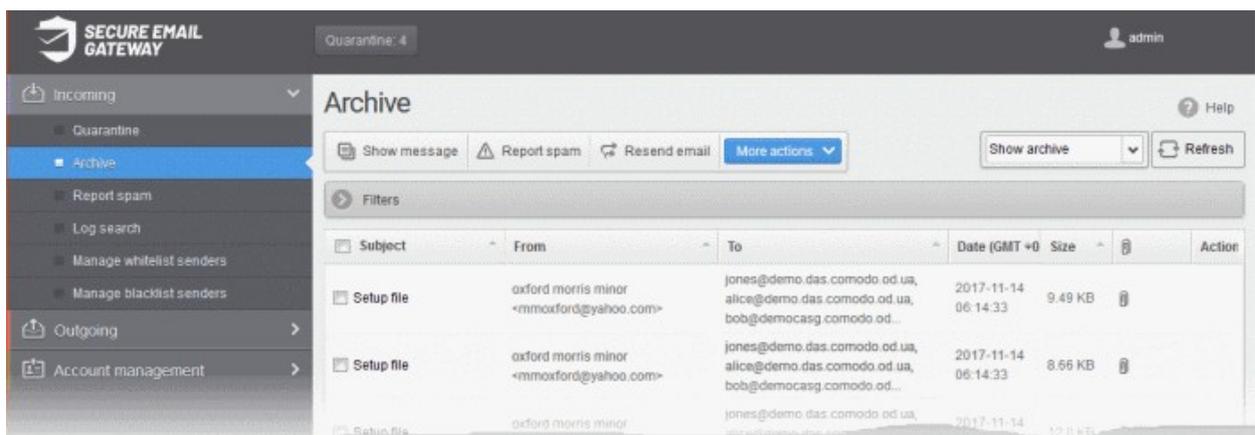
After first login, you might be able to login on subsequent occasions without providing your credentials if so configured your administrator. A message will be shown after logging-in for the first time if this feature is enabled:



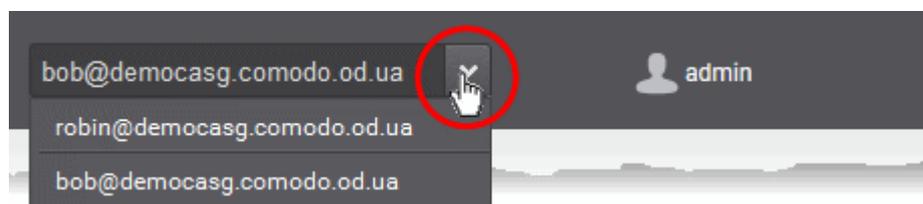
- Click 'Yes' to enable the feature.

You can change these settings anytime in 'My Profile' > 'Change settings'. The 'Stay signed in' check-box will only be available if your administrator has enabled the option for the domain. See **'Managing My Profile'** for more details.

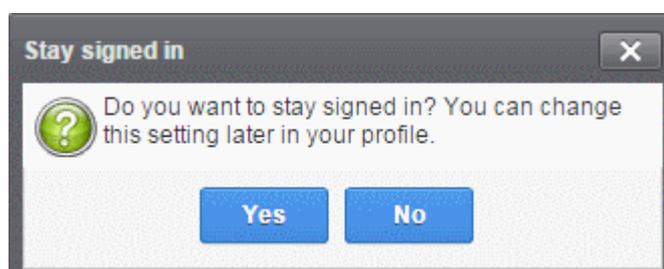
Once you have successfully logged-in, the CSEG dashboard for your email account is displayed.



If you have aliases, you can choose any of your primary and alias email accounts from the drop-down at the top right. The CSEG dashboard for the chosen account is displayed.



Depending on the settings configured by the administrator, you can access your CSEG account without providing your credentials each time after logging-in the first time. You will see an alert when you are logging-in for the first time in a browser after the auto-login feature is enabled by the administrator.



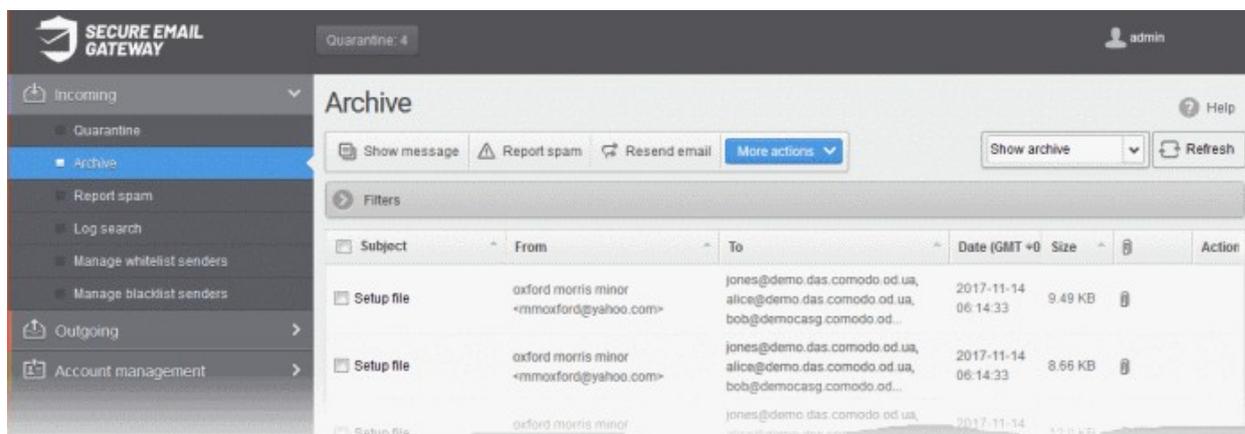
Clicking 'Yes' will enable the 'Stay signed in' check box in the 'My Profile' interface. You can change the settings anytime in the 'Change settings' section from the 'My Profile' interface. The 'Stay signed in' check box will be available only if the administrator has enabled this option for the domain. See '[Managing Profile Settings](#)' for more details.

Please note that this auto-login feature will work in the same browser that you used to access CSEG and opted for this feature. If you use another browser, you have to login again. The auto-login feature will be valid for a certain period only depending on the number of days configured by the administrator. If the period expires, then you have to login again.

## 3.2 The User Interface

- The CSEG user interface has three main functional areas - 'Incoming', 'Outgoing' and 'Account management'.
- You can access these areas using the links on the left. Each area has several sub-sections.

**Note:** Access to various interfaces depends on the permission levels set for you by your administrator. For example, 'Quarantine', 'Report spam', 'Log search' and 'Manage report subscriptions' may not be available to you. Please contact your administrator should you require access to them.



- **Incoming** - Manage quarantined mail, perform log searches of incoming mails, report spam, manage whitelisted and blacklisted senders. See the [Incoming](#) section for more details.
- **Outgoing** - Run log searches of outgoing mails. See the [Outgoing](#) section for more details.
- **Account Management** - Change password, update the recipient whitelist and manage subscriptions to quarantine reports. See [Account Management](#) for more details.
- **Support** - The [support.comodo.com](http://support.comodo.com) link at the bottom of interface opens the Comodo support portal, an online knowledge base and support ticketing system. This is the fastest way to get help with any issues you encounter.

Various interfaces displays a help button  at the top-right of the interface. Click this button to view help on the interface you have open at the time.

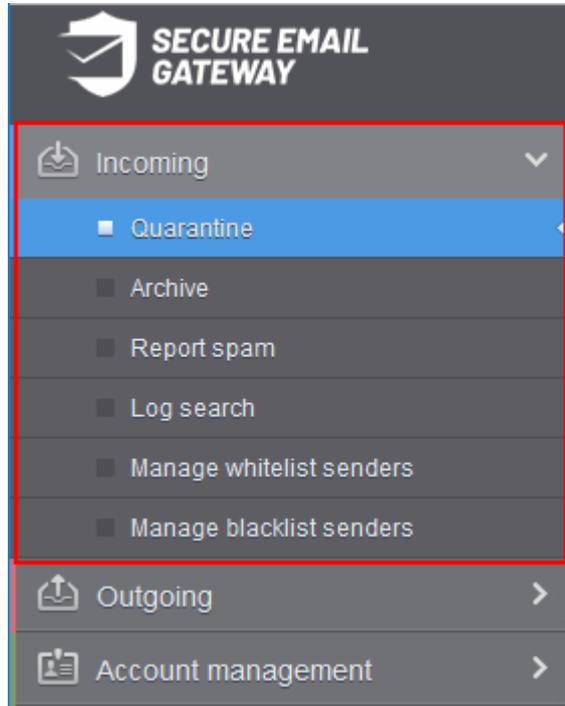
Click the following links for more details on each of the sections:

- [Incoming](#)
- [Outgoing](#)
- [Account Management](#)

## 3.2.1 Incoming

The 'Incoming' area lets you view/release quarantined emails, perform log searches of incoming mails and add senders to the whitelist or blacklist.

**Note:** Access to various interfaces depends on the permission levels set for you by your administrator. For example, the 'Quarantine' screen may not be available if this feature is not enabled for you.



Click the following links for more details on each area in the 'incoming' section:

- [Quarantine](#)
- [Archive](#)
- [Report Spam](#)
- [Log Search](#)
- [Manage Whitelist Senders](#)
- [Manage Blacklist Senders](#)

### 3.2.1.1 Quarantine

- CSEG scans all messages received by your mail server to identify spam and malicious email.
- If enabled by your administrator or by yourself, you will receive notifications when a mail sent to you or your aliases is quarantined.
- The notification mail contains a link to view the message. The link will expire after 24 hours. See '[Managing Profile Settings](#)' for more details about enabling/disabling quarantine mail alerts.



## New quarantined message for [admin@bulut.ml](mailto:admin@bulut.ml)

Sender: [muratti66@hotmail.com](mailto:muratti66@hotmail.com)  
Date: Dec 05, 2019 07:04  
Subject: püff  
Reason: spam Combined (0.99)

For help, see the User guide: <https://help.comodo.com/topic-445-1-917-12240-Introduction-to-Comodo-Dome-Antispam---MSP.html>

Having Trouble? Support is here to help, [domesupport@comodo.com](mailto:domesupport@comodo.com) or review the [Users Guide](#)

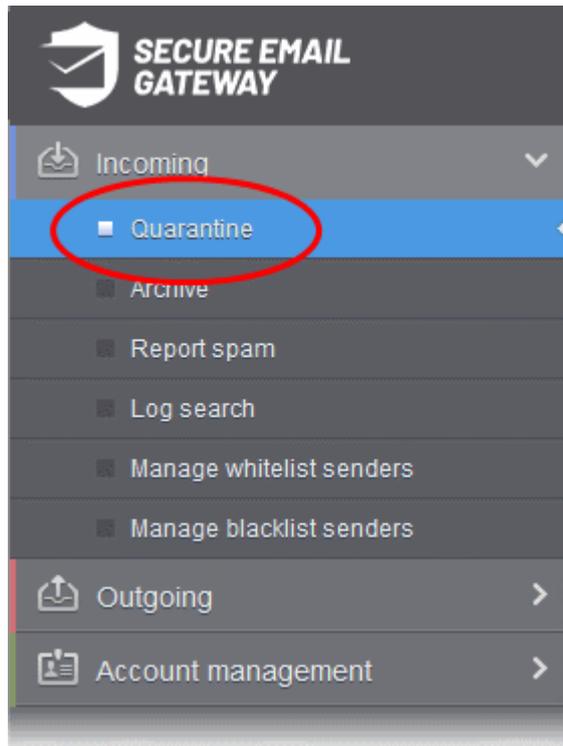
- The notification mail contains links to request the mail is released from quarantine, to whitelist/blacklist the sender or to delete the mail from quarantine.
- If you want to release the mail from quarantine or blacklist/whitelist the sender, you need to login to the CSEG user interface and open the quarantine interface.
- The 'Quarantine' interface shows mails addressed to you but quarantined by CSEG. You can view the mails and even download attachments from them if you are sure they are safe. You may also send requests to your administrator to release quarantined emails or add senders to the whitelist or blacklist.

**Note:** Please contact your administrator if you are not able to view your quarantined mail.

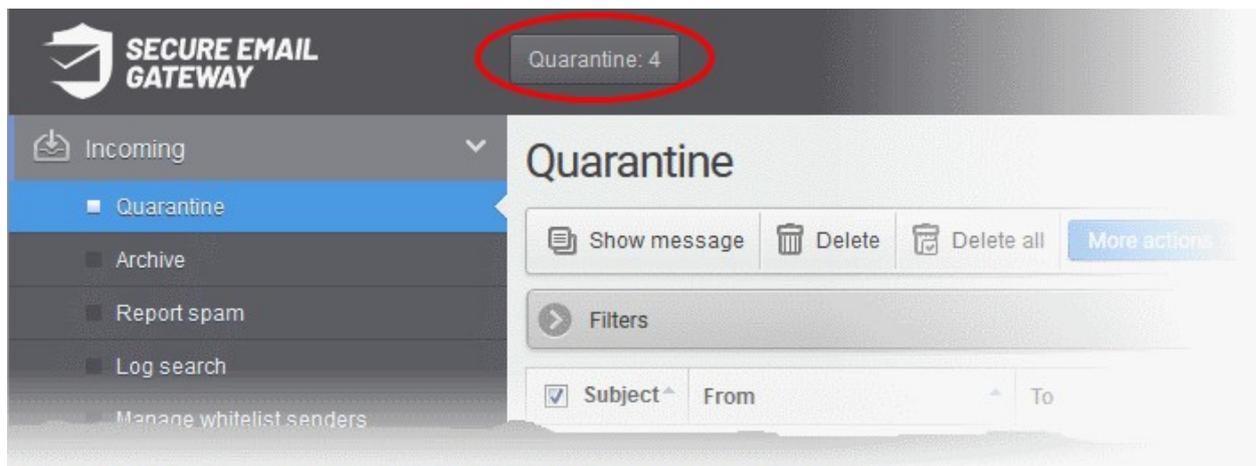
**Tip:** You can configure CSEG to send you regular quarantine reports. The report lists all your quarantined messages. See [CSEG Reports](#) for more on this.

### Open the quarantined interface

- Click 'Incoming' on the left then select 'Quarantine'



- Alternatively, click the 'Quarantine' button at the top.



The quarantine area opens:

## Quarantine ? Help

Show message
Delete
Delete all
More actions ▾

Show messages for all aliases
 Refresh

Filters

Subject	From	To	Recipient	Date (GMT)	Reason	Size	🗑️	Action
<input type="checkbox"/> Fw: Become a certified cloud computing professional	Stealing Talent <teacher@stealingtalent.com>	robin@democasg.com	robin@democasg.com	2016-02-2 09:04:25	spam Combined (0.15)	20.89 KB	🗑️	
<input type="checkbox"/> Fw: Make your journey more exciting with 0 first year fee and rewards	Bullock Travels <marketing@yaktouring.org>	bob@democasg.com	bob@democasg.com	2016-02-2 08:43:01	spam Combined (0.15)	14.42 KB	🗑️	
<input type="checkbox"/> Fw: Investment with lasting returns	Money Swindlers <campaign@mswindlers.org>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:47	spam Combined (0.14)	5.91 KB	🗑️	
<input checked="" type="checkbox"/> Fw: Get upto 90% off on household items.	Brokenpot Sellers <offers@brokenpotsellers.co.uk>	bob@democasg.com	bob@democasg.com	2016-02-2 07:35:03	spam Combined (0.19)	6.1 KB	🗑️	

⏪
|

/

▶
[ 1 - 4 / 4 ]

Per page 15

**Note:** Depending on the permission level configured for your email account by your administrator, the buttons in the interface may vary. For example, 'Show message' button may not be available in the interface. The 'Request release' button may appear as 'Release' button in the 'More actions' drop-down button enabling you to release quarantined mail without approval from the administrator.

- **More Actions** - Request that the mail is released from quarantine, or that the sender is added to the blacklist or whitelist.
- **Show messages for all aliases** - By default, the list only shows mails sent to your primary email address. Select this option to view messages sent to all your mailboxes.

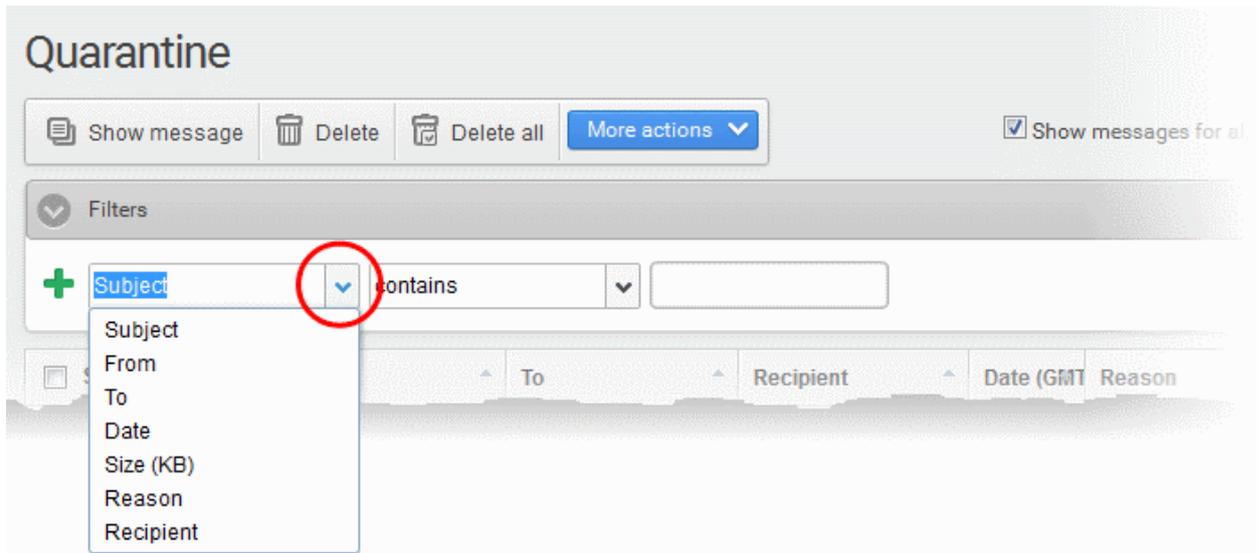
**Note:** The option 'Show messages for all aliases' will not be available if you have have switched to an alias account.

From this interface you can:

- **View quarantined mails**
- **Delete quarantined mails**
- **Request administrator to release quarantined mails**
- **Request administrator to add senders to blacklist**
- **Request administrator to add senders to whitelist**

### Use Filters to search quarantined emails

- Click anywhere on the 'Filters' stripe to open (or close) the filters area.



- Choose the filter by which you want to search from the first drop-down, then a condition in the 2<sup>nd</sup> text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the mail subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Date:** Search by date and time mails quarantined. Select the date (column 3) and select a condition in column 2.
- **Size (KB):** Search quarantined mails by their size. Select or enter the mail size in column 3 and select a condition in column 2.
- **Reason:** Enter the quarantined reason in the text box (column 3) and select a condition 2.
- **Recipient:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

## View Quarantined Mails

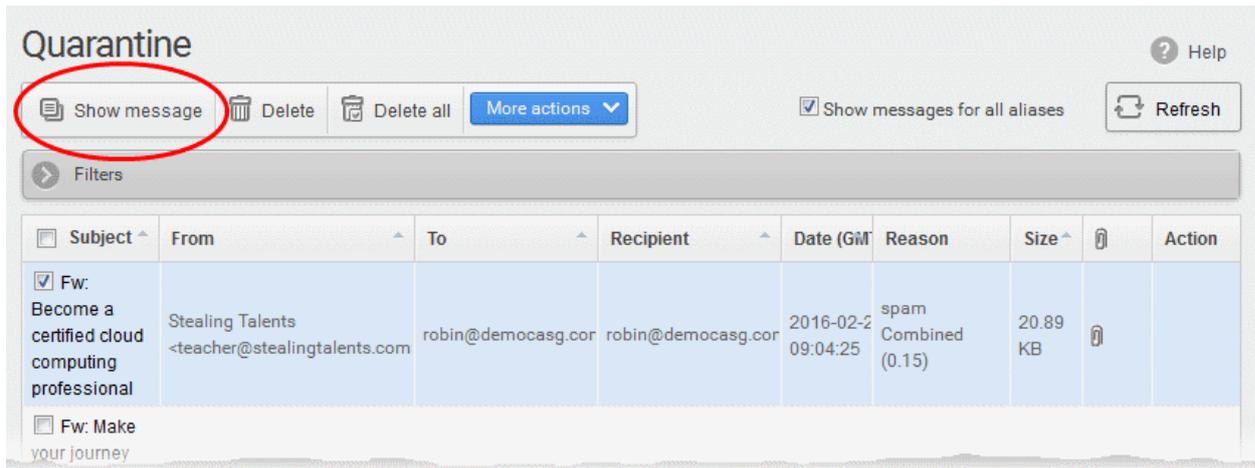
**Note:** The administrator of your email account should have enabled this feature for you. If this is enabled, the 'Show message' button will be available in the interface.

You can view the quarantined mails in two ways:

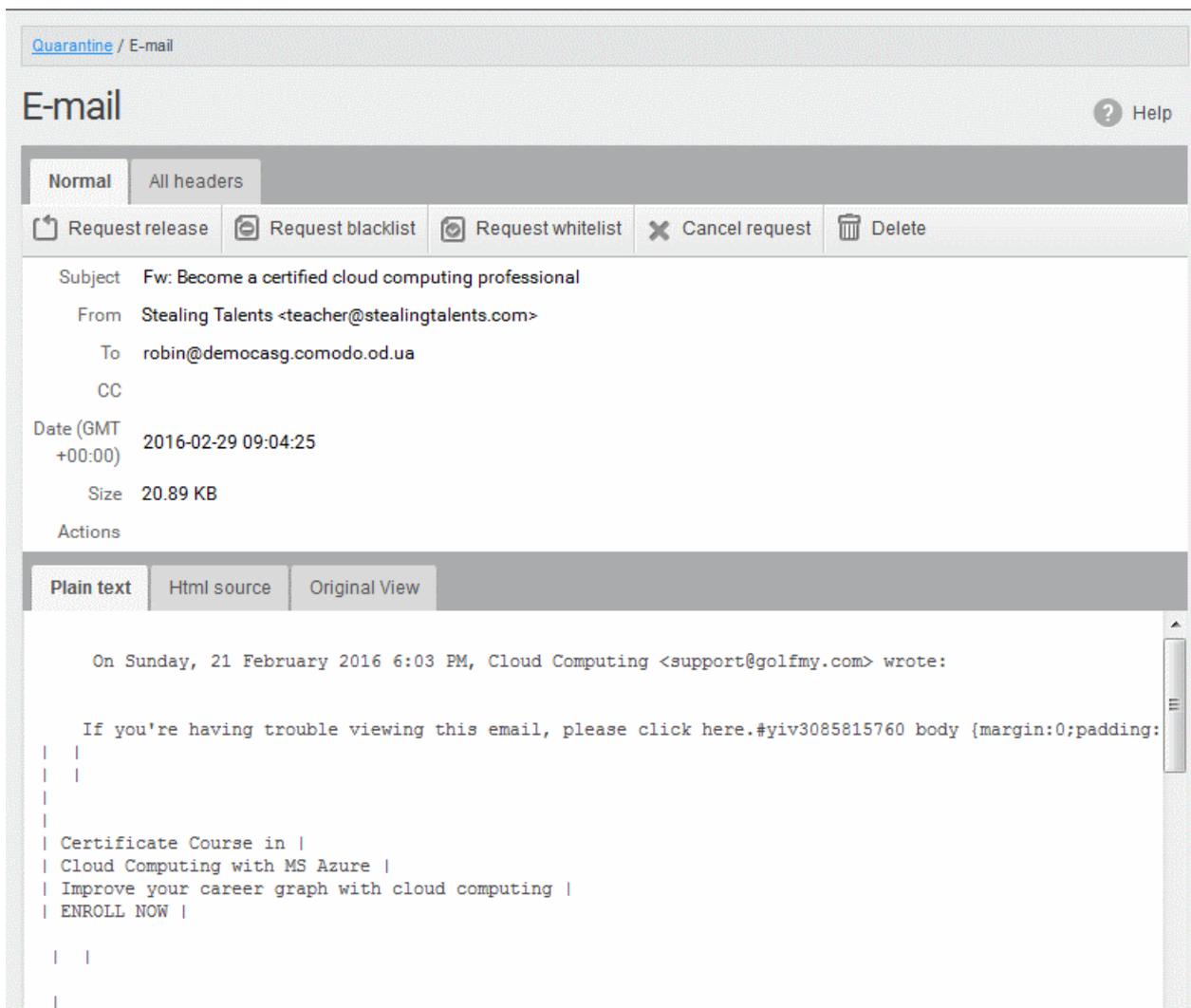
- **In the same CSEG window**
- **In a new CSEG window**

### View quarantined mails in the same CSEG window

- Select the mail that you want to view and click the 'Show Message' button.
- OR
- Click on the email link in the subject column that you want to view its details.

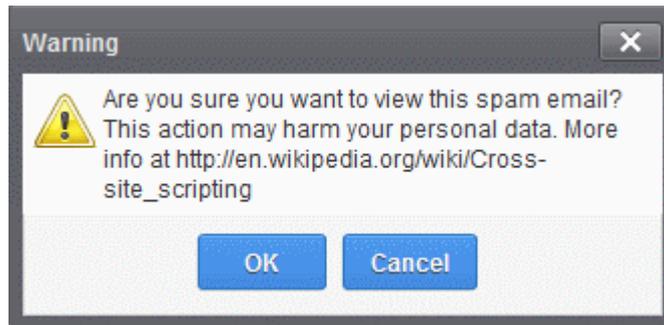


The selected mail opens:



By default, the email opens in normal view and shown in plain text, where the images, banners and links are not be displayed.

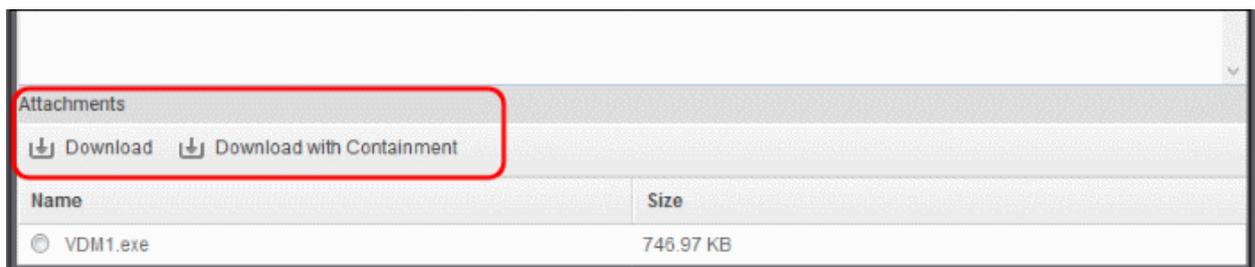
- Click 'Html source' to view the source code of the mail.
- Click the 'Original View' tab to view images and links. A warning message is shown as follows:



- Click 'OK' to view the email.

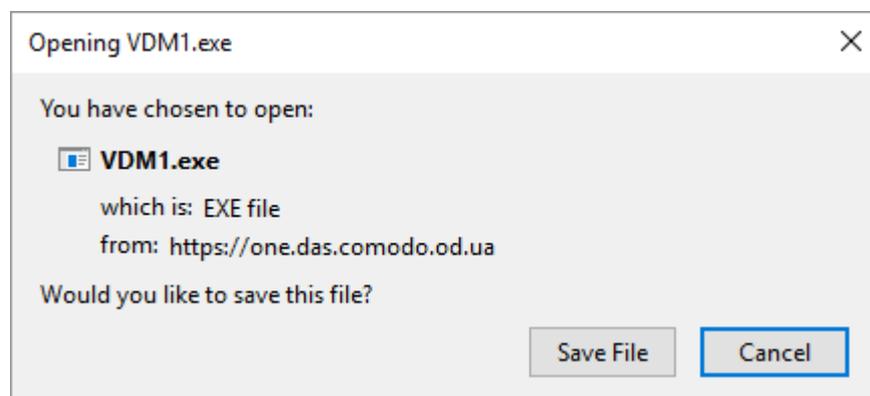
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **release** the email or to add the sender to **whitelist** or **blacklist**.

If there is an attachment, you can download it from this dialog.



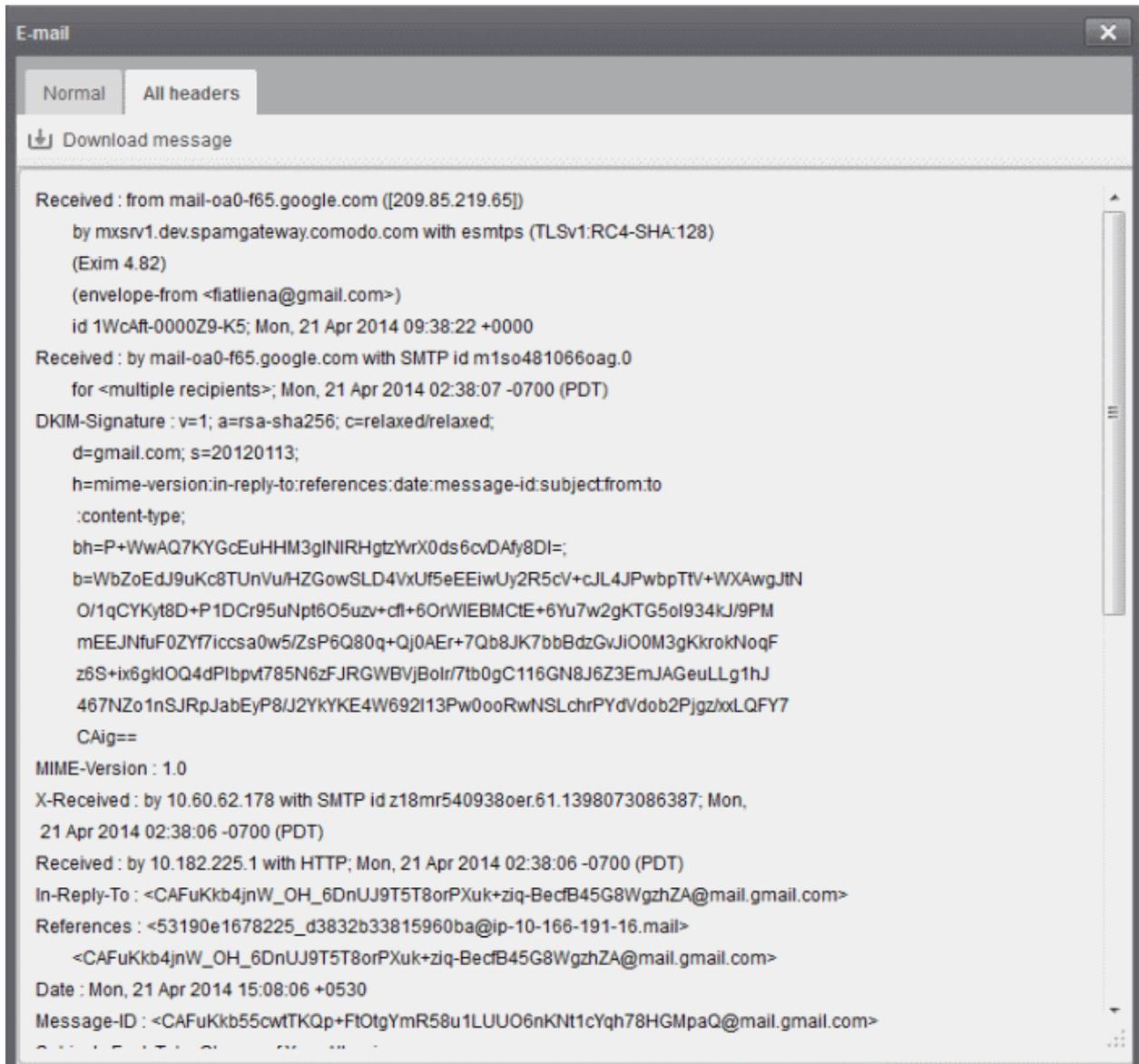
- Select the attachment and click 'Download' or 'Download with Containment'
  - **Download** – You can save the file / attachment as original.
  - **Download with Containment** – Containment is a technology whereby attachments with an 'unknown' trust rating are run inside a secure, sandbox environment. You can open and run the file as normal, but it is prevented from making potentially damaging changes to your computer.

'Download with containment' is only available if enabled by your administrator.



You can open the attachment with an appropriate application or save to a desired location in your computer.

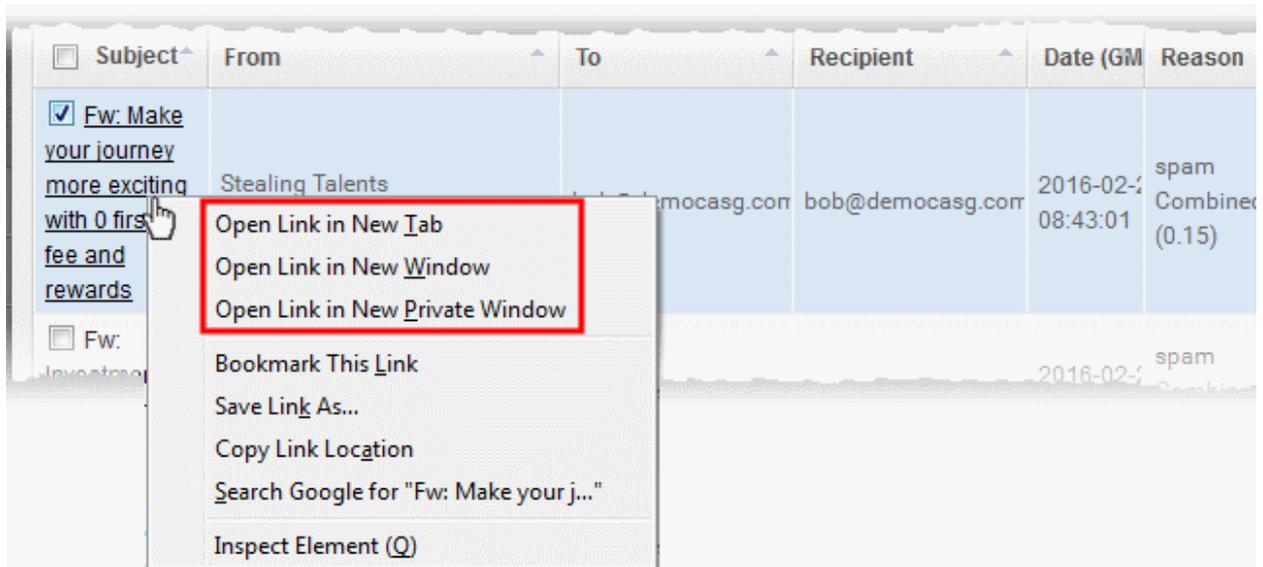
- Click 'All headers' to view the email headers, which contain information about the route taken by the mail before it reached your mailbox. The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.



- To download the email as a HTML file, click 'Download' message.

### View a quarantined mail in a new window

- Right-click on the subject line of the mail you want to view and choose to open in a new tab or new window from the context sensitive menu.

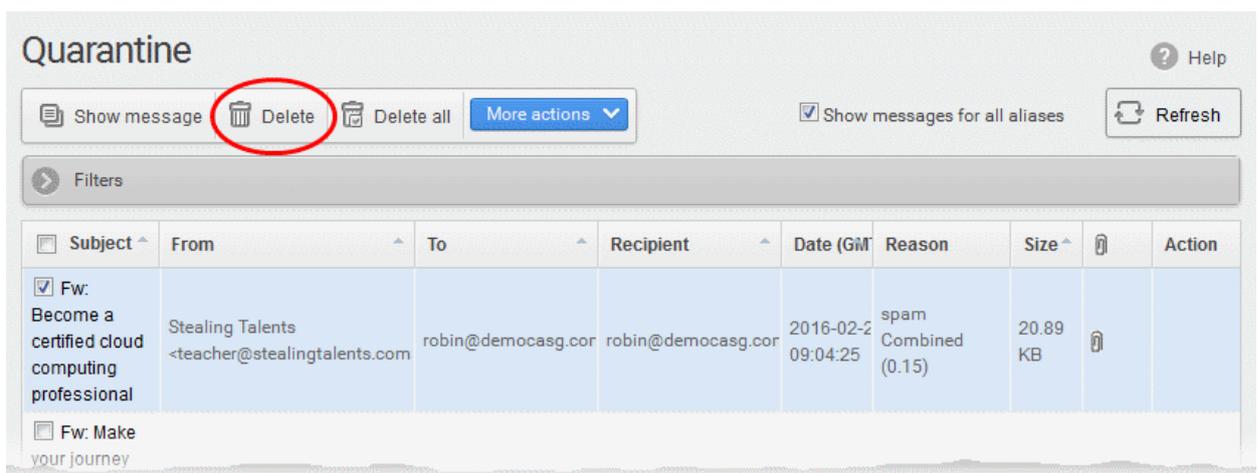


Your browser may display a warning pop-up window notification. Click 'Options' > then select 'Allow pop-ups for...' to allow the message to open in a new window. Click 'Show message in new window' again.

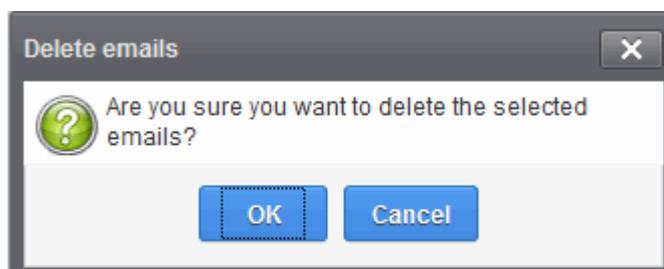


## Delete a quarantined mail

- Select the mail that you want to delete and click the 'Delete' button

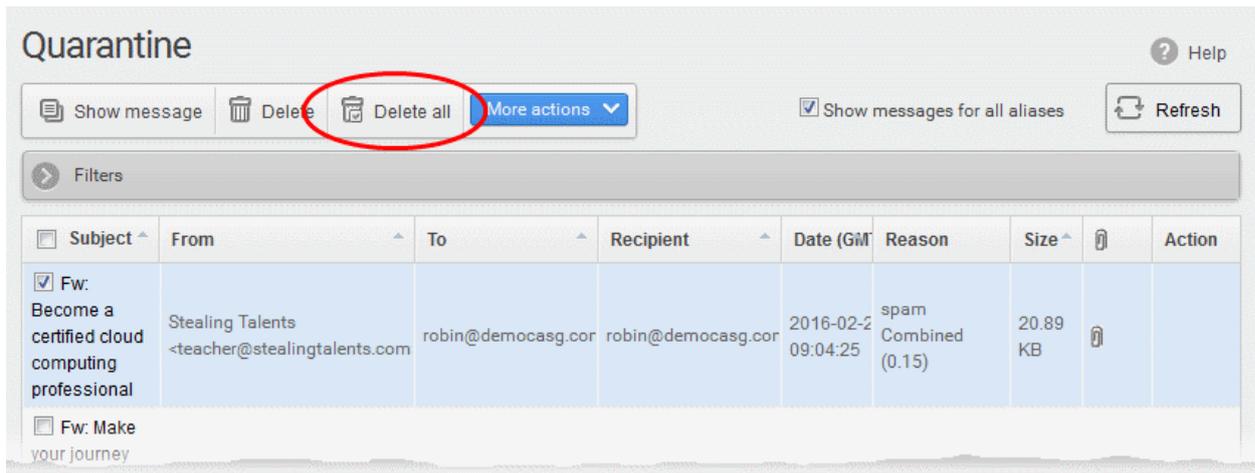


An alert is shown to confirm the deletion. Click 'OK' to delete the selection email.

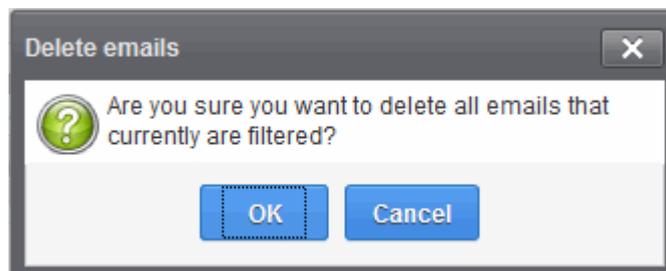


The selected mail is deleted and will no longer be in the quarantined mail list.

- To delete all the quarantined mails click the 'Delete All' button.



An alert is shown to confirm the deletion.



- Click 'OK' to delete all quarantined emails.

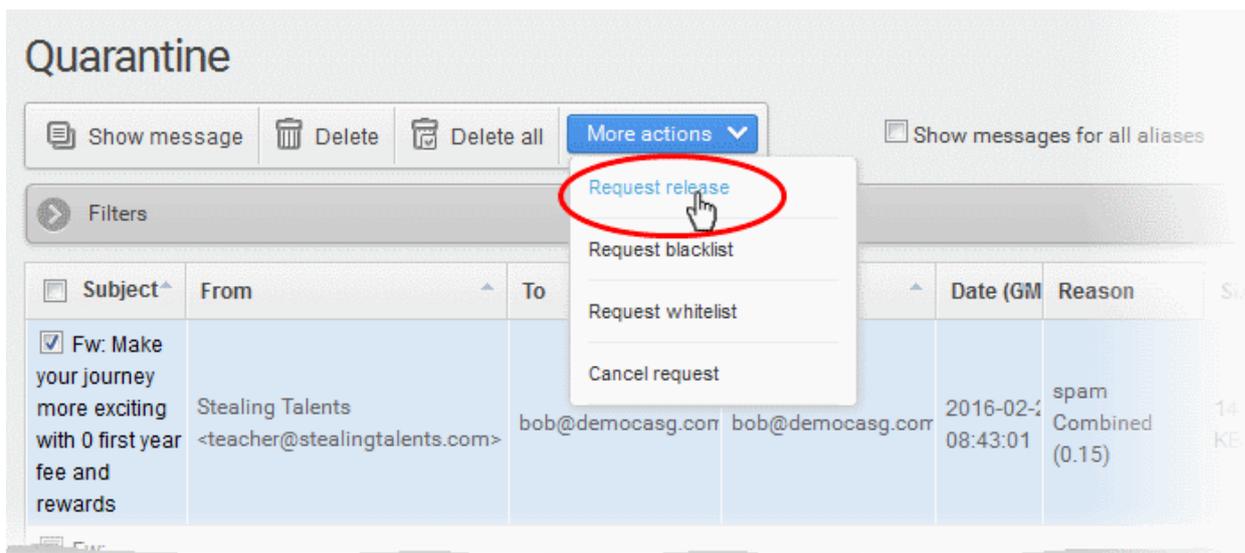
All the quarantined emails for the selected domain are deleted.

### Request administrator to release quarantined mails

After viewing and ensuring that the selected email is not a spam you can request your email account administrator to release the email.

**Note:** Depending on the permission level configured for your email account by your administrator, the button for releasing quarantined email is either 'Release' or 'Request release' in the 'More actions' drop-down button. If the interface displays 'Release' button, you can release the selected email from the list without approval from your administrator.

- Select the mail that you want to release and click 'More actions' > 'Request Release'



An email notification is sent to your administrator for your request and you will also receive the request email. This request is also displayed in the 'Action' column of the users' quarantined interface. If the administrator accepts the request, the user receives the email and if it is rejected, 'Release' icon in the 'Action' column are no longer shown.

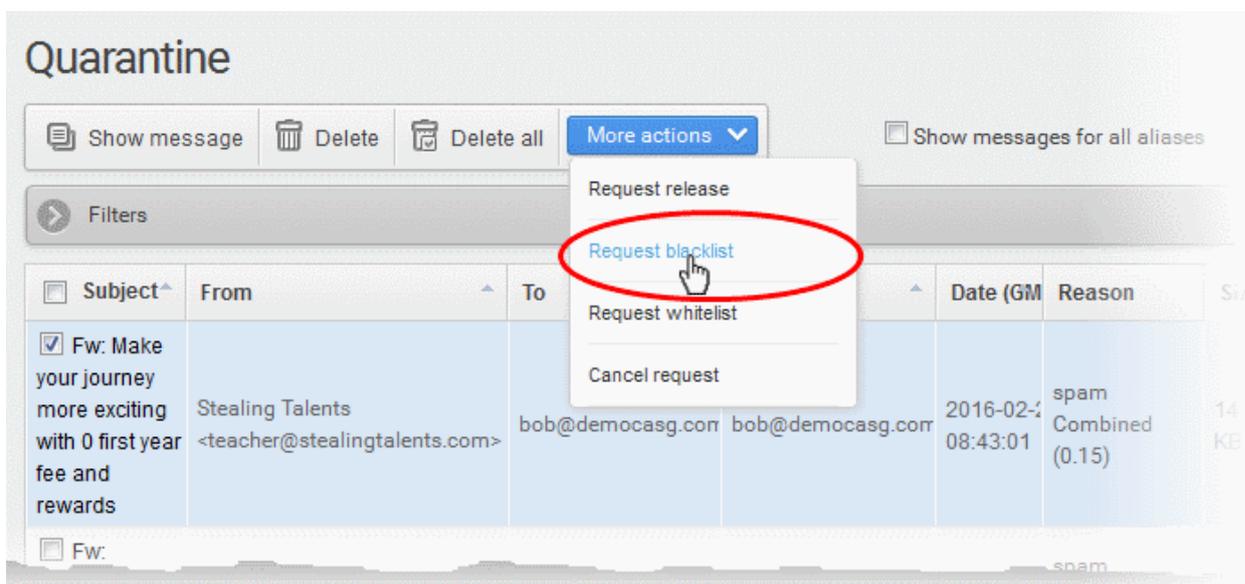
- Click 'More actions' then 'Cancel request' to call off the request before the administrator accepts the request

### Request to add a sender to the blacklist

To avoid receiving spam emails, you can request the administrator to add the senders of these emails to blacklist.

**Note:** Depending on the permission level configured for your email account by your administrator, the button for adding senders to blacklist is either 'Blacklist this Sender' or 'Request blacklist' in the 'More actions' drop-down button. If the interface displays 'Blacklist this Sender' button, you can add the sender to blacklist without approval from your administrator.

- Select the mail whose sender you want to add to the blacklist and click 'More actions' > 'Request Blacklist'



A notification is sent to your administrator for your request and you also will receive the request email. This request is also shown in the 'Action' column of the users' quarantined interface.

- If the administrator accepts the request, the sender is added to blacklist and the user will no longer receive any mail from that sender.
- If the request is rejected, 'Blacklist this Sender' icon in the Action column will no be longer be displayed.

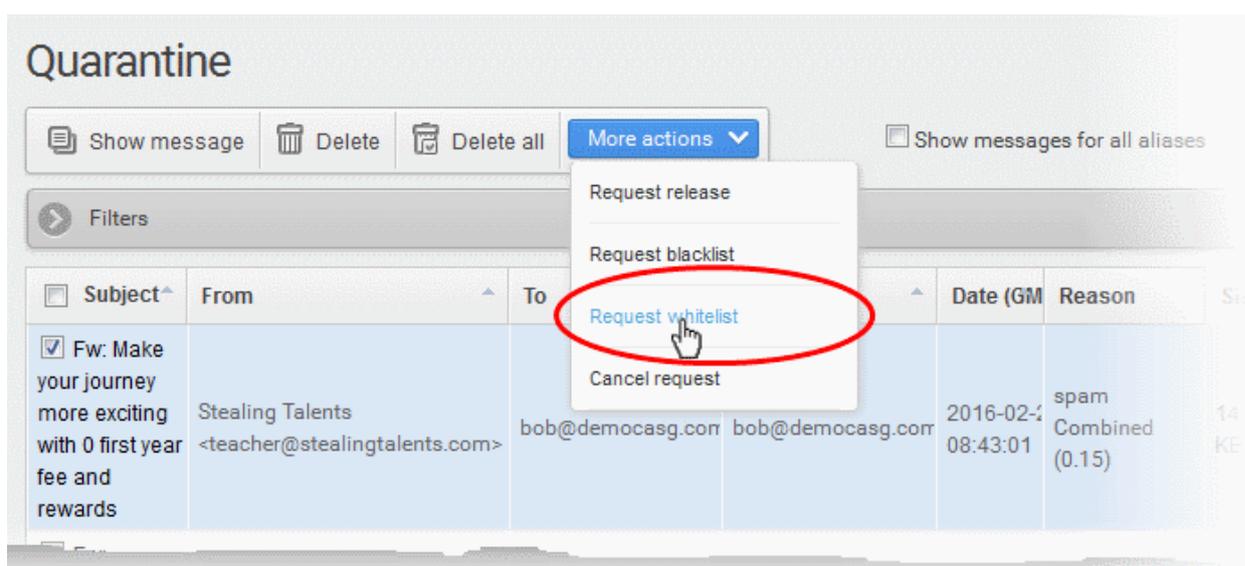
- Senders added to blacklist are displayed in the 'Manage blacklist senders' interface. See **Managing Blacklisted Senders** for more details.
- To call off the request before the administrator accepts the request, choose the mail > click 'More actions' then 'Cancel request'.

## Request to add a sender to the whitelist

If mail from a sender that you trust gets quarantined, you can request your administrator to add the sender to the whitelist.

**Note:** Depending on permissions set by your administrator, the link in the 'More Actions' drop-down is either 'Whitelist this Sender' or 'Request whitelist'. If the interface displays 'Whitelist this Sender' button, you can add the sender to whitelist without approval from your administrator.

- Select the mail that you want its sender to be added to whitelist and click 'More actions' > 'Request Whitelist'



An email notification is sent to your administrator with your request. You also will also receive the request email. This request is also shown in the 'Action' column of the users' quarantined interface.

- If the administrator accepts the request, the sender is added to whitelist and the mails from them are no longer quarantined.
- If the request is rejected, 'Whitelist this Sender' icon in the 'Action' column is no longer shown.

Senders added to whitelist are displayed in the 'Manage whitelist senders' interface. See **Manage Whitelisted Senders** for more details.

- Click 'More actions' then 'Cancel request' to call off the request.

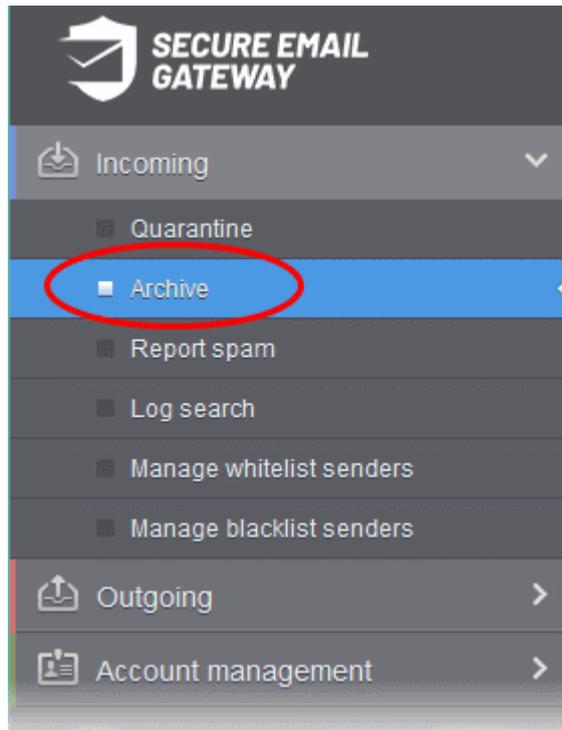
### 3.2.1.2 Mail Archive

CSEG is capable of saving copies of your emails in the archive.

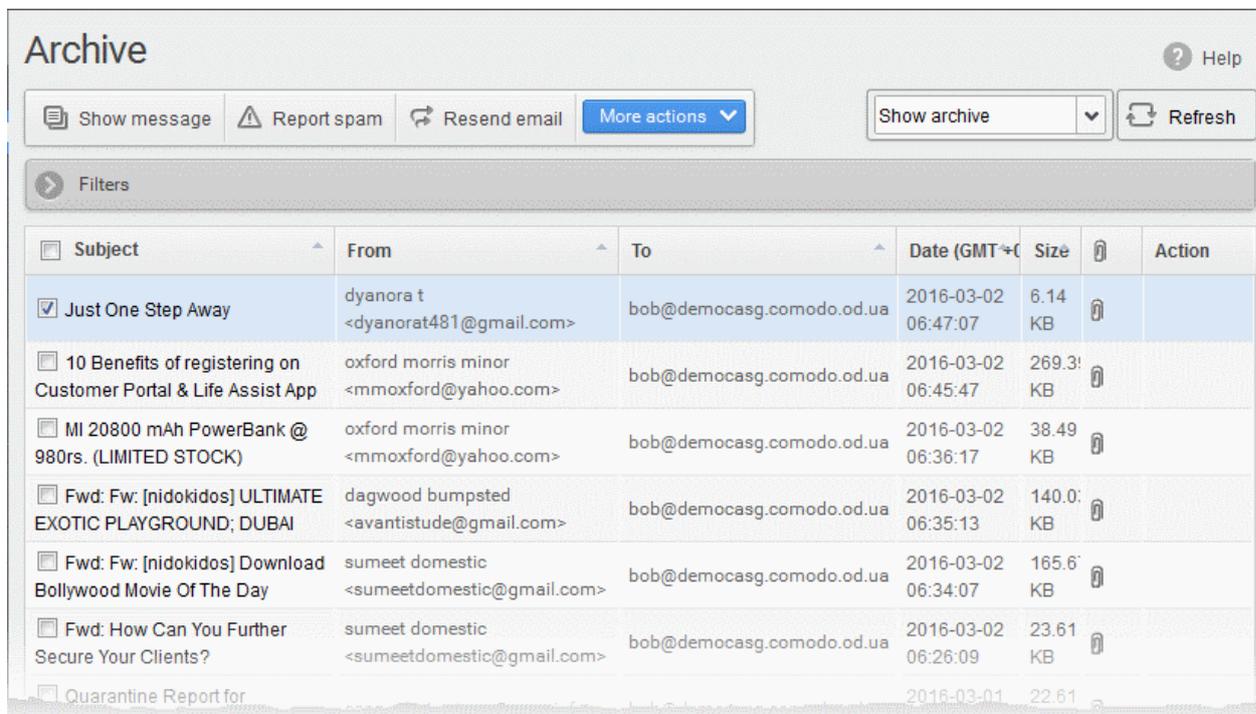
- The mail retention period is set by your administrator.
- The archive interface lets you view, reply and resend mail to yourself. You can also report spam from here.

#### Open the mail archive interface

- Click 'Incoming' on the left then choose 'Archive'



Your archived mails are shown as follows:



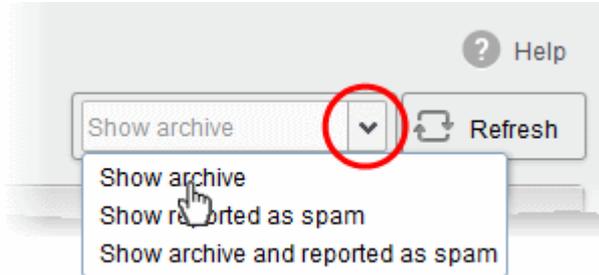
From this interface, you can:

- **View archived mails**
- **Resend selected mail to yourself**
- **Report spam mails**
- **Reply to a mail**
- **Forwarding archived emails**
- **Add senders to blacklist**

- **Add senders to whitelist**
- **Use 'Filters' to search for specific emails**

## Page Filter

The drop-down menu at top-right lets you filter archived mail by status:



- **Show archive:** Displays all non-spam archived mails
- **Show reported as spam:** Displays archived mail that you have marked as spam
- **Show archive and reported as spam:** Displays both spam and non-spam archived mails
- You can search for specific mails by using filters. See **Use 'Filters' to search archived emails** for more details.

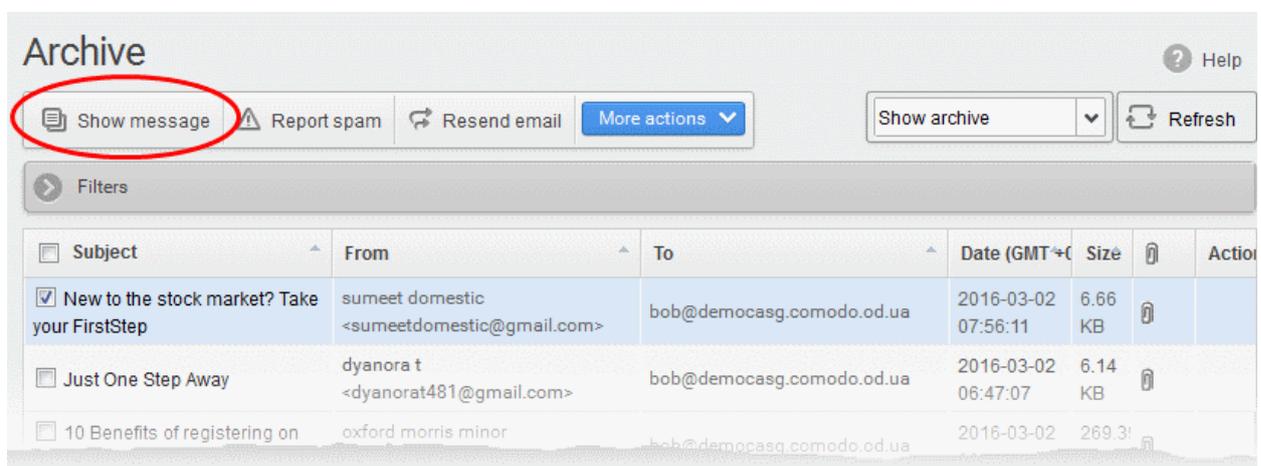
## View Archived Mails

There are two ways to view the content of archived mail:

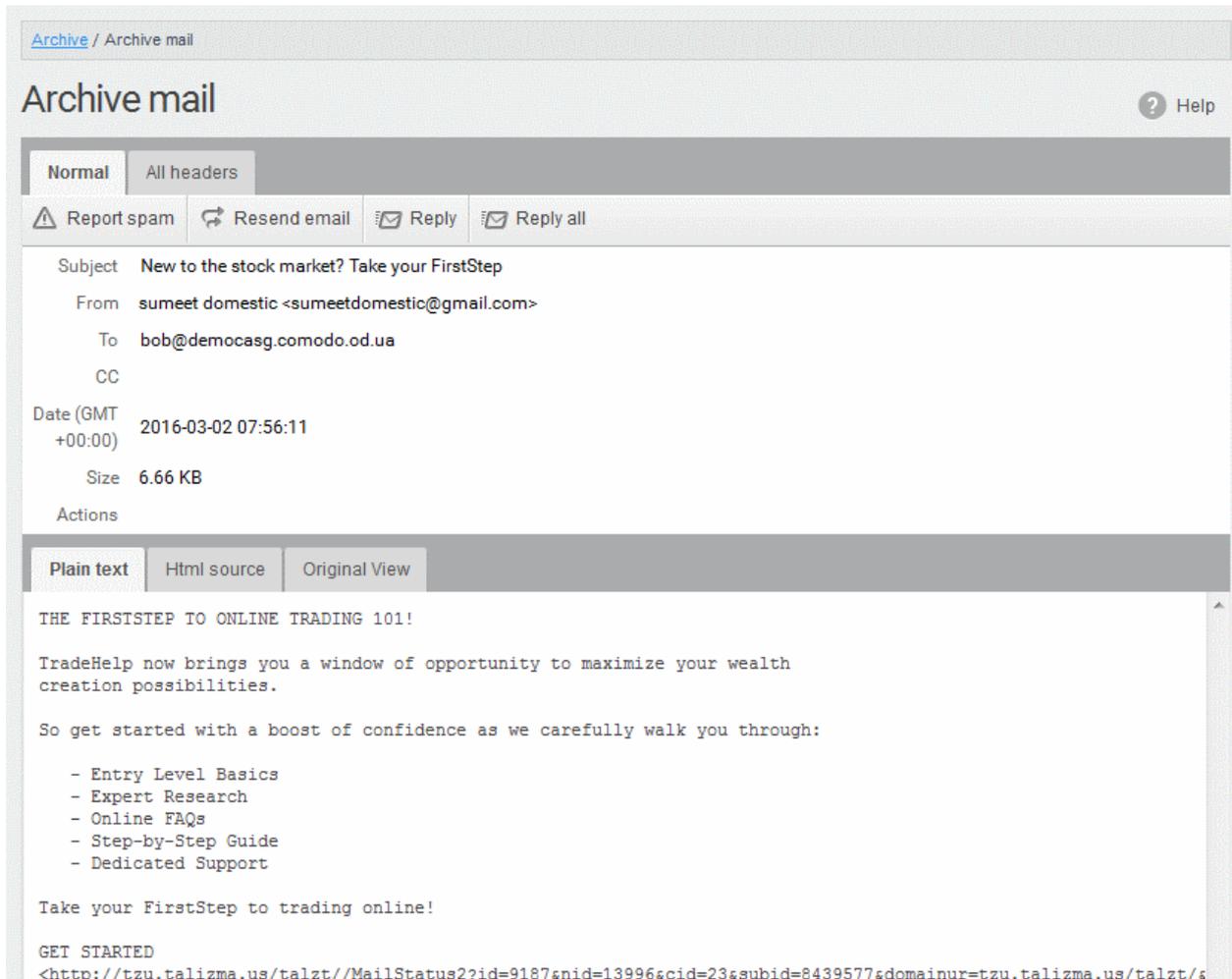
- **In the same CSEG window**
- **In a new CSEG window**

### View in the same CSEG window

- Select the mail in interface and click the 'Show Message' button.  
OR
- Click the email link in the subject column

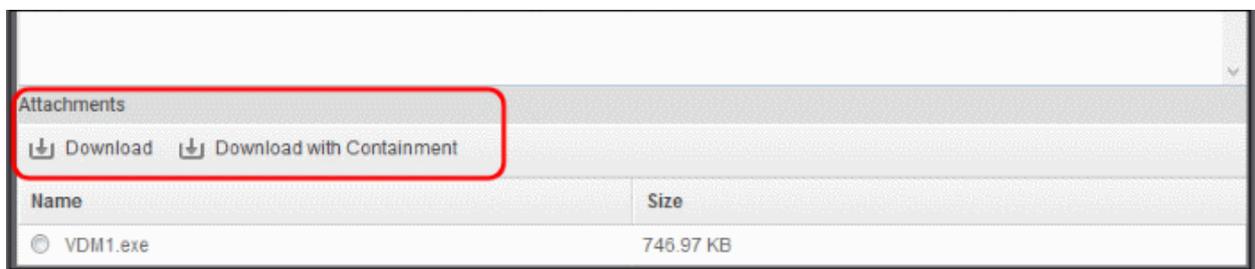


The selected mail opens:

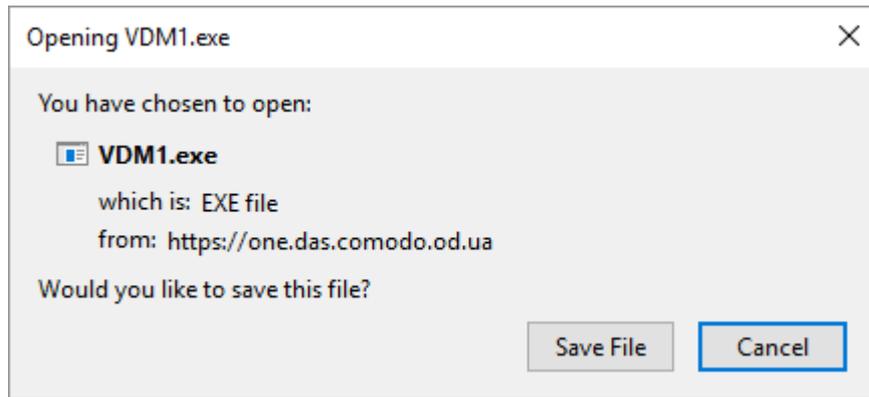


By default, the email opens in normal view and shown in plain text, where the images, banners and links are not displayed. Click 'Html source' to view the source code of the mail. To view images and links, click the 'Original View' tab.

- If there is an attachment, you can download it from this dialog.

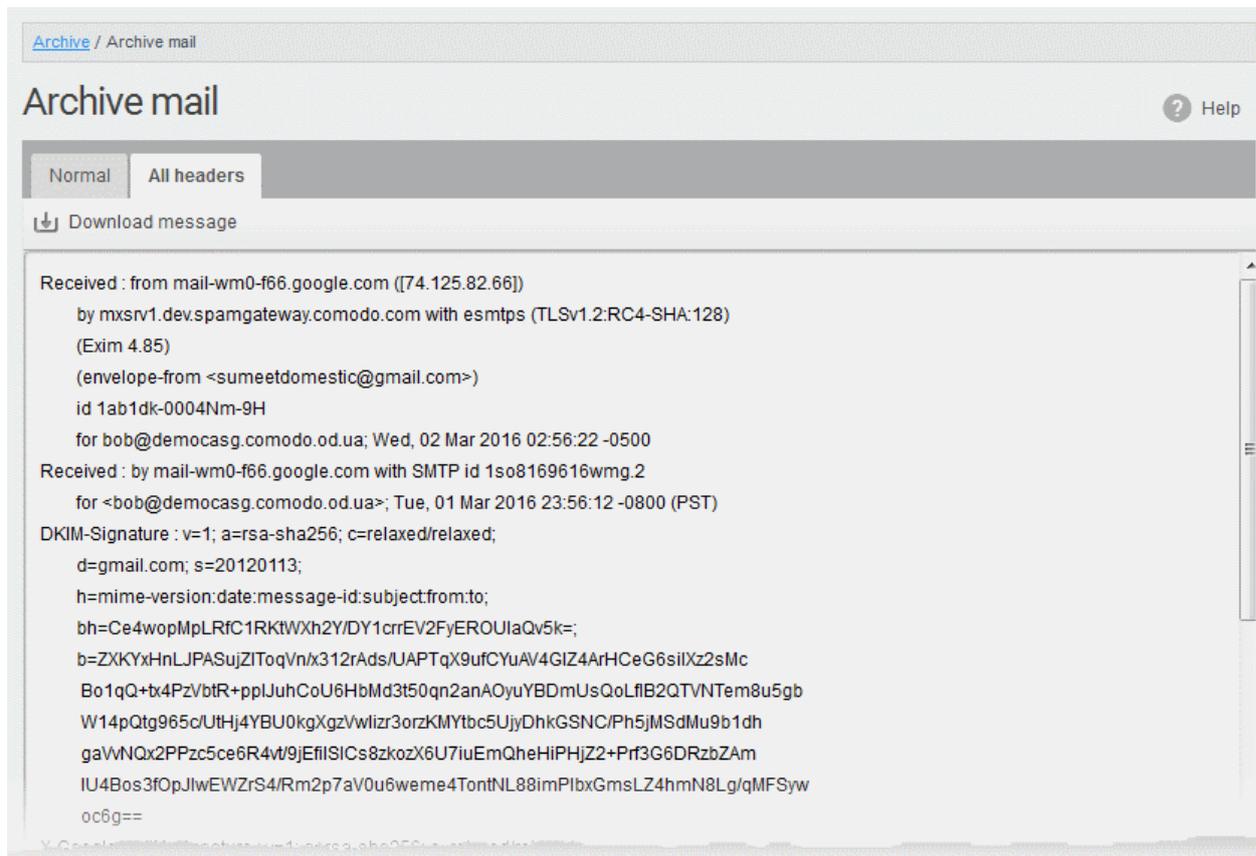


- Select the attachment and click 'Download' or 'Download with Containment'
    - Download – Save the original file.
    - Download with Containment – Containment is a technology whereby attachments with an 'unknown' trust rating are run inside a secure, sandbox environment. You can open and run the file as normal, but it is prevented from making potentially damaging changes to your computer.
- 'Download with containment' is only available if enabled by your administrator.



You can open the attachment with an appropriate application or save to a desired location in your computer.

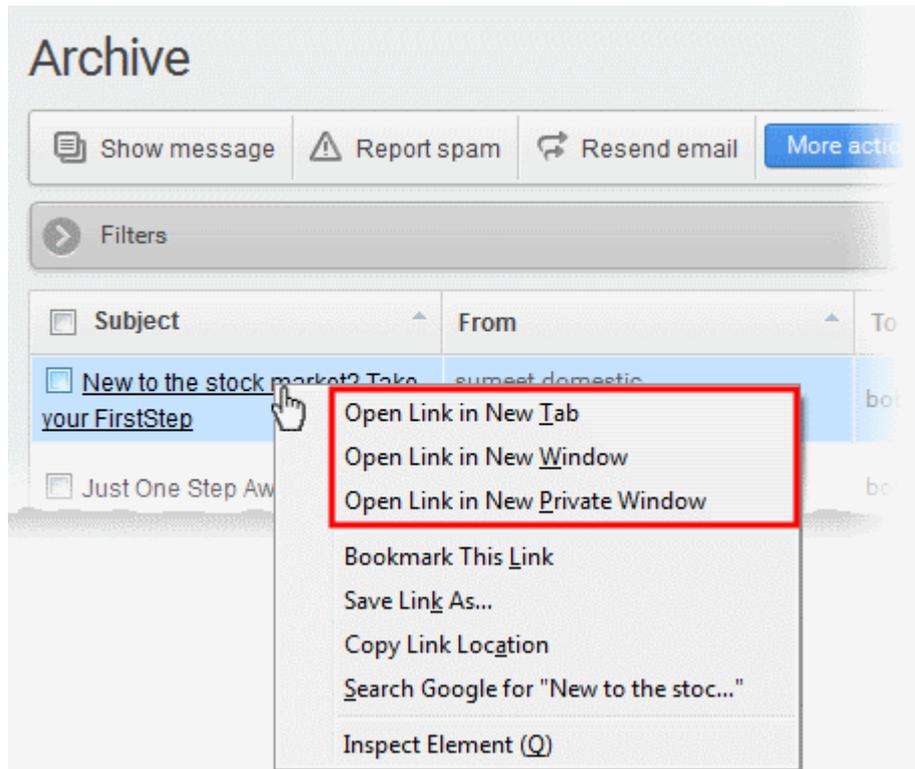
- **'All headers' tab** – Email headers contain information about the route taken by the mail before it reached your mailbox. This lets you check the authenticity of the mail:



- To save the email as a HTML file, click 'Download' message.

### View archived mail in a new window

- Right-click on the subject line of the mail you want to view
- Choose whether to open in a new tab, new window, or new private window:



- Your browser may display a pop-up warning.
- Click 'Options'> then select 'Allow pop-ups for...' to allow the message to open in a new window.
- Click 'Show message in new window' again.

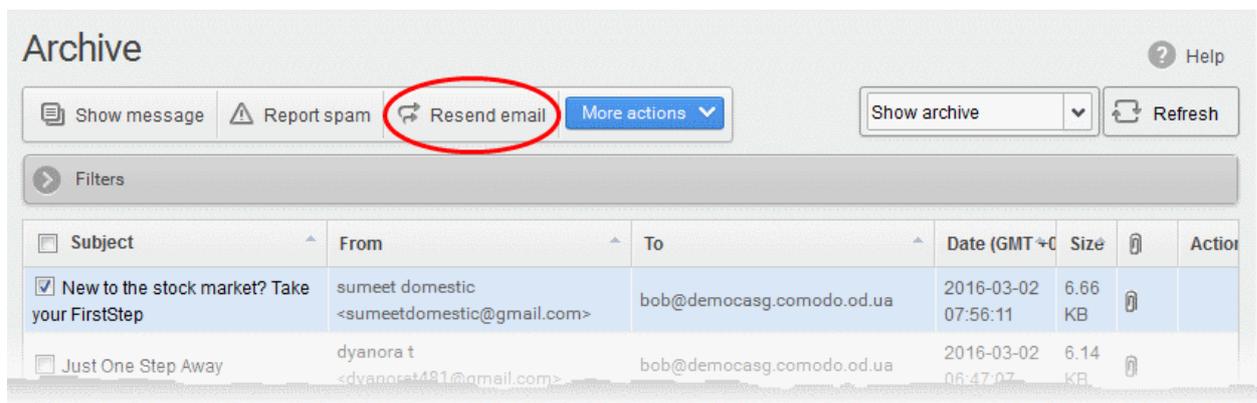


## Resend mails from Archive to your inbox

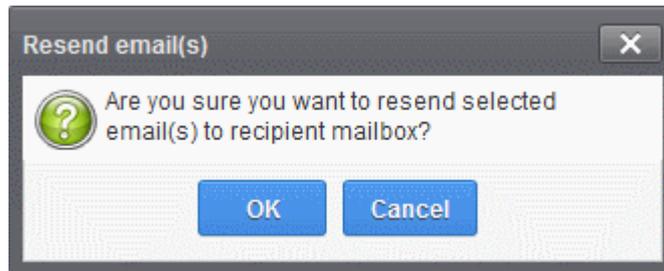
The 'Archive' interface lets you to re-send selected mails to yourself so that you can access them from your mail client. This is useful if you want to recover mails that you have deleted.

### Resend a mail

- Select mail(s) from and click the 'Resend' email button:



A confirmation dialog is shown:



- Click 'OK' to receive the mail(s) at your mail box

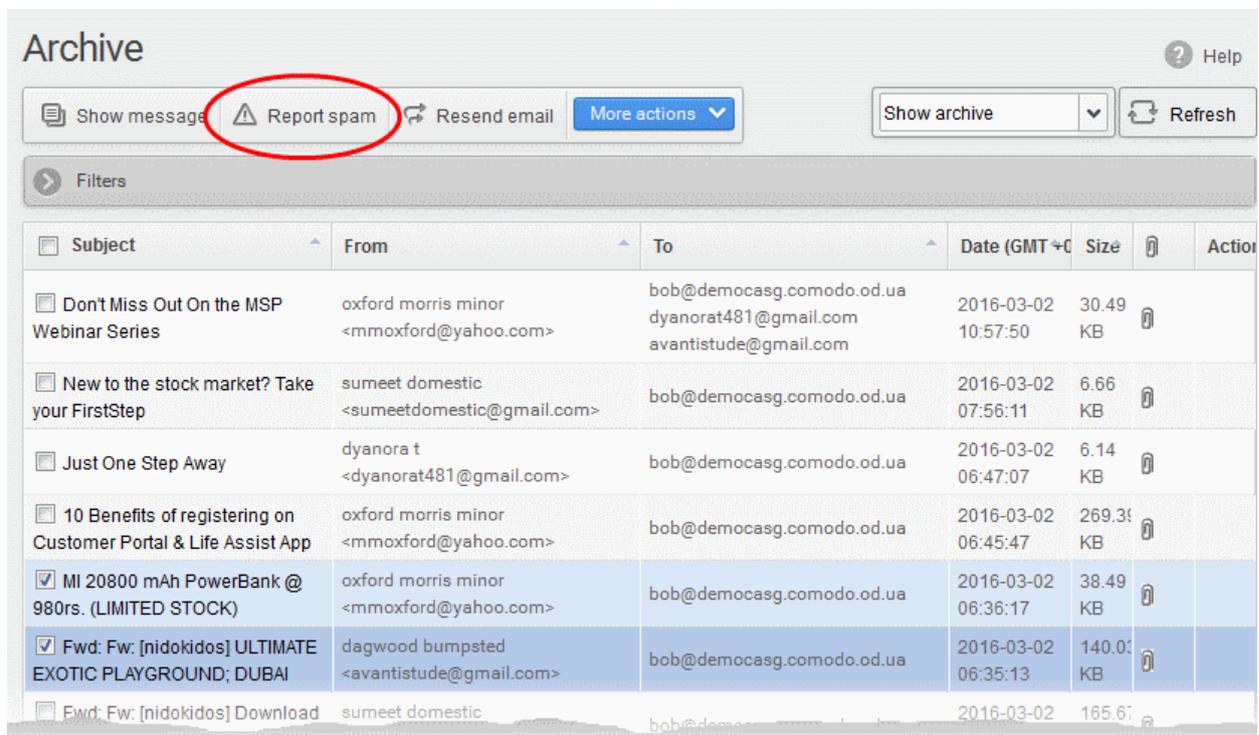
CSEG will only resend the mail to your mailbox, and not to any other recipients in the 'To', 'CC' and 'BCC' fields of the emails.

### Report spam from the archived mails

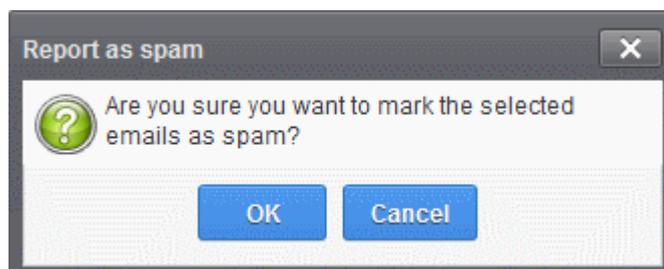
You can submit mails that you suspect are spam to Comodo for analysis. We will analyze reported mails and, if we confirm them as spam, will update our filters to quarantine similar mails in future.

### Report spam emails

- Select the mail(s) to be submitted as spam, from the 'Archive' interface and click the 'Report Spam' button from the top



A confirmation dialog is shown:



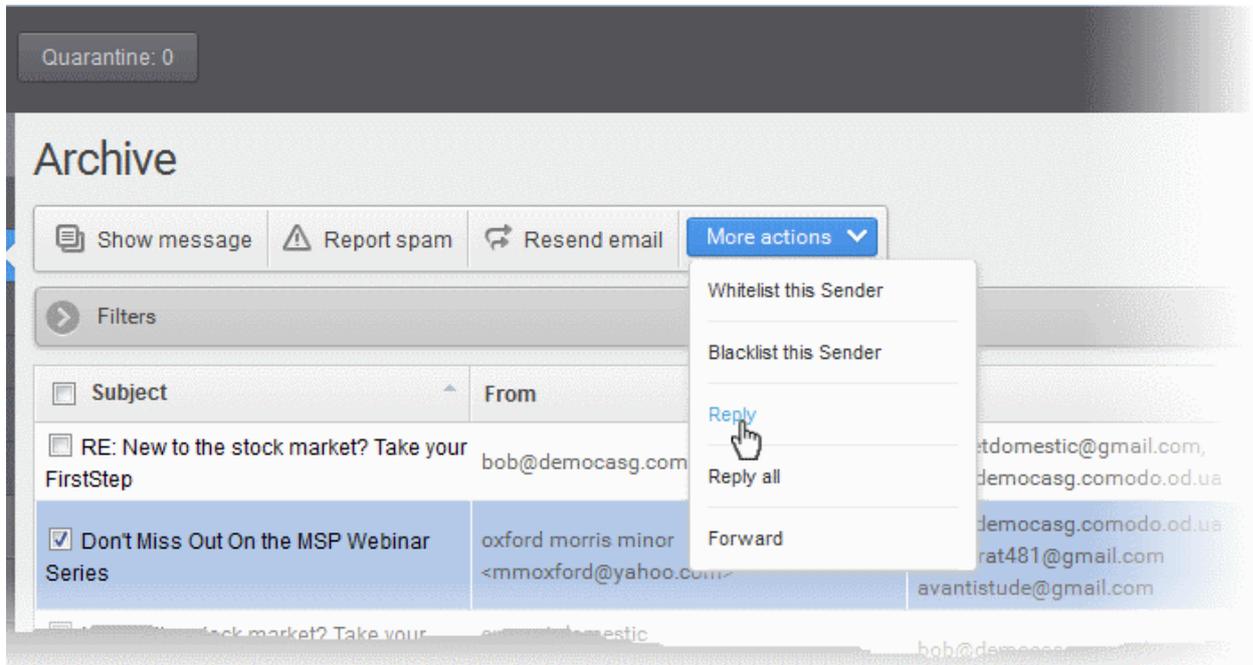
- Click 'OK' to upload the mails for analysis

## Reply to Mails from Archive

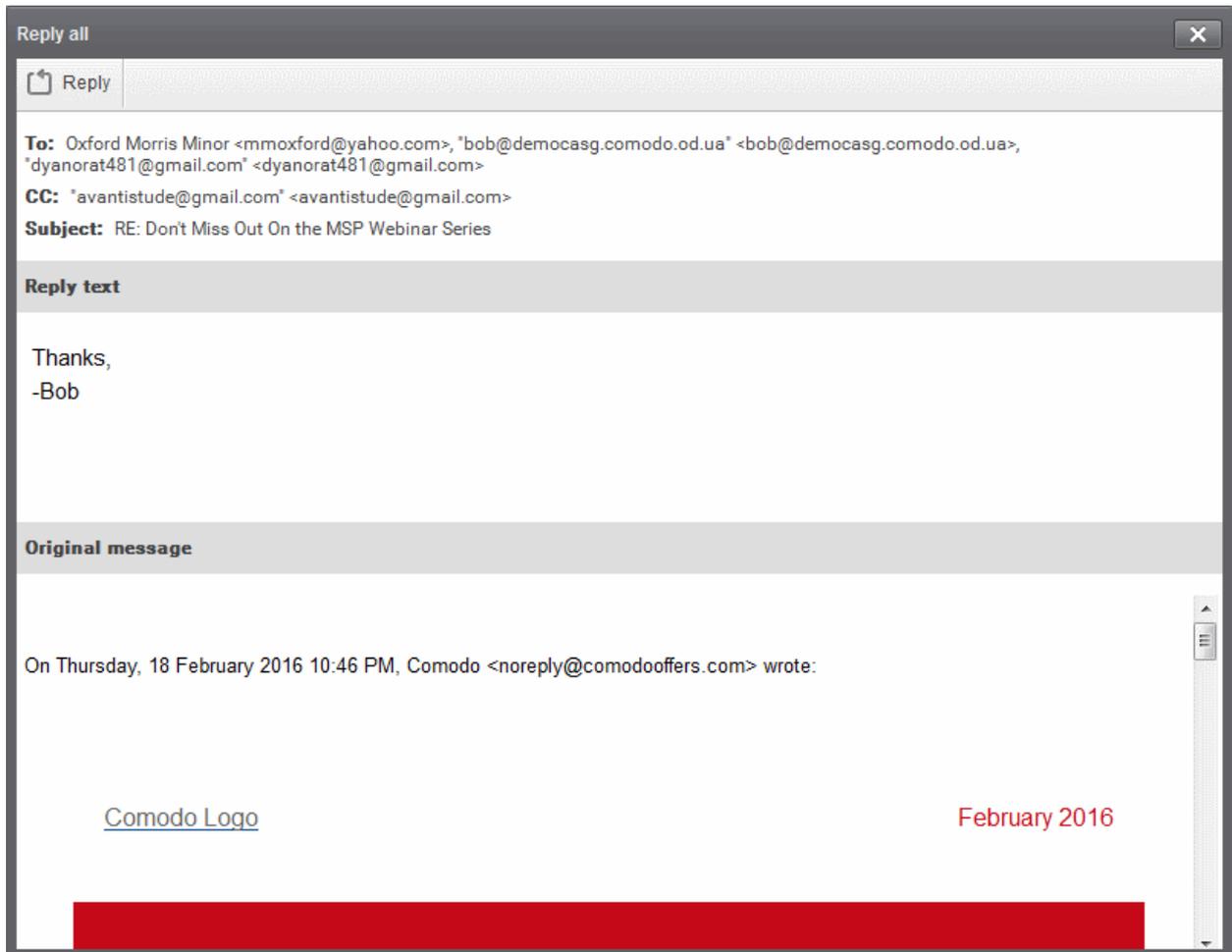
You can send replies to archived mails. This is useful if you have accidentally deleted a mail from your mail box but wish to send a reply to the sender. You can also choose to send the reply only to the sender or to all for which the email was addressed.

### Send a reply to a mail from archive

- Select the mail from the 'Archive' interface
- Click 'More actions' and choose the reply option
  - Reply - The reply mail is sent only to the sender email address
  - Reply all - The reply mail is sent to all email addresses in the 'To' and 'CC' fields of the selected mail

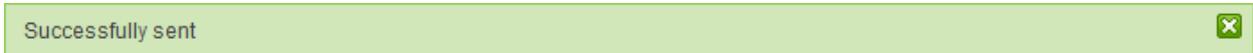


The Reply/Reply all interface opens:



- Enter your reply message in the 'Reply text' field and click Reply from the top left

The message is sent to the selected email addresses.

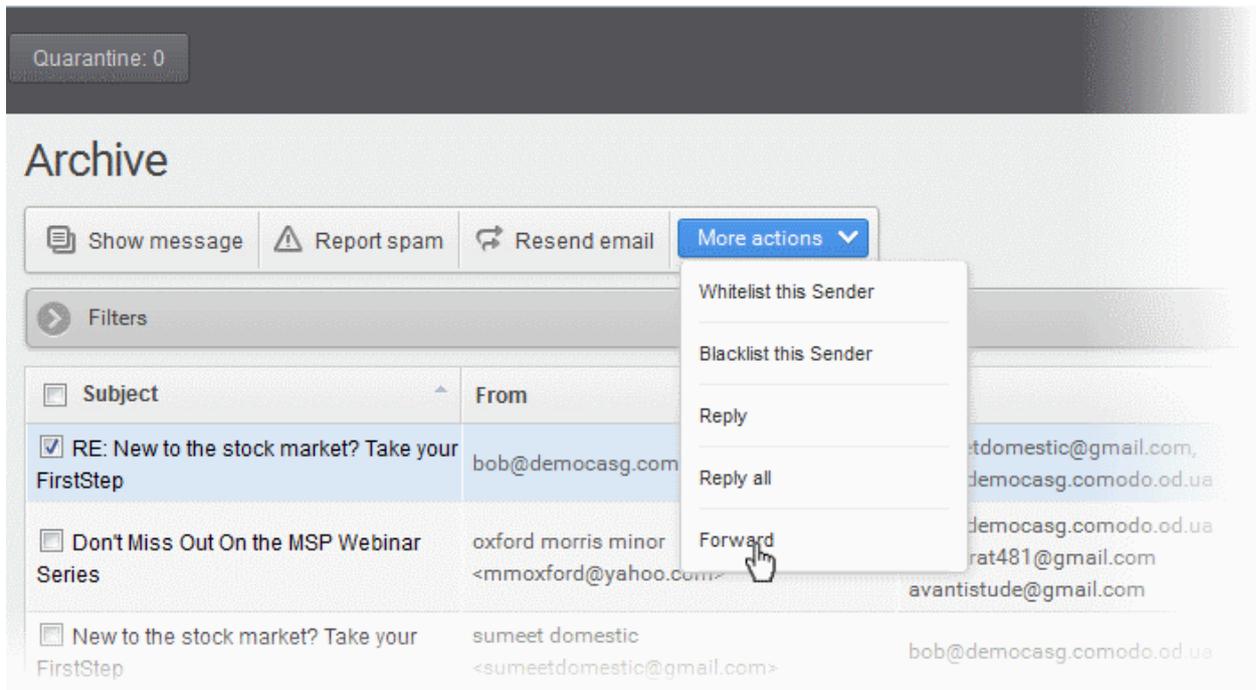


## Forward archived emails

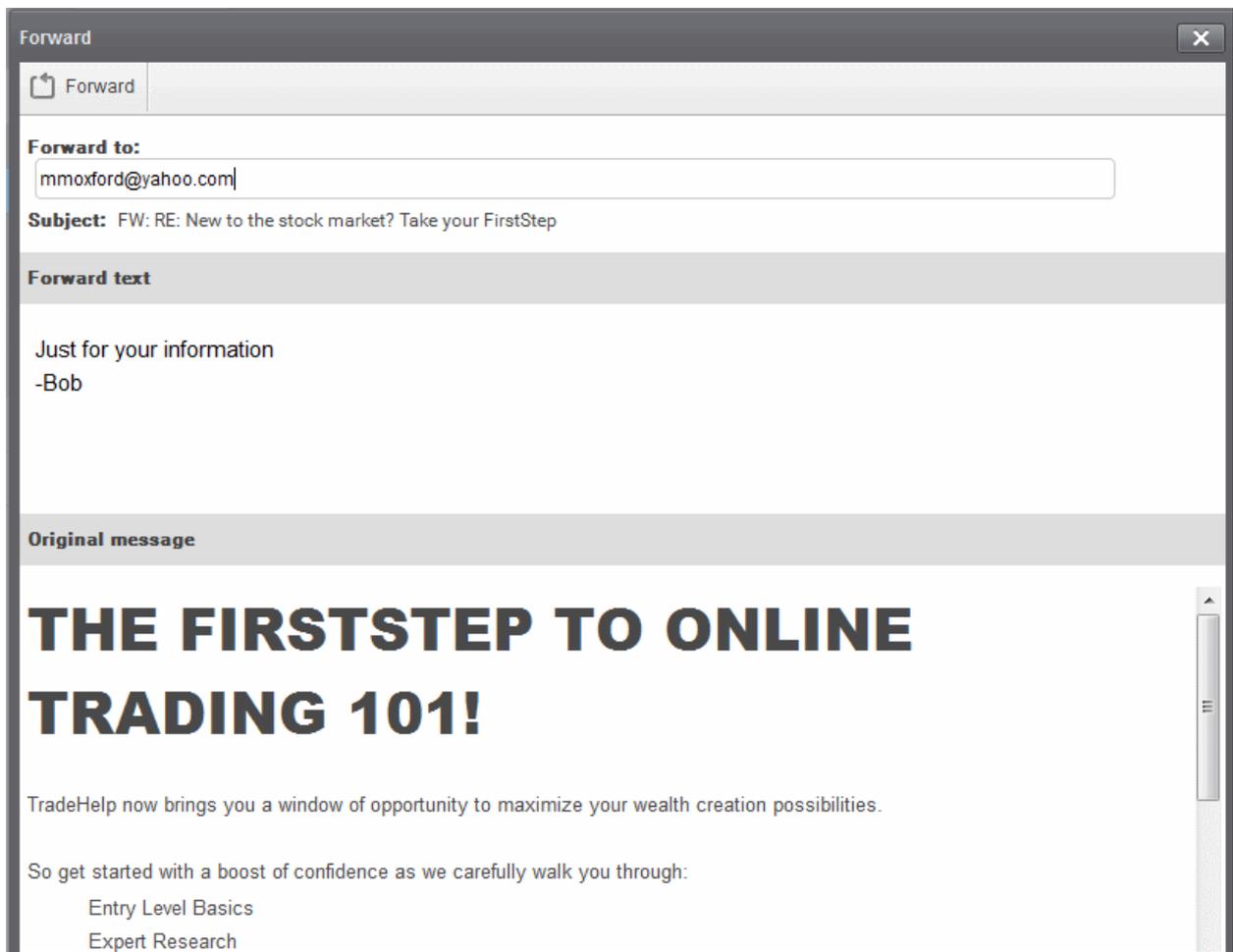
You can forward mails from your archive to different mail addresses. This is useful if you want to share an email with other people or to send the mail to your alternative email address.

### Forward a mail from archive

- Select the mail from the Archive interface
- Click 'More actions' and choose 'Forward'



The 'Forward' interface opens:



- Enter your forward message in the 'Forward text' field, enter the email address to which the mail has to be forwarded and click 'Forward' from the top left

The message is sent to the entered email addresses.

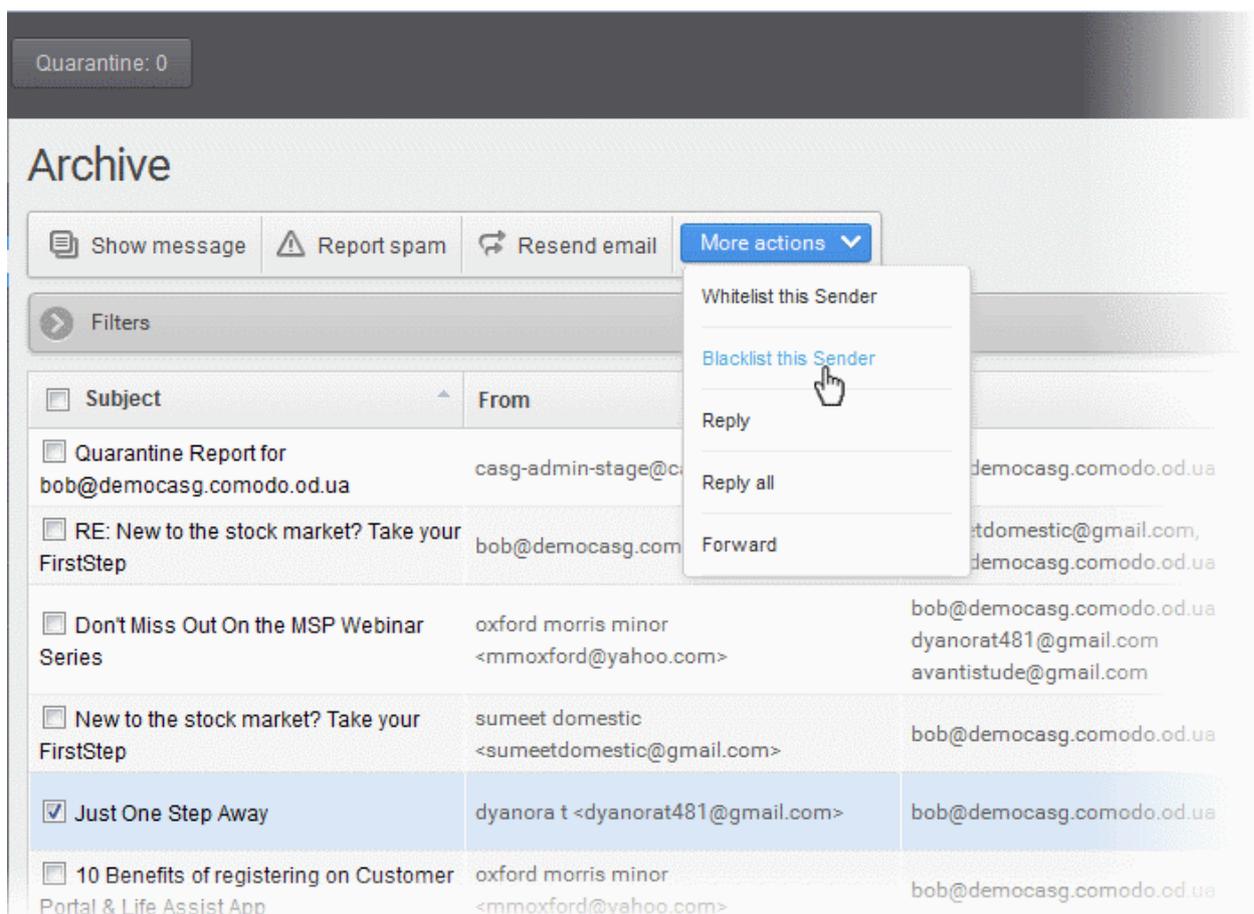
Successfully sent ✕

## Add senders to blacklist

To stop receiving emails from a specific senders whose mails are available in the archive, you can request the administrator to add those senders to blacklist.

**Note:** Depending on the permission level configured for your email account by your administrator, the button for adding senders to blacklist is either 'Blacklist this Sender' or 'Request blacklist' in the 'More actions' drop-down button. If the interface displays 'Blacklist this Sender' button, you can add the sender to blacklist without approval from your administrator.

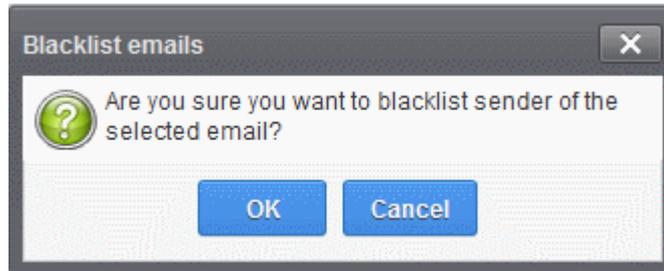
- Select the mail that you want its sender to be added to blacklist and click 'More actions' > 'Request Blacklist' or 'Blacklist this sender'.



Upon request to the administrator, an email notification is sent to your administrator with a copy to you. This request is also displayed in the 'Action' column of the 'Archive' interface. If the administrator accepts the request, the sender is added to blacklist and you will no longer receive any mail from that sender. If the request is rejected, the 'Blacklist this Sender' icon in the 'Action' column is no longer displayed.

- If you want to call off the request before the administrator accepting it, choose the mail, click 'More actions' and choose 'Cancel request'.

If the administrator has provided the permission to blacklist a sender without approval, a confirmation dialog is displayed on clicking 'Blacklist this Sender'.



- Click 'OK' for confirmation

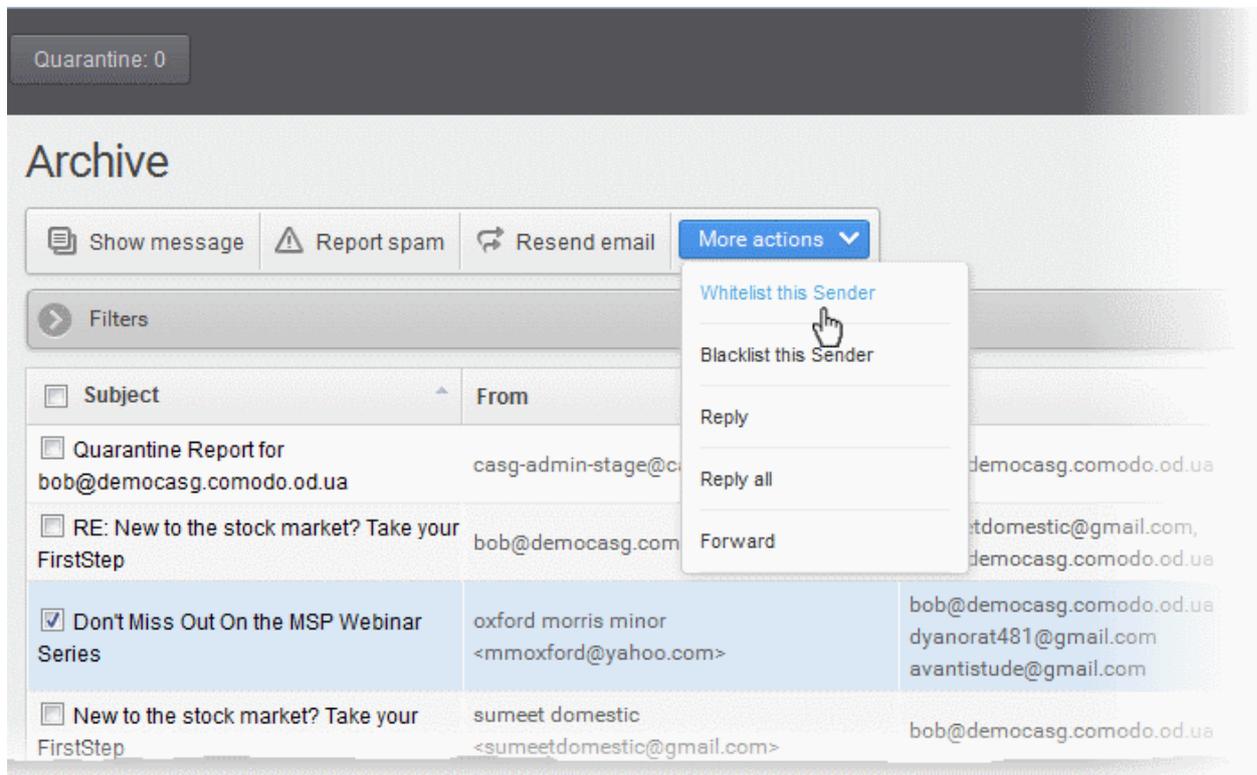
Senders added to blacklist are displayed in the Manage blacklist senders interface. See [Managing Blacklisted Senders](#) for more details.

## Add senders to whitelist

You can add authenticated senders to whitelist from the archive interface, so that the mails from those senders are not subjected to security checks.

**Note:** Depending on the permission level configured for your email account by your administrator, the button for adding senders to whitelist is either 'Whitelist this Sender' or 'Request whitelist' in the 'More actions' drop-down button. If the interface displays 'Whitelist this Sender' button, you can add the sender to whitelist without approval from your administrator.

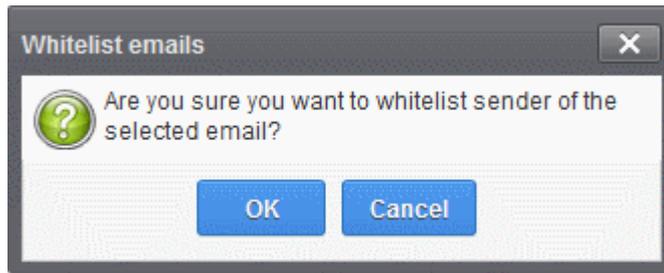
- Select the mail that you want its sender to be added to whitelist and click 'More actions' > 'Request Whitelist' or 'Whitelist Sender'.



Upon request to the administrator, an email notification is sent to your administrator with a copy to you. This request is also displayed in the 'Action' column of the 'Archive' interface. If the administrator accepts the request, the sender is added to whitelist and the mails from them will bypass security checks. If the request is rejected, the 'Whitelist this Sender' icon in the Action column is no longer displayed.

- Senders added to whitelist are displayed in the 'Manage whitelist senders' interface. See [Managing Whitelisted Senders](#) for more details.
- If you want to cancel the request before the administrator accepting it, choose the mail, click More actions and choose 'Cancel request'.

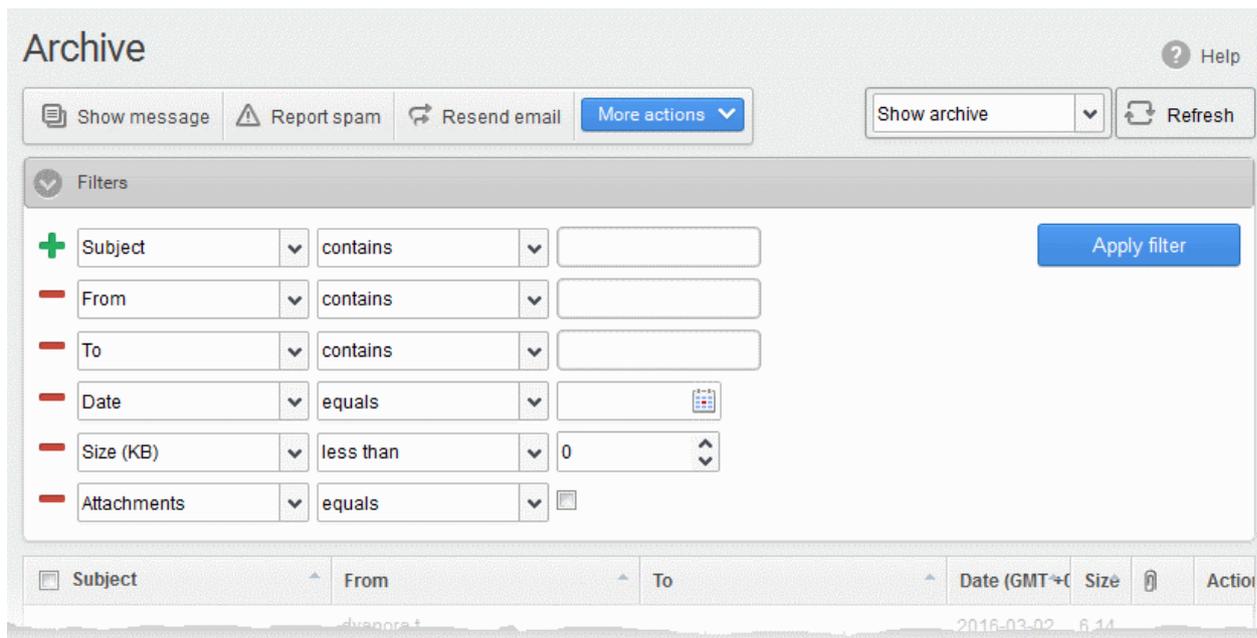
If the administrator has provided the permission to whitelist a sender without approval, a confirmation dialog is displayed on clicking 'Whitelist this Sender'.



- Click 'OK' for confirmation

## Use 'Filters' to search archived emails

- Click anywhere on the 'Filters' stripe to open (or close) the filters area.



- Choose the filter by which you want to search from the first drop-down, then a condition in the 2<sup>nd</sup> text box. Some filters have a third box for you to type a search string.
- Click 'Apply Filter'.

You can filter results by the following parameters:

- **Subject:** Type the email subject in the text box (column 3) and select a condition in column 2.
- **From:** Enter the sender name or address in the text box (column 3) and select a condition in column 2.
- **To:** Enter the recipient name or address in the text box (column 3) and select a condition in column 2.
- **Date:** Search by date and time mails archived. Select the date (column 3) and select a condition in column 2.
- **Size (KB):** Search archived mails by their size. Select or enter the mail size in column 3 and select a condition in column 2.
- **Attachments:** Enable or disable the checkbox (column 3) and select the condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

## 3.2.1.3 Report Spam

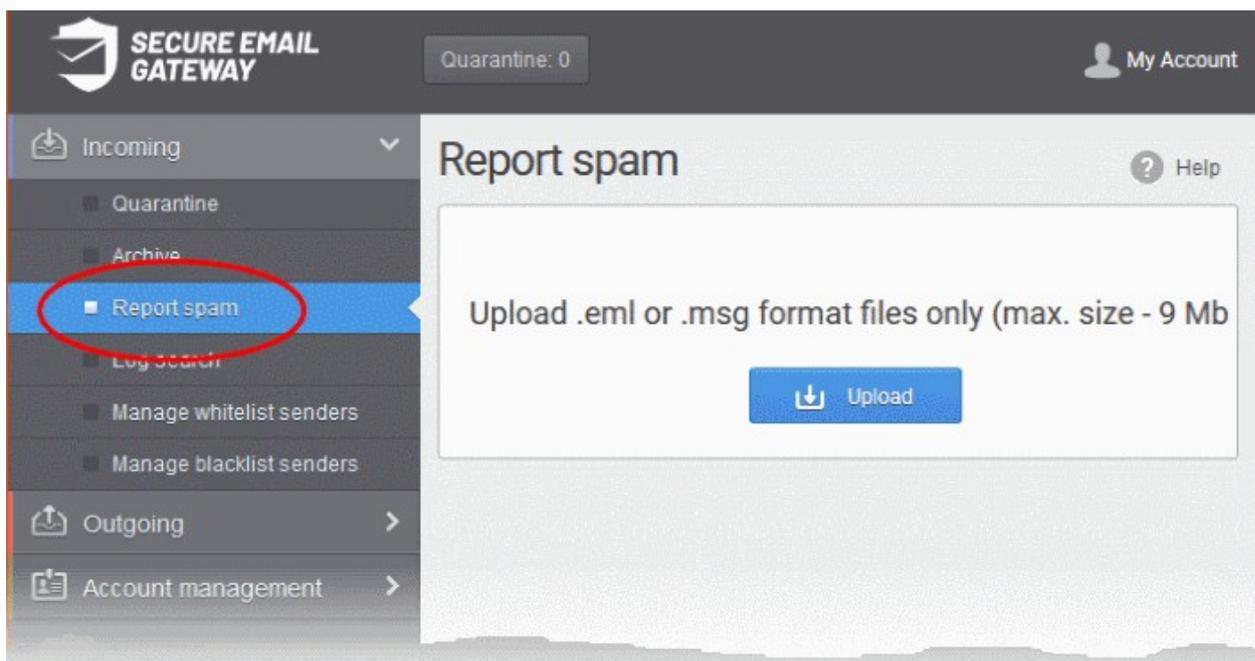
The 'Report Spam' feature lets you to upload and submit suspected junk emails that have got through our spam filters. Comodo will analyze reported mails and, if we confirm them as spam, will update our filters to quarantine similar mails in future. CSEG accepts a range of different mail formats including .eml and .msg.

Users can also report spam by sending it to [spam@antispamgateway.comodo.com](mailto:spam@antispamgateway.comodo.com). Add the spam email as an attachment in .eml or .msg format.

**Note:** The administrator of your email account should have enabled this feature for you. If enabled, the 'Report spam' sub-tab is available on the left under the 'Incoming' tab.

### Report a spam mail

- Click 'Incoming' on the left then choose 'Report spam'

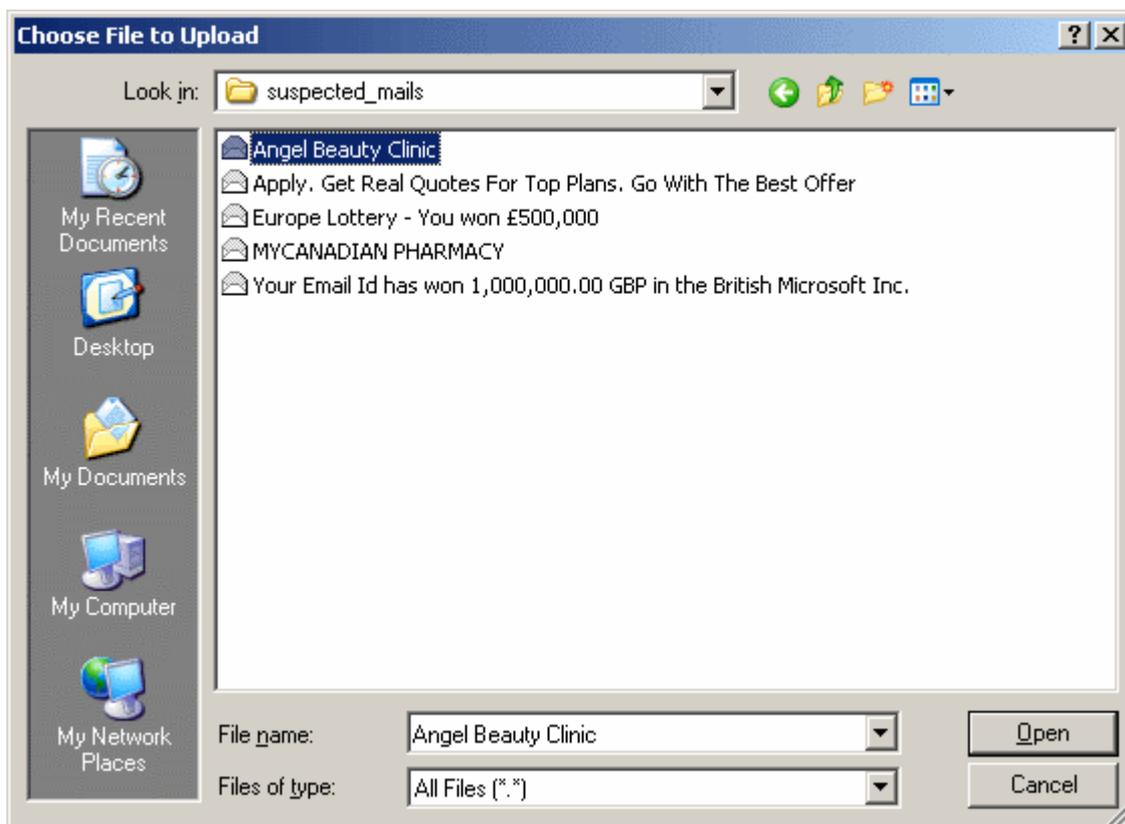


The 'Report Spam' interface opens:

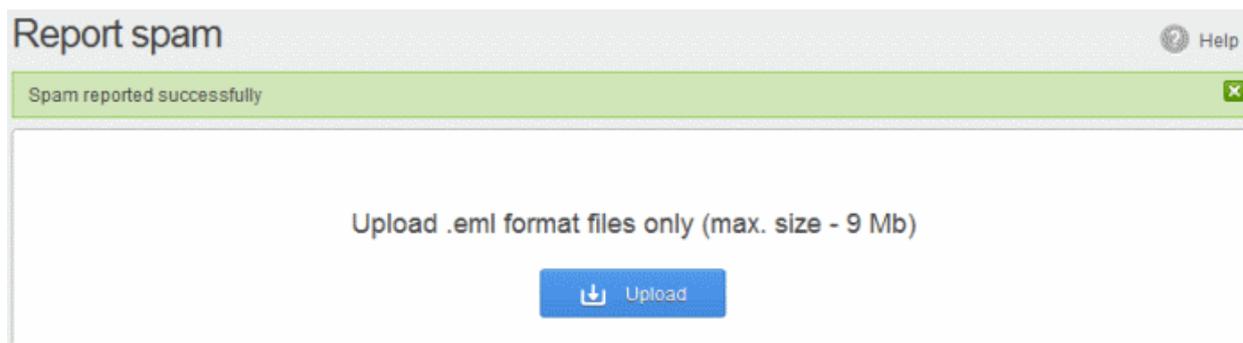
- Click the 'Upload' button.
- Navigate to the location where the suspected email(s) is/are stored on your system. Select the mail that you want to report as spam and click 'Open'. The maximum size of the file that can be uploaded is 9 MB.

**Note:** The files should be email format (with .eml extension) and its size should not exceed 9 MB. The following error message will be displayed if any of the above is not complied with.

Perhaps the body of the file is damaged or it is not \*.eml format or it size greater than 9Mb (outgoing\_users.csv) ✕



The mail is processed for uploading and success message is shown after the process is completed.



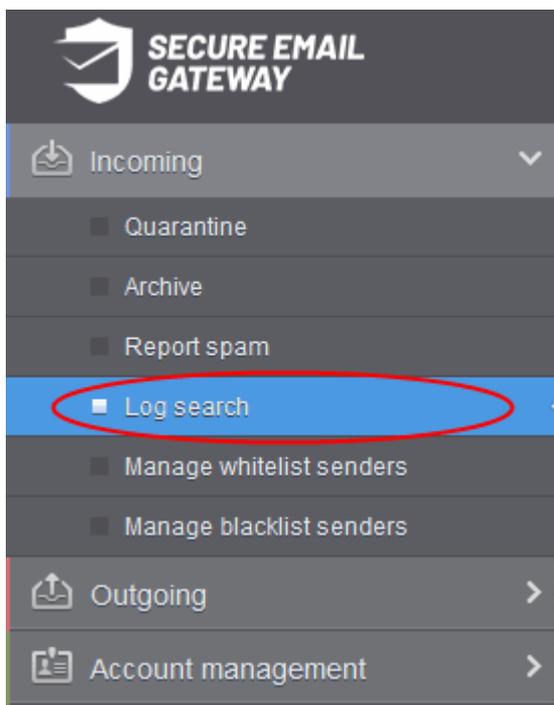
### 3.2.1.4 Log Search

- The 'Log search' area lets you search for specific email messages. You can modify your search according to multiple criteria, including date range, sender, recipient and IP address.

**Note:** The administrator of your email account should have enabled this feature for you. If enabled, the 'Log search' will be available on the left under 'Incoming'.

#### Search your incoming emails in logs

- Click 'Incoming' on the left then click 'Log search'.



The 'Log search (incoming)' interface opens:

The screenshot shows the 'Log search (incoming)' interface. At the top right is a 'Help' button. The main search area contains the following fields:

- Date range:** Two date pickers showing '2017-11-13 10:20:46' and '2017-11-14 10:20:46'.
- Message ID:** An empty text input field.
- Sender:** An empty text input field.
- Recipient:** A text input field containing 'jones' and '@demo.das.comodo.od.ua'.
- Sender IP:** An empty text input field.
- Sender host:** An empty text input field.

Below the fields is a checkbox labeled 'Include results from the last minutes:' which is currently unchecked. At the bottom center is a blue 'Search' button.

- **Date range:** The date range for which you want to search the log file.
- **Message ID:** A unique message identifier (*optional*).
- **Sender:** The sender email address in this field.
- **Recipient:** The currently logged in user name will be displayed in this field.
- **Sender IP:** The IP address of the sender.
- **Sender Host:** The sender host name.
- **Include results from the last minutes:** If selected, CSEG will include messages that are currently being migrated from the filtering server to the logging server in the search results.

The option "Include results from the last minutes" will slow down the search result retrieval

- Click the 'Search' button.

CSEG will search for the entered terms and display the results.

Date and time	Host (Exim id)	Sender hostname	Sender	Recipient	Subject	Classification
2014-10-29 14:53:43	mxsrv3.spamgat 1XjUd0-0006V6-1	mxsrv3.spamgat 178.33.199.69	admin@csg.com	john	demo spam email 1	Rejected External pattern match
2014-10-29 14:45:07	mxsrv2.spamgat 1XjUUF- 0001RZ-B8	mxsrv2.spamgat 178.33.199.66	demo@csg.com	john	Spam email 1	Rejected Rejected by relay restriction for this recipient
2014-10-29 14:44:59	mxsrv1.spamgat 1XjUUX- 0006NV-Bj	mxsrv2.spamgat 178.33.199.66	demo@csg.com	john	Spam email 2	Rejected Rejected by relay restriction for this recipient

1 / 1 [ 1 - 3 / 3 ] Per page 15

### 3.2.1.5 Manage Whitelist Senders

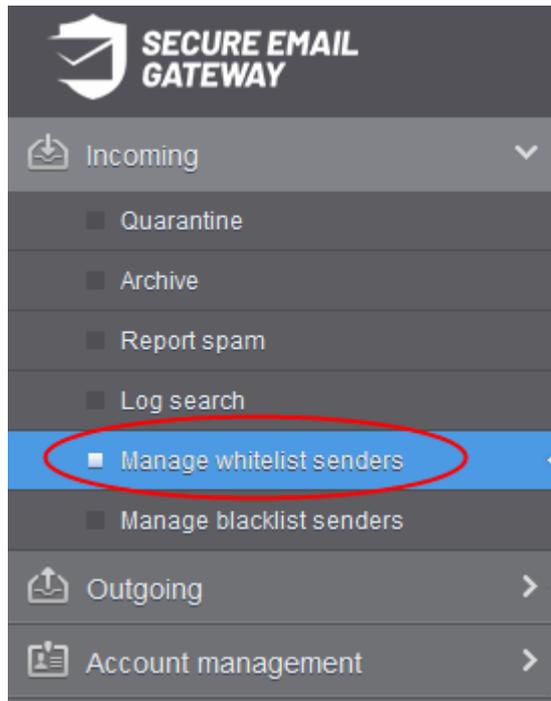
CSEG allows you to define a whitelist of senders on a per user basis.

- All filtering checks are disabled for whitelisted senders.
- Comodo recommends you use this option only if you are certain that the sender is trustworthy.
- You can add senders to the whitelist from both the 'Quarantine' and 'Manage Whitelisted Senders' interfaces.
- In either case, you can only add senders if you have the correct permissions to do so. If you do not have the permissions, please contact your administrator to add senders to the whitelist.

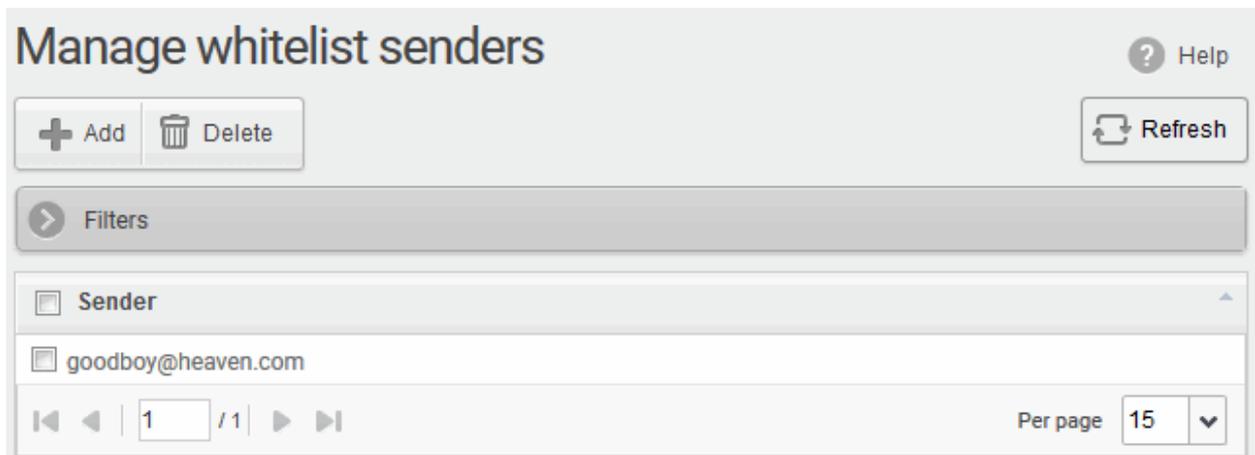
This section explains how to whitelist senders using the 'Manage Whitelisted Senders' interface.

#### Manage whitelist senders

- Click 'Incoming' on the left and choose 'Manage whitelist senders'



Whitelisted senders for your mail account are listed:

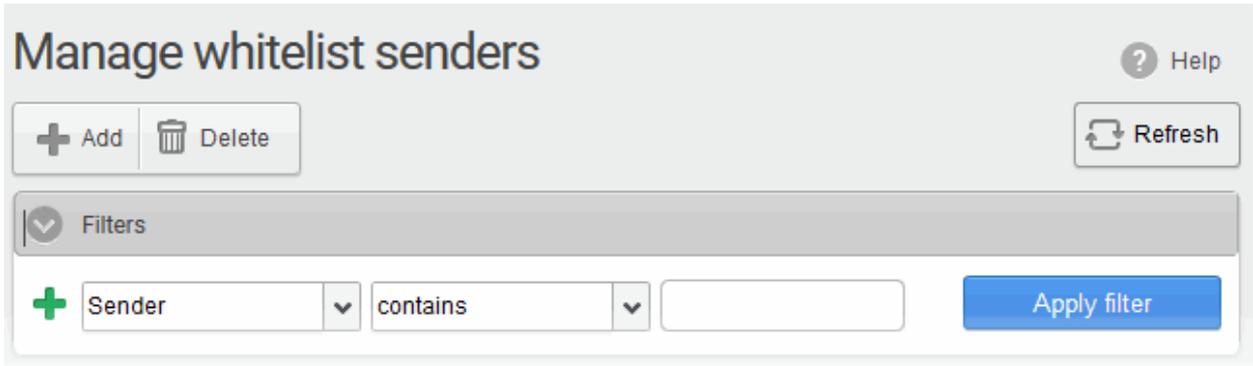


From this interface you can:

- **Add senders to whitelist manually**
- **Remove senders from whitelist**

**Note:** The 'Add' and 'Delete' buttons are available only if the administrator of your account has enabled this for you. If this is not enabled, you can just view the whitelisted senders in this interface.

- Click the 'Sender' header to sort the entries in ascending or descending order of senders' names.
- Click anywhere on the 'Filters' stripe to open (or close) the filters area.



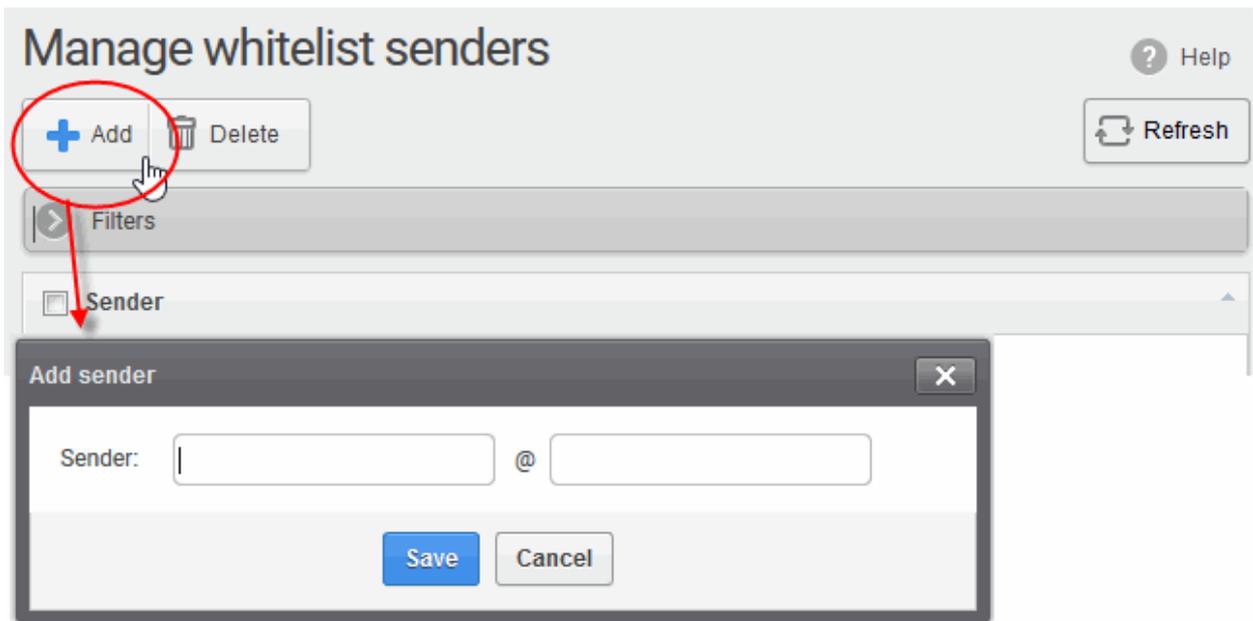
- You can filter results by sender
    - Sender:** Type a sender's mail address in the text box (column 3) and select a condition in column 2.
- Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

You can add multiple filters to the same search by clicking .

### Manually add senders to whitelist

- Click the 'Add' button at the top.

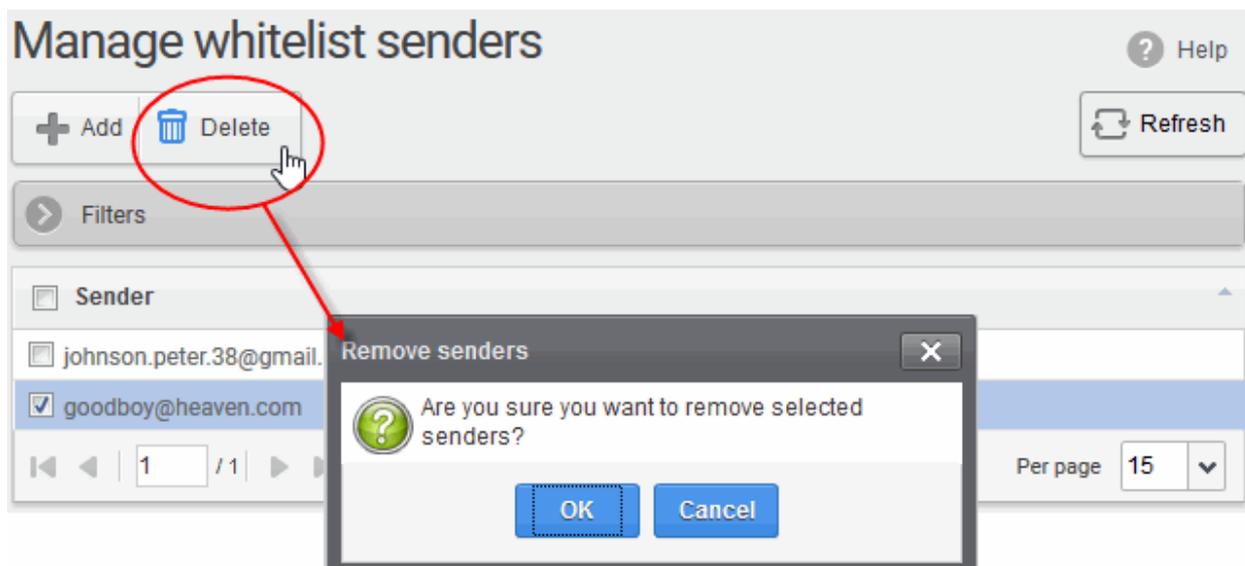
The 'Add sender' dialog opens:



- Enter the sender's username in the first text box and sender's email domain name in the second text box after the @ symbol.
- Click the 'Save' button. Repeat the process to add more senders to whitelist.

### Remove senders from whitelist

- Select the sender(s) from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.

### 3.2.1.6 Manage Blacklisted Senders

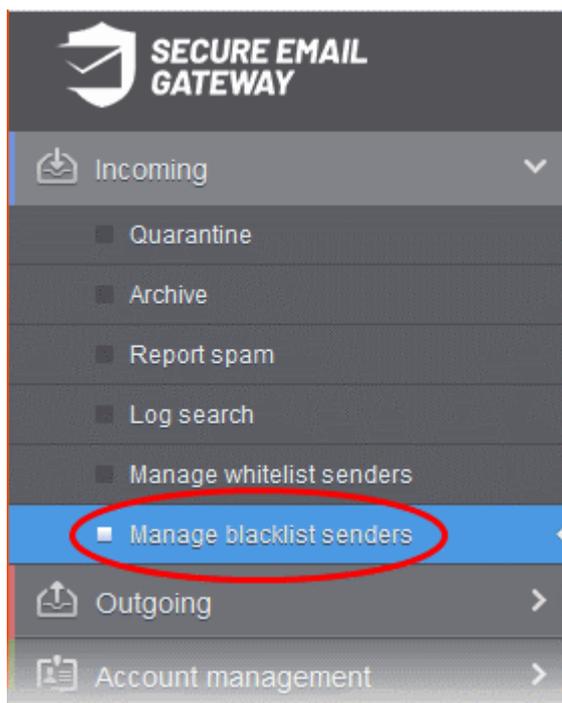
- CSEG allows you to blacklist senders who frequently send you unsolicited emails
- The sender will be blocked only for you and not for other users in the domain.
- The messages from blacklisted senders will not be quarantined.
- The sending SMTP server will send a 'bounce' message to the sender.

You can add senders to blacklist in three ways:

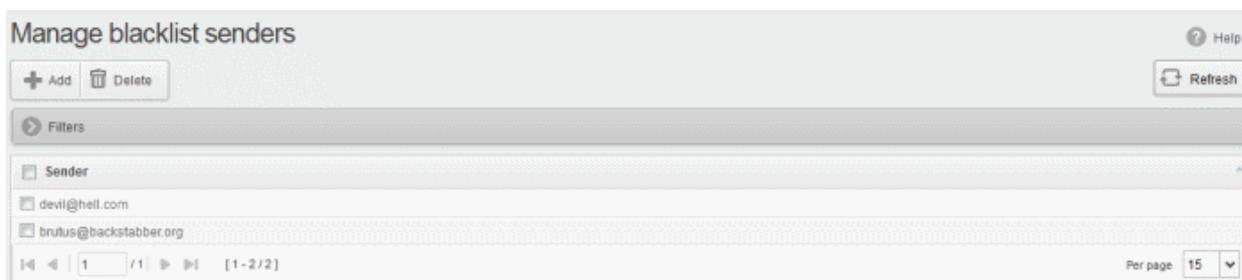
- From the '**Quarantine**' interface - You can send requests to your administrator to blacklist senders by selecting the mails sent by them but added to the quarantine. See the **Quarantine** section for more details.
- From the '**Archive**' interface - You can send requests to your administrator to blacklist senders by selecting mails sent by them, from the 'Archive' interface. See the **Mail Archive** section for more details.
- From the 'Manage whitelist senders' interface - You can manually add or or remove senders to blacklist if your administrator has granted you sufficient permissions.
- The reminder of this section contains more details on the items above.

#### Manage blacklisted senders

- Click 'Incoming' on the left then select 'Manage blacklist senders'



The 'Manage blacklist senders' interface is shown with a list of senders blacklisted for your mail account.



From this interface users can:

- **Add senders to blacklist manually**
- **Remove senders from blacklist**

**Note:** The 'Add' and 'Delete' buttons are available only if the administrator of your account has enabled this for you. If this is not enabled, you can just view the blacklisted senders in this interface.

- Click on the 'Sender' column header to sort the entries in ascending or descending order of sender names.
- Click anywhere on the 'Filters' tab to open (or close) the filters area.



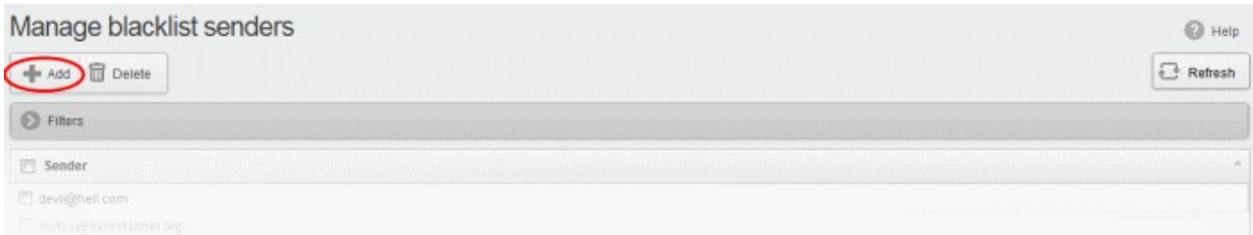
- You can filter results by sender
  - **Sender:** Type a sender's mail address in the text box (column 3) and select a condition in column 2.

Click anywhere on the 'Filters' tab to close the filters area. Click the 'Refresh' button to remove filters.

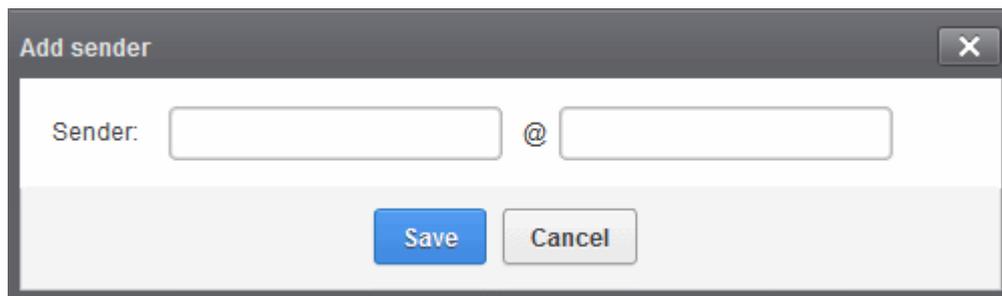
You can add multiple filters to the same search by clicking .

## Manually add senders to blacklist

- Click the 'Add' button at the top.



The 'Add sender' dialog is displayed.



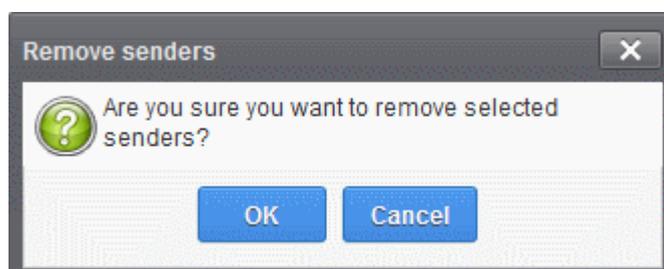
- Enter the sender's username in the first text box and sender's email domain name in the second text box after the @ symbol.
- Click the 'Save' button. Repeat the process to add more senders to blacklist.

## Remove senders from blacklist

- Select the sender(s) from the list and click the 'Delete' button.



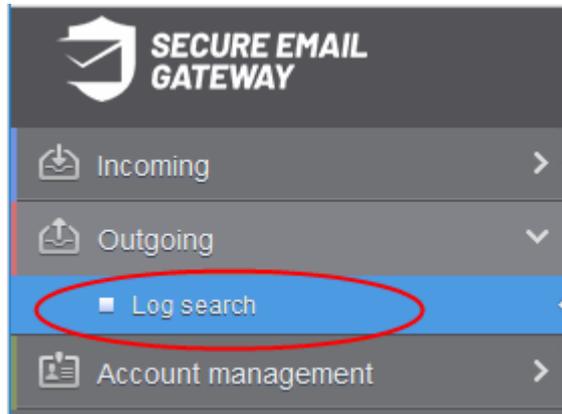
- Click 'OK' in the confirmation dialog for your changes to take effect.



## 3.2.2 Outgoing

- The 'Log search' feature lets you to search for sent email messages, such as mails with virus, spam mails or as per the filter criteria selected in the 'Classification' drop-down.
- From here you can also run a search based on other filters such as date range, recipient, sender IP and host.

**Note:** The administrator of your email account should have enabled this feature for you. If enabled, the 'Log search' is available in the left hand side navigation area under the 'Outgoing' tab.



Click the following link for more details in the 'Outgoing' section:

- [Log search](#)

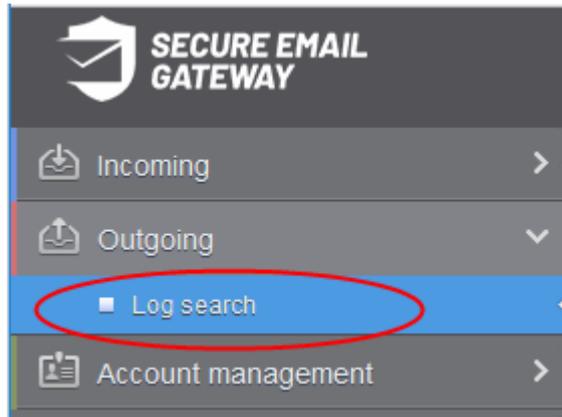
### 3.2.2.1 Log Search

The 'Log search' lets you search for sent email messages based on filters such as date range, recipient email address, sender IP and classification.

**Note:** The administrator of your email account should have enabled this feature for you. If this is enabled, the 'Log search' is available in the left hand side navigation area under the 'Outgoing' tab.

#### Search your outgoing emails in logs

- Click 'Outgoing' on the left then 'Log search'



The 'Log search (Outgoing)' interface opens:

The screenshot shows the 'Log search (outgoing)' interface. It features a search form with the following fields and options:

- Date range:** 2017-11-13 09:10:53 - 2017-11-14 09:10:53
- Message ID:** [Empty text box]
- Sender:** jones @demo.das.comodo.od.ua
- User:** [Empty text box] @demo.das.comodo.od.ua
- Recipient:** [Empty text box]
- Sender IP:** [Empty text box]
- Sender host:** [Empty text box]
- Classification:** All (dropdown menu)
- Include results from the last minutes:**

At the bottom of the form are two buttons: 'Search' and 'Download'.

- **Date range:** The date range for which you want to search for the sent mails.
- **Message ID:** Enter a unique message identifier (optional )
- **Sender:** The currently logged in user name is displayed in this field.
- **User:** The username of the outgoing email address that was used for your outgoing mails. Note, that even though many users may be configured with the same username for their outgoing mails, only the mails sent by you will be displayed for the search.
- **Recipient:** The email address of the recipient (for example, 'testuser1@domain.in') that you want to search for sent mails.
- **Sender IP:** The IP address of the sender.
- **Sender host:** The sender host name.
- **Classification:** Select the type of email that you want to search from the drop-down options.

- **Include results from the last minutes:** If selected, CSEG will include messages that are currently being migrated from the filtering server to the logging server in the search results.

The option "Include results from the last minutes" will slow down the search result retrieval

- Click the 'Search' button.

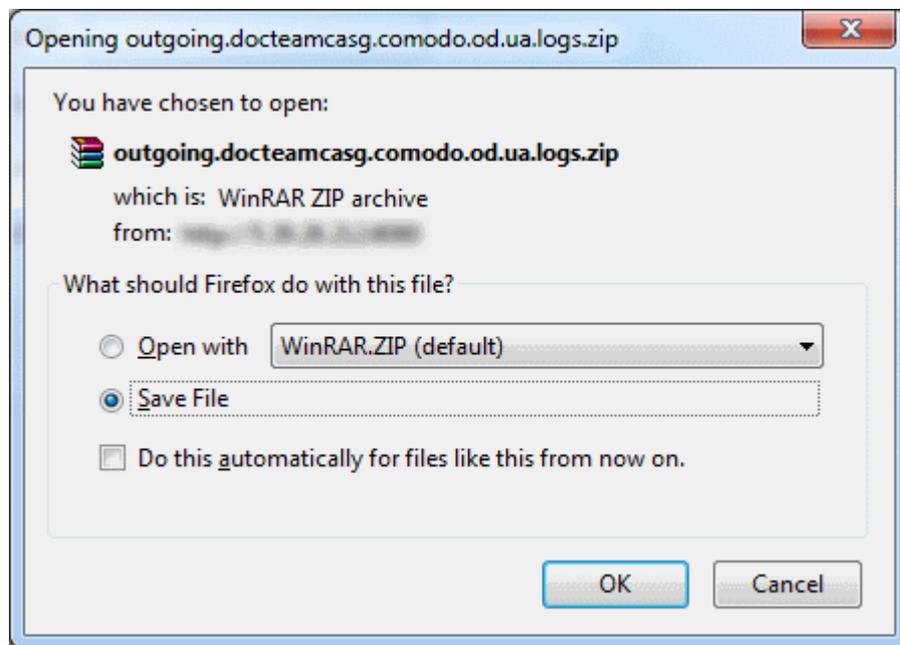
CSEG will search for the sent mails based on the filters entered and / or selected and display the results.

Date and time	Host (Exim id)	Sender hostn	User	Sender	Recipient	Subject	Classification
2014-10-29 14:49:16	mxsrv3.spamg 1XjUYS- 0005Ws-OH	mail2.comodo. 91.196.95.33	john	john@doctean	demo2@docte	outgoing subject 2	Accepted
2014-10-29 14:48:43	mxsrv2.spamg 1XjUYF- 0002Do-AU	mail2.comodo. 91.196.95.33	john	john@doctean	demo1@docte	outgoing subject	Accepted

Navigation: [1 - 2 / 2] Per page 15

- Click the 'Download' button to download the log report of sent mails for the filters entered and/or selected.

The download dialog is shown:

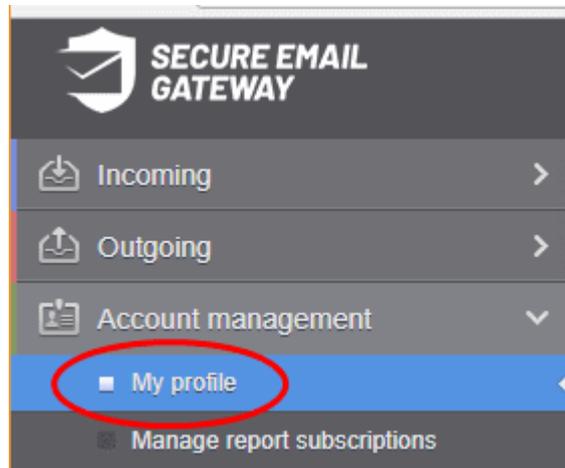


You can choose to open the file by using the browse option or save the file in your system. The compressed log file is saved in the folder that you have configured for saving download files. The values in the log report are separated by commas and this file can be opened with application such as Excel or Openoffice Calc for easy analysis.

## 3.2.3 User Account Management

Account management section lets you change password, whitelist your email, set quarantine alerts, and subscribe to quarantine reports.

**Note:** You can only access 'Change settings' and 'Manage report subscriptions' if they are enabled by your administrator. If enabled, you will see them under 'Account management' on the left.



Click the following links for more details on each area:

- [Manage profile settings](#)
- [Managing subscription for periodical summary reports](#)

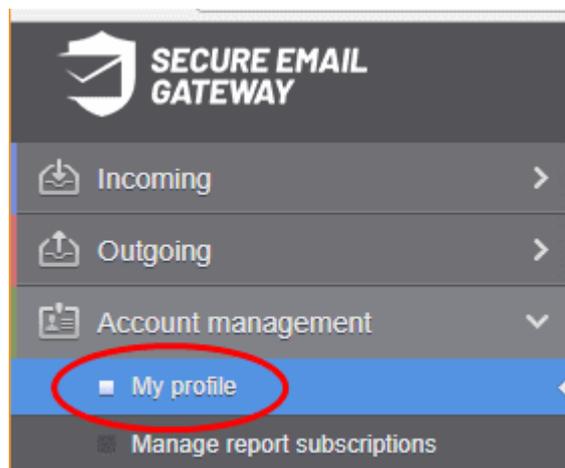
### 3.2.3.1 Manage Profile Settings

The 'My Profile' area lets you change password and whitelist your email.

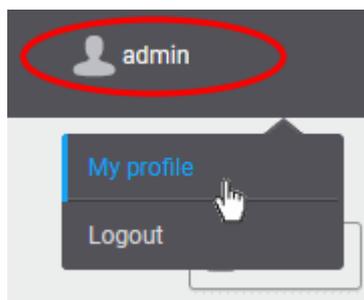
- All CSEG filters are disabled on whitelisted recipients.
- You can also configure quarantine alerts and session logged-in settings in this interface.

You can open your profile as follows:

- Click 'Account management' on the left then 'My profile':



Alternatively, click your username at top-right then select 'My Profile'.



This opens the 'My Profile' page:

**Note:** The 'Change settings' section is available in the 'My profile' interface only if the feature is enabled for you by your administrator.

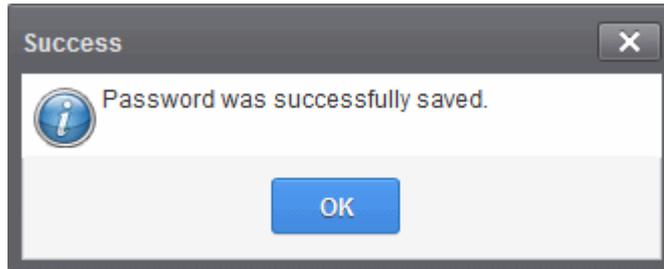
The interface allows you to:

- **Change your current password**
- **Add or remove from recipient whitelist**
- **Enable or disable quarantine alerts**
- **Enable or disable containment**
- **Configure non human or public email**
- **Configure session timeout settings**

### Change your password

- In the 'Change password' section, enter a new password and confirm it.
- Click 'Save'

You will see the following confirmation:



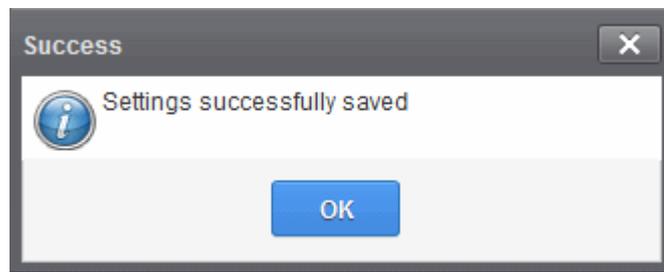
- Click 'OK'.

Now you can access CSEG using the new password.

### Add or remove from a Recipient Whitelist

- Scroll to the 'Change settings' section:
  - **Whitelist my email** - Enable this to add yourself to the recipient whitelist. Emails sent to you will not be filtered by CSEG.

A confirmation dialog will open:



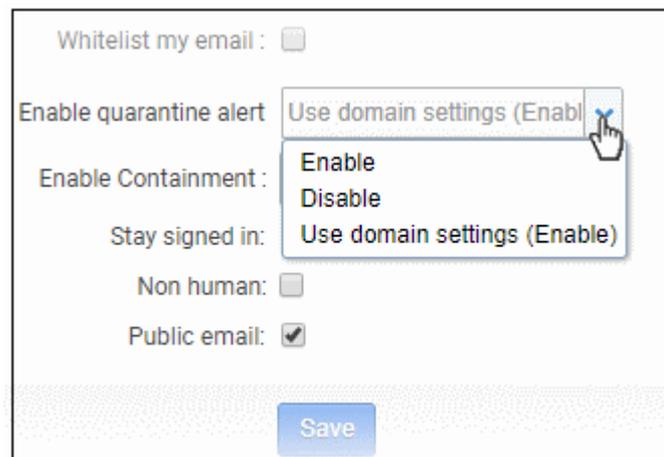
- Click 'OK'.

### Enable/disable quarantine alerts

Choose whether to receive notifications when an email addressed to you is identified as spam and moved to quarantine.

The default setting is as configured by the domain administrator.

- Click the 'Enable quarantine alert' drop-down:



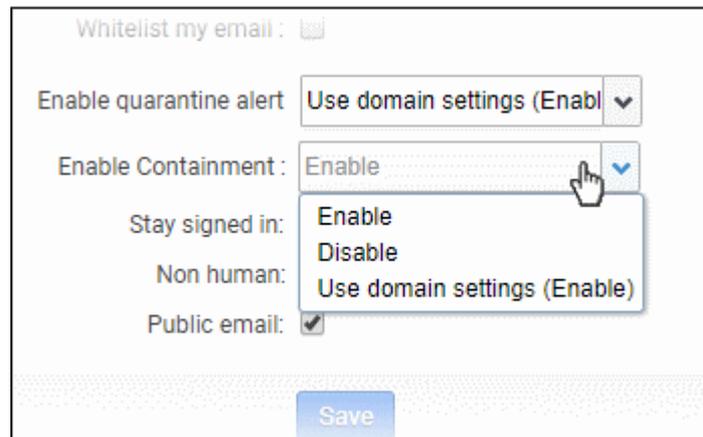
- **Enable** - Notifications will be sent to you whenever your incoming mail is quarantined
- **Disable** - No notifications will be sent whenever your incoming mail is quarantined
- **Use domain settings** - Depends on the selection by the administrator. If enabled, you will receive email alerts whenever your incoming emails are quarantined. If disabled, you will not receive notifications for your quarantined emails.

- Click the 'Save' button to apply your changes.

## Enable / disable containment

Containment is a security technology whereby email attachments with an 'unknown' trust rating are run inside a secure, sandbox environment.

The default setting here is configured by the domain administrator. You can change these settings if required.



- **Enable** – Attachments that have an unknown trust rating are run in a secure container when you open them. This means the attachment cannot damage your computer should it turn out to be malicious.
- **Disable** - Files with an unknown trust rating run uncontained on your computer.
- **Use domain settings (Enable)** – Use whatever the admin decides for the domain. The default is 'Enabled', but this can change if your admin makes changes.
- Click 'Save' to apply your changes.

## Non-human / public email settings

- These settings let you mark an email address as a public address, and/or a mailing list.
- These designations don't affect the filtering applied to the address, or any other aspect of protection. Rather, they let us analyze how much, and what types of spam are sent to these types of addresses.
- These metrics help us to create better rules to combat spam and to improve the mail-filter in general.



- **Non-human** – A mailing list, or other non-personal address. For example, info@yourdomain.com, sales@yourdomain.com
- **Public email** – An address which you promote for people to contact you. For example the address might be published on your website, your twitter feed or your Facebook page.

- You can check both boxes if an address is both 'non-human' and 'public'. For example, like 'sales@yourdomain.com'.
- Click the 'Save' button to apply your changes.

### Session timeout settings

- Your administrator should have enabled these settings for the domain



- **Stay signed in** – The default idle session time-out period is 30 minutes. If enabled, you stay logged in to CSEG till you log out.
- Click the 'Save' button to apply your changes.

### 3.2.3.2 Manage Subscriptions to Summary Reports

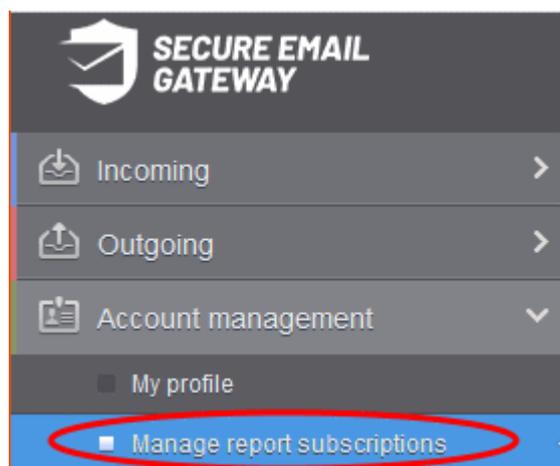
- The 'Manage report subscriptions' section lets you sign up for quarantine summary reports.
- These reports list all mails sent to you that were identified as spam and placed in quarantine.
- The reports are sent to your email address.

The **CSEG Reports** section has more details on their content.

**Note:** Your account admin should have enabled this feature for you. If enabled, you should see 'Manage report subscriptions' under 'Account management'.

### Configure report subscription for a user

- Click the 'Account management' on the left then click the 'Manage report subscriptions'.



The 'Manage report subscriptions' interface opens:

## Manage report subscriptions ? Help

▼ Quarantine report

Hour	Day of month	Day of week	Send empty	Enabled	Start date	Report length
<input type="radio"/> Every hour <input checked="" type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> <input type="checkbox"/> 0  <input type="checkbox"/> 1  <input type="checkbox"/> 2  <input type="checkbox"/> 3  <input checked="" type="checkbox"/> 4                 </div>	<input type="radio"/> Every day <input checked="" type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> <input type="checkbox"/> 14  <input type="checkbox"/> 15  <input type="checkbox"/> 16  <input type="checkbox"/> 17  <input type="checkbox"/> 18                 </div>	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 5px;"> <input type="checkbox"/> Sunday  <input type="checkbox"/> Monday  <input checked="" type="checkbox"/> Tuesday  <input type="checkbox"/> Wednesday  <input type="checkbox"/> Thursday                 </div>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Nov 21, 2017 04:00	Next report for 7 day(s) from last run (2017-11-14 04:00)

- Select 'Enabled' check-box if you want to receive the periodical quarantine summary reports.
- Leave the 'Send empty' checkbox unchecked if you do not want to receive empty reports.
- Select the frequency of the report to be sent to you from the 'Hour', 'Day of month' or 'Day of week' columns.
  - **Hour** - The reports are generated and sent at the selected hour of the day or date chosen from 'Day of month' or 'Day of week' columns.
  - **Day of month** - The reports are generated and sent every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
  - **Day of week** - The reports are generated and sent every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
  - **Start date** - Shows the begin date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
  - **Report length** - Shows the period of the report that are generated depending on the options chosen.
- Click 'Save' for your settings to take effect.
- Click 'Reset settings to default' button to configure default report generation period. The report is generated every 24 hours starting from last report generated time or from 00:00 hours.

## 4 CSEG Reports

Comodo Secure Email Gateway MSP allows you to subscribe to quarantine reports. You can choose to receive reports on a daily, weekly or monthly basis.

Each report contains statistics on mails that were sent to you, but instead moved to quarantine. The report also shows the sender, recipient, date and attachments of each mail. Click the subject line to open the mail in a new window.

- By default, reports are disabled for new users. Reports can be enabled or disabled for a user in **Account management > Manage Report Subscriptions**.

You can subscribe to receive reports daily, weekly or monthly at the selected hour.

- **Daily** - The report is generated and emailed to you daily.
- **Weekly** - The report is generated and emailed to you every seventh day from the date set in the 'Start date' field. The report will contain details of the mails quarantined during the past seven days.
- **Monthly** - The report is generated and emailed to you every 30th day from the start date set in the 'Start date' field. The report will contain details of the mails quarantined during the past 30 days.

An example of a Quarantine summary report is shown below:



Here is the quarantine report for [admin@korumail.tk](mailto:admin@korumail.tk) from Dec 10, 2019 11:00 to Dec 11, 2019 11:00 (GMT +07:00).

Subject	From	To	Date (GMT +07:00)	Reason	Size		Actions
<a href="#">test</a>	<a href="mailto:test@suslu.tk">test@suslu.tk</a> < <a href="mailto:test@suslu.tk">test@suslu.tk</a> >	<a href="mailto:admin@korumail.tk">admin@korumail.tk</a>	Dec 10, 2019 20:44	unknown Blocked extension	1129.16 KB		<a href="#">Release</a> <a href="#">Blacklist this Sender</a> <a href="#">Whitelist this Sender</a> <a href="#">Delete</a>
<a href="#">test</a>	<a href="mailto:test@suslu.tk">test@suslu.tk</a> < <a href="mailto:test@suslu.tk">test@suslu.tk</a> >	<a href="mailto:admin@korumail.tk">admin@korumail.tk</a>	Dec 10, 2019 21:03	unknown Blocked extension	1129.17 KB		<a href="#">Release</a> <a href="#">Blacklist this Sender</a> <a href="#">Whitelist this Sender</a> <a href="#">Delete</a>
<a href="#">test</a>	<a href="mailto:test@suslu.tk">test@suslu.tk</a> < <a href="mailto:test@suslu.tk">test@suslu.tk</a> >	<a href="mailto:admin@korumail.tk">admin@korumail.tk</a>	Dec 10, 2019 21:12	unsure Combined (0.21) Incorrect attachments extension detected	2.42 KB		<a href="#">Release</a> <a href="#">Blacklist this Sender</a> <a href="#">Whitelist this Sender</a> <a href="#">Delete</a>
<a href="#">test</a>	<a href="mailto:test@suslu.tk">test@suslu.tk</a> < <a href="mailto:test@suslu.tk">test@suslu.tk</a> >	<a href="mailto:admin@korumail.tk">admin@korumail.tk</a>	Dec 10, 2019 21:29	unsure Combined (0.21) Incorrect attachments extension detected	2.43 KB		<a href="#">Release</a> <a href="#">Blacklist this Sender</a> <a href="#">Whitelist this Sender</a> <a href="#">Delete</a>

- Click a 'Subject' link to open the mail in a new CSEG window. You need to login to CSEG to read the mail in the new window.

## Appendix - CSEG Feature List

Features	Availability
Number of domains and incoming / outgoing users	Depends on the subscription
Number of domain aliases	5
Active Directory / LDAP Synchronization	✓
Create / Modify User Groups	✓
Assign permissions to User Groups	✓
Number of user aliases per user	5
Incoming / Outgoing email filtering	✓
View all quarantined emails	✓
Release quarantined emails	✓
Whitelist / Blacklist quarantined emails	✓
Configure spam detection settings	✓
Report spam emails	✓
View queued emails in Delivery Queue	✓
Create local recipients	✓
Clear incoming / outgoing email cache	✓
Log search incoming emails	✓
Log search outgoing emails	✓
Create domain aliases	✓
Configure domain settings	✓
Configure email size restrictions	✓
Configure 'Blocked extensions' settings	✓
View users' release requests	✓
View users' whitelist / blacklist requests	✓
Whitelist / Blacklist recipients	✓
Whitelist / Blacklist senders	✓
View users' login history	✓
Email archive	✓
Number of email administrator accounts	Unlimited
Report management	✓

## About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

## About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)