

COMODO
Creating Trust Online®



Comodo Antispam Gateway

Software Version 2.9

Administrator Guide

Guide Version 2.9.032817

Comodo Security Solutions
1255 Broad Street
Clifton, NJ, 07013

Table of Contents

1 Introduction to Comodo Antispam Gateway	4
1.1 Release Notes	5
1.2 Purchasing License	8
1.3 Adding more Users, Domains or Time to your Account	9
1.4 License Information	14
2 Getting Started	17
2.1 Incoming Filtering Configuration	17
2.1.1 Configuring Your Mail Server.....	17
2.1.2 Configuring MX Record.....	18
2.1.2.1 Updating MX Records in Windows 2003/2008 Server.....	19
2.1.2.2 Updating MX Records on a host using BIND (and the 'named' daemon).....	19
2.1.2.3 Updating MX Records for Comodo DNS.....	20
2.1.2.4 Updating MX Records for GoDaddy.....	22
2.1.2.5 Updating MX Records for Enom.....	23
2.1.2.6 Updating MX Records for Network Solutions.....	24
2.1.2.7 Updating MX Records for Yahoo! Small Business.....	24
2.1.2.8 Updating MX Records for 1and1.....	25
2.1.2.9 Updating MX Records for 4D Web Hosting.....	26
2.1.2.10 Updating MX Records for DNS Park.....	26
2.1.2.11 Updating MX Records for DreamHost.....	26
2.1.2.12 Updating MX Records for DynDNS.....	27
2.1.2.13 Updating MX Records for IX Web Hosting.....	27
2.1.2.14 Updating MX Records for No-IP.....	28
2.1.2.15 Updating MX Records in CPanel.....	28
2.2 Outgoing Filtering Configuration	30
2.2.1 Per-User Authentication.....	31
2.2.2 Outgoing Smarthost setup.....	31
2.2.2.1 Configuring QMail to use a Smarthost	31
2.2.2.2 Configuring PostFix to use a Smarthost.....	32
2.2.2.3 Configuring Sendmail to use a Smarthost.....	32
2.2.2.4 Configuring Exchange 2000/2003 to use a Smarthost.....	32
2.2.2.5 Configuring Exchange 2007/2010 to use a Smarthost.....	33
2.2.2.6 Configuring Exim to use a Smarthost.....	34
2.2.2.6.1 Configuring Exim / cPanel to use a Smarthost.....	35
2.2.2.6.2 Configuring Exim / Directadmin to use a Smarthost.....	37
3 The Administrative Interface	37
3.1 Logging-in to the Administrative Interface	39
3.2 The Dashboard Area	40
3.2.1 Domain Management.....	43
3.2.1.1 Domains.....	43
3.2.1.1.1 Adding Domains.....	46
3.2.1.1.2 Deleting Domains.....	48

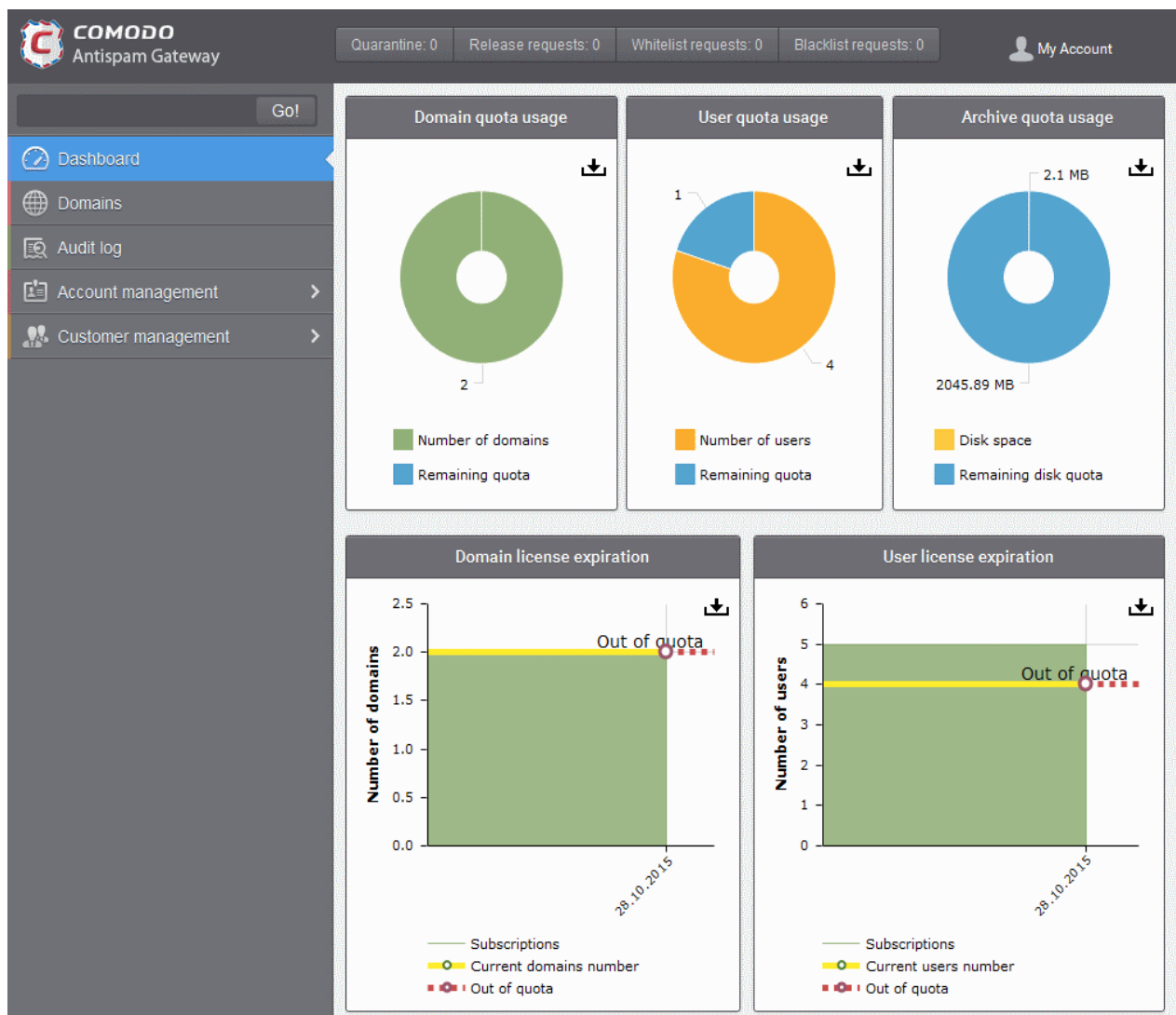
3.2.1.1.3 Editing Domains.....	49
3.2.1.1.4 Managing Domain.....	51
3.2.1.1.4.1 Domain Dashboard.....	52
3.2.1.1.4.2 Incoming.....	55
3.2.1.1.4.3 Outgoing.....	115
3.2.1.1.4.4 Email Management.....	131
3.2.1.1.4.5 Domain Audit Log	158
3.2.1.1.4.6 Domain Rules.....	169
3.2.1.1.4.7 Account Management.....	217
3.2.1.1.4.7.1 User Account Management.....	217
3.2.1.1.4.7.2 Managing User auto-import.....	238
3.2.1.1.4.7.3 Viewing User History.....	240
3.2.1.1.4.7.4 Importing Users from LDAP	243
3.2.2 Audit Log.....	252
3.2.3 Administrator Account Management.....	260
3.2.3.1 Administrators.....	260
3.2.3.2 User Groups & Permissions.....	268
3.2.3.3 Admin Groups & Permissions.....	276
3.2.3.4 My Comodo Account.....	285
3.2.3.5 My Profile.....	286
3.2.3.5.1 Change Settings.....	288
3.2.3.6 Users History.....	289
3.2.4 Customer Management.....	289
3.2.4.1 End User License and Subscriber Agreements	289
3.2.4.2 Viewing License Information.....	290
3.2.4.3 Manage Report Subscriptions.....	291
3.2.4.4 Configuring Language for Messages from CASG.....	294
3.2.4.5 Notification Email Settings.....	294
4 CASG Reports - An Overview.....	295
4.1 Quarantine Report.....	296
4.2 Domain Statistics Report.....	297
4.3 Auto-Imported Users Report.....	298
4.4 Quarantine Release Report.....	299
4.5 Reported Spam Report	300
Appendix 1 - CASG Error Codes.....	302
Appendix 2 - CASG Comparison Table.....	303
Appendix 3 - Troubleshooting LDAP.....	304
Appendix 4 - Useful Links.....	305
About Comodo.....	306

1 Introduction to Comodo Antispam Gateway

Comodo Antispam Gateway (CASG) is an enterprise email filtering solution that blocks spam, email-borne viruses and other unwanted mail from reaching user in boxes. CASG can be quickly configured for any email system and can be up and running in no time.

Features and benefits include:

- Antispam protection for incoming mails
- Antispam protection for outgoing mails
- Enhances productivity of employees and servers
- Intuitive web interface facilitates easy use and configuration
- Easy management of domains email restrictions
- Whitelist / blacklist recipients and senders
- Archiving incoming mails



Guide Structure

This guide is intended to take you through the configuration and use of Comodo Antispam Gateway and is broken down into the following main sections. The guide can be navigated using the bookmark links on the left.

- **Release Notes** - A list of new features that have been appeared in the CASG.
- **Purchasing License** - How to purchase CASG licenses.
Adding More Users, Domains Or Time To Your Account - Describes how to obtain domains, add more users to your account.
- **License Information** - Describes how to keep track of subscription status and various license related alerts.
- **Getting Started** - Describes how to configure your mail server with the CASG service
 - **Incoming Filtering Configuration**
 - **Outgoing Filtering Configuration**
- **The Administrative Interface** - Provides a snapshot of main functional areas of CASG.
 - **Logging-in to the Administrative Interface** - How to login into the CASG interface.
 - **The Dashboard Area** - Describes briefly about Domain management, Account management, Customer management and Statistics area.
 - **Domain Management** - Detailed explanation on how to add domains, edit domain and manage domains. This section also deals with adding users to whitelist and blacklist and view log reports.
 - **Audit Log** - Detailed explanation on how to view and export log reports for all the domains in the account.
 - **Account Management** - Detailed explanation on how to add new administrators and change login passwords, subscription to periodical reports and configure language for messages from CASG.
 - **Customer Management** - Provides information on accounts.
- **CASG Reports - An Overview** - An Overview of the Domain and Quarantine summary reports periodically generated and sent to the administrators and users by CASG.
- **Appendix 1** - CASG Error Codes
- **Appendix 2** - CASG Comparison Table
- **Appendix 3** - Troubleshooting LDAP
- **Appendix 4** - Useful Links

1.1 Release Notes

Version History	
Version Number	List of Changes
Version 2.8	<ul style="list-style-type: none"> • Added 'Domain Rules' feature to define rules for whitelisting, blacklisting and forwarding mails and filtering mails based on TLD names of email domains • Added ability for users to view quarantined mails received at their Alias email addresses
Version 2.6	<ul style="list-style-type: none"> • Added ability to assign the language for outgoing and received messages • Added Spam trap email for administrators • Added Sites filtering option for administrators • Added 'Non human' and 'Public email' that allow to more accurately filter spam for this type of email address.

Version 2.4	<ul style="list-style-type: none"> • Added ability to create Domain Rules rules for adding senders to whitelist/blacklist • Added ability for admins and users to add senders to whitelist/blacklist from the Archive interface • Added 'Quarantine release' and 'Report spam' reports for administrators • Geolocation restriction feature added that allows to create access control policies • Added ability to forward mails from one user to another user in the same domain
Version 2.2	<ul style="list-style-type: none"> • Added 'User auto-import report' for administrators. The report contains information about all auto-imported users under each domain. • Added notification for user-auto-import events • Added ability to specify blacklist/whitelist senders by TLD • Added ability to import sender whitelists/blacklists per user from CSV file. • End users can reply to emails from mail archive • End users will be notified when emails are quarantined that were addressed to them. They can open the quarantined email by clicking the link in the notification email.
Version 2.1	<ul style="list-style-type: none"> • Added more audit events • Added Users auto import • Added Relay restrictions
Version 2.0	<ul style="list-style-type: none"> • New user interface • Added Domain Audit Log feature, which enable administrators to view the events for selected domains in customer's account • Customers can purchase storage space for archiving incoming mails • Added more audit events • Added ability to whitelist / blacklist senders for each user • Various bug fixes
Version 1.12	<ul style="list-style-type: none"> • Added Audit Log feature, which enable administrators to view the events for all the domains in customer's account • Various bug fixes
Version 1.11	<ul style="list-style-type: none"> • Added ability to assign group permissions for administrators • Added ability to login to CASG service via CAM credentials • Administrators can unlock users immediately who were locked out after three unsuccessful attempts to login • Added ability to customize notification emails • Added ability to configure number of users for each domain belonging to an account • Various bug fixes
Version 1.10	<ul style="list-style-type: none"> • Added ability to import users from Active Directory server of Domain, through LDAP • Added ability to administrators to receive quarantine request emails through alternative email address(es) • Added ability to export configured Recipient Whitelist, Sender Whitelist, Recipient Blacklist and Sender Blacklist to CSV files
Version 1.9	<ul style="list-style-type: none"> • Added ability to assign group permissions to multiple users and filtered users

	<ul style="list-style-type: none"> • Added a user ability to search for logs of all domain • Added 'Reset to default' button for Incoming Spam Detection settings • Added 'Include results from the last minutes' parameter to the Incoming & Outgoing Log search pages • Added user login audits, including name of user, IP, logged time and session duration
Version 1.8	<ul style="list-style-type: none"> • Added option for administrators to configure idle session timeout period • Various bug fixes
Version 1.7	<ul style="list-style-type: none"> • Added option to purchase multiple licenses for single domain or multiple domains • Added new feature - Groups & Permissions. Allows administrators to create groups and configure permission levels for each group. Ability for administrators to add users to groups with preset policies. • Users in Power group can release quarantined emails without administrator's approval • Added ability for administrators to blacklist senders from Quarantine interface • New option for administrators to import users to whitelist / blacklist from csv format files • Added ability for administrators to import aliases from csv format files • Added new options for report generation - Ability for administrators to receive global reports for all domains and domain level report for selected domain • Login As button removed disabling an administrator to login as another administrator • Email size restriction - Administrators to contact Comodo if more than 250 MB email size is required • Various bug fixes
Version 1.6	<ul style="list-style-type: none"> • Added Released Emails, Blacklisted Emails and Whitelisted Emails features in Email Management • Added ability for administrators to release or reject users' request to release quarantined emails • Added ability for administrators to accept or reject users' request to add senders to whitelist or blacklist • Email notifications to administrators and users for requests such as to release quarantined mails, add senders to whitelist or blacklist • Added ability for administrators to prioritize domain routes using drag and drop feature • New option for administrators to set number of quarantined mails to be displayed per page • New option to stop empty reports from being sent to recipients • Right-click options to open links in new tab or new window • Various bug fixes
Version 1.5	<ul style="list-style-type: none"> • Added outgoing (SMTP) user management support • Added email aliases support • Added the ability for administrators to clear outgoing domain callout cache

	<ul style="list-style-type: none"> Added the ability for administrators to search for a specific outgoing email message
Version 1.4	<ul style="list-style-type: none"> Added periodical Domain and Quarantine summary reports feature Added ability for administrators to set language for messages displayed/sent by CASG according to their location Added automatic locking feature - the CASG account will be locked if the administrator/user login attempts fail for set number of times due to incorrect entry of username/password Added ability for administrators to view quarantined email message content through a new CASG window
Version 1.3	<ul style="list-style-type: none"> User interface improvements Embedded links to on-line help Ability to configure the number of days for which logs are available New options for domain settings Various bug fixes
Version 1.2	<ul style="list-style-type: none"> Added licensing options Fixed various bugs
Version 1.1	<ul style="list-style-type: none"> Added ability for administrators to view email message content through the CASG interface Added ability to report spam in multiple formats to Comodo for potential global blacklisting Added ability to quickly switch the domain that is currently being managed Added ability to reset 'Blocked Extensions' list to default values
Version 1.0	<ul style="list-style-type: none"> Added Mail Quarantine feature Added Whitelist / Blacklist pages Added Domain management feature Added Customer management Added Account management

1.2 Purchasing License

In order to get started with CASG, you must first purchase the service then configure the service. You have the option to purchase multiple licenses for single or more domains. The number of users and domains that are allowed for all the licenses purchased will be added and displayed in the **Customer Info** page. Follow the 'Buy Now' link on the website to purchase Antispam Gateway. Your Comodo Antispam Gateway account will be created once the signup process is complete - please refer to the email you receive after signup or activation. You can now login into the account with your username and password.

Note: A free version of CASG with limited features is also available for those who would like to try the application before purchasing a paid version. Please refer to **Appendix 2 - CASG Comparison Table** for more details on the features available for free and paid CASG versions.

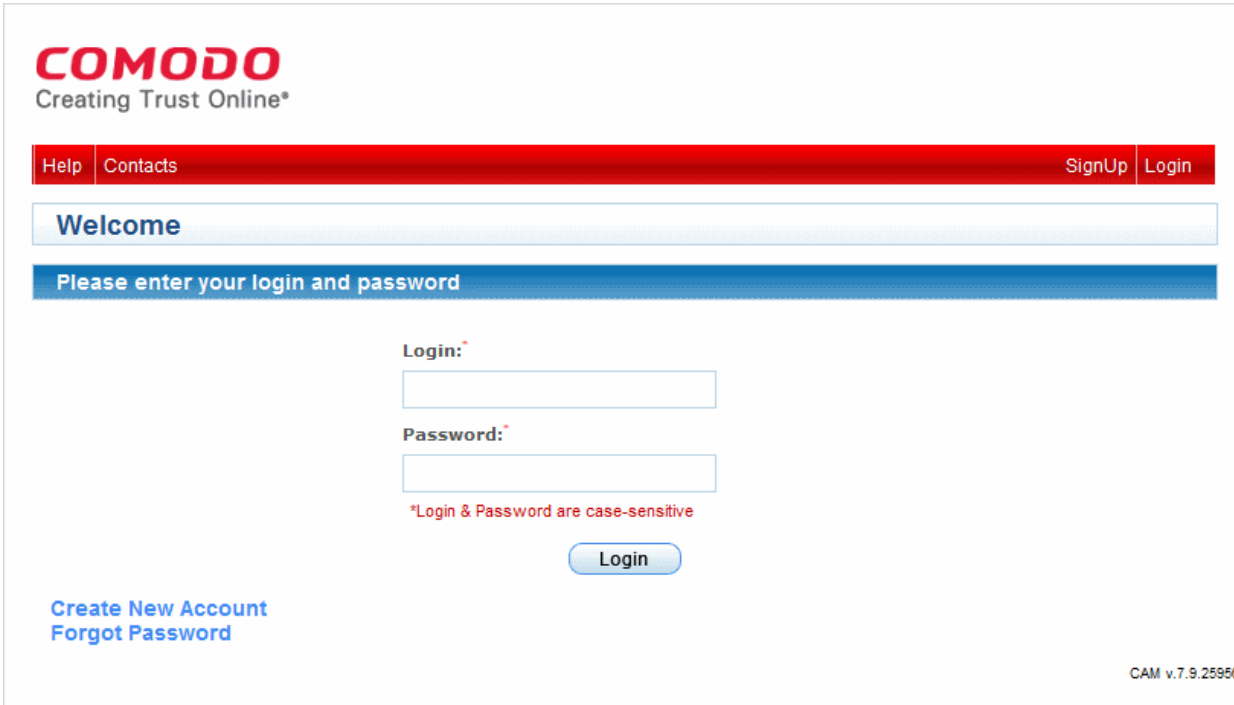
You can view the license details in the main interface after activation. See the section '**License Information**' for more details.

1.3 Adding more Users, Domains or Time to your Account

New users, domains and license term extensions as well as multiple licenses can be added to your account by logging into your CAM account at <https://accounts.comodo.com/>. Please read on for a step-by-step guide to this process.

To create CAM account

- Visit the Comodo Accounts Manager page at <https://accounts.comodo.com/>. The 'Register or Log In' page will be displayed.



The screenshot shows the Comodo Accounts Manager (CAM) login interface. At the top left is the Comodo logo with the tagline "Creating Trust Online®". A red navigation bar contains "Help" and "Contacts" on the left, and "SignUp" and "Login" on the right. Below this is a "Welcome" message in a blue box. A blue banner prompts the user to "Please enter your login and password". The login form includes a "Login:" label and an input field, followed by a "Password:" label and another input field. A red asterisk is next to both labels. Below the password field is a red note: "*Login & Password are case-sensitive". A blue "Login" button is centered below the fields. On the bottom left, there are links for "Create New Account" and "Forgot Password". The version number "CAM v.7.9.25958" is displayed in the bottom right corner.

- Click the 'Create New Account' link. The Signup page for all the services offered by Comodo will be displayed.

- Click 'Sign Up to Antispam Gateway'. Select the subscription package you want from the list. You have the option to purchase a single domain license or multi-domain license:
 - **Single Domain License** - One email domain. For example, xyz.com or abc.xyz.com, can be configured along with a total number of licensed users.
 - **Multi-Domain License** - More than one email domain. For example, you can configure xyz.com, abc.xyz.com, abc.org along with a total number of licensed users across all your domains.

- Choose the term for your new license

Choose EU if:

- You already have one or more domains that are being filtered by the ASG EU servers
- You access the ASG admin console using the following link:
<https://antispamgateway.comodo.com/admin/login.zul>

Choose US if

- You already have one or more domains that are being filtered by the ASG US servers
- You access the ASG admin console using the following link:
<https://us.antispamgateway.comodo.com/admin/login.zul>

COMODO Creating Trust Online® **Comodo Antispam Gateway**

1 License Selection > 2 Confirmation > 3 Order Summary

Comodo Sign-Up Page

Please, select currency that will be used for purchase (note that not all products can be available in currencies other than US Dollar)

US Dollar

Monthly Quarterly Annually Biannually Triennial Other

Base License-1 Domain 5 Users (1 domain, 5 users) at \$7.00 for 1 month

-Without additional domains-

-Without additional users-

-Without additional archive space-

Please select your region: EU

Important note for existing customers:

Please choose EU if you already have one or multiple domains that are being filtered by the ASG EU servers and you are accessing the ASG Admin console using the following link:<https://antispamgateway.comodo.com/admin/login.zul>

Please choose US if you already have one or multiple domains that are being filtered by the ASG US servers and you are accessing the ASG Admin console using the following link:<https://us.antispamgateway.comodo.com/admin/login.zul>

- If you do not have a base package or if you want to extend your license for the chosen term, select the checkbox at the left of the first drop-down and choose the base package from the first drop-down
- If you already have a base package and you want to add additional domains, users and/or subscribe for additional archive space, choose your requirements from the respective drop-downs
- Enter the User Details and Contact Information in the respective sections.
- If you already have an account with Comodo, select the 'Yes' radio button. You will only need to enter your Email Address/Login ID, Password, and Contact Information.

Customer Information (an * indicates required fields)

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

User Details

Are you an existing Comodo customer? Yes No

Email*

Email is case-sensitive

Password*
(8 characters min.)

Password is case-sensitive

Password Confirmation*

Street Address*

Address2

City*

Country* ▼

State or Province ▼

Postal Code*

Billing Information

The same as Contact Information

Note: Fields marked with * are mandatory.

- Select your payment method and complete the required payment fields:

Payment Options





Purchase Order

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

Credit Card Details

Credit Card Number*

Security Code* [What is it?](#)

Name exactly as it appears on your credit card*

Expiration date* ▼ - ▼

- If you want to be kept informed about Comodo products and updates, select the 'Communication Options' checkbox:

Communication Options

Yes! Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!

- Read and accept the 'End User License and Subscriber Agreement' by selecting 'I accept the Terms and Conditions' checkbox.

Note: The checkbox is enabled only after reading the full agreement by scrolling the page.

Terms and Conditions

END-USER LICENSE AND SUBSCRIBER AGREEMENT
Comodo Antispam Gateway

IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO ANTISPAM GATEWAY ("SERVICES"). BY DOWNLOADING, INSTALLING, OR USING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS HEREIN, DO NOT DOWNLOAD OR USE THE SERVICES OR CLICK ON "I ACCEPT".

This user license agreement is between you ("you" or "Subscriber"), as either an

I accept the Terms and Conditions

CONTINUE

- Click the 'Continue' button to move to the 'Confirmation' step.

Help | Contacts
SignUp | Login

✓ **Signup Information** >
 2 **Confirmation** >
 3 **Order Summary**

Order Confirmation

Please confirm your order:

Product	Product terms	Full price
Comodo Antispam Gateway 1 Domain 5 Users	Monthly	\$7.00
Total Amount:		\$7.00

Place Order
Cancel

- Review your order details and click the 'Place Order' button to confirm your order
Your order summary will be displayed.

Order #13953171-1

Comodo Security Solutions, Inc.
United States
support.comodo.com

julius@dithersconstruction.com
Mount Road
Riverdale 123456
US

Thank you for your purchase. Your order is complete and the confirmation will be sent to your email shortly.

Subscription Details			
Product Name		License Key	
Comodo Antispam Gateway		7594b10-4a3e-4b43-a8e1-218e8d7566a	
INVOICE NUMBER	13953171-12	SUBSCRIPTION ID	13953171-12

Order Details	
ORDER NUMBER	13953171-1
ORDER DATE	2015-01-20
ORDER TOTAL	\$0.00
SUBSCRIPTION EXPIRES ON	March 21, 2015

How to get started: We will send you an email explaining how to download and install your Comodo Software. You will be asked to enter your License Key during the installation process.

You can access your Comodo Account via <https://accounts.comodo.com/account/login>. This login provides you with the ability to modify your password, add subscriptions for other products, change billing and contact information, and review the ongoing status of your service.

[\[Print \]](#)

[\[Start using Comodo Antispam Gateway \]](#)

You will receive a confirmation email which includes help on how to log into your account and configure your DNS MX records.

After purchasing a CASG license, you will automatically become an administrator in CASG. Repeat the process for purchasing another CASG license. The number of users and domains that are allowed for all the licenses purchased will be added and displayed in the **Customer Info** page.

1.4 License Information

After purchasing your license, we advise you to keep track of your usage limits and the number of days remaining on your license(s) to avoid service interruptions. You have the option to upgrade or downgrade your license as per your requirements. You will begin to receive license renewal reminders via email before the expiration of license(s).

You can view your account status in the 'Customer Management' area in the main interface.

- Click 'Customer Info' from the 'Customer management' drop-down menu in the left hand side navigation area.
- The image below shows an example of a customer who has purchased multiple licenses:

The screenshot shows the Comodo Antispam Gateway Administrator interface. At the top, there are status indicators for Quarantine (0), Release requests (0), Whitelist requests (0), and Blacklist requests (0). A 'My Account' link is visible in the top right. The left sidebar contains navigation options: Dashboard, Domains, Audit log, Account management, and Customer management (expanded to show Customer info, Manage report subscriptions, and Email template settings). The main content area is titled 'Customer info' and includes a 'Help' icon. The 'Customer info' section displays: Name: Demo Customer, CAM login: julius@dithersconstruction.com, and CAM email: julius@dithersconstruction.com. Below this is a 'Totals' section showing: Number of users: 4, Max. number of users: 5, Number of domains: 2, Max. number of domains: 2, Disk quota (GB): 2.0, and Disk space: 2.1 MB. A 'Subscriptions' table follows, with columns for Max. number of users, Max. number of domain, License expiration date, Disk quota (GB), and Enabled. The table contains three rows of subscription data. At the bottom, there is an 'End-User License and Subscriber Agreement' section with a warning: 'Comodo AntiSpam Gateway 2 THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS.' Below this is a small text block: 'IMPORTANT - PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO ANTISPAM GATEWAY ("SERVICES"). BY DOWNLOADING, INSTALLING, OR USING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT

In the 'Customer Info' panel you will find the details of subscription(s) for your account, such as number of users, number of domains and the space available for archiving mails. For multiple licenses, the number of users and domains that are allowed for all the licenses purchased will be added and displayed in the Totals column.

- **Name:** Displays the name of the account.
- **CAM Login:** Displays the login user name for the account in Comodo Accounts Manager (CAM) at <https://accounts.comodo.com>. The administrator can use this login username to log in to CAM for purchasing additional licenses and renewal of existing licenses.
- **CAM email:** Displays the email address for the account as registered at CAM.

Account Summary

- **Number of users** - Displays the current number of users for all domains on the account.
- **Max. Number of users** - The maximum number of users that can be added as per all the subscriptions made for the account. The total number of users across all domains cannot exceed this number.
- **Number of domains** - Displays the number of domains on the account.
- **Max. number of domains** - The maximum number of domains that can be configured as per all the subscriptions made for the account.
- **Disk quota** - The maximum disk space allocated for mail archiving.
- **Disk space** - Displays the disk space currently used by the mail archive.

Details on Subscriptions

- **Max. number of users**- The maximum number of users that can be added for the account as per the specific subscription, that is, number of users cannot exceed the number given in this field for all domains included.

- **Max. number of domains** - The maximum number of domains that can be configured as per the specific subscription.
- **License expiration date** - Provides details about the expiry date of the license for the specific subscription.
- **Disk quota (GB)** - Displays the space available for archiving all incoming messages.
- **Enabled** - Displays whether the subscription is active or not.

End-User License and Subscriber Agreement

- **End-User License and Subscriber Agreement** - Displays the complete End-User License and Subscriber Agreement.

The 'Customer Info' panel alerts the administrator about license(s) expiration date and if Domain/Users limit is exceeded.

Administrators will start receiving license renewal reminders via email 30 days (default) before your license(s) are due to expire.

Note: The number of days before expiration of license that you start to receive license renewal reminders and the number of reminders per day that you receive depends on the settings configured in CASG.

An example of license renewal reminder is shown below:

Dear Customer,

Your Comodo Antispam Gateway account is due to expire in 5 days.

Please renew your subscription using your [account](#) page or contact support.

Please note that on 03-06-2012 your account will be suspended for 60 days and after that all your data will be eliminated.

If you have multiple licenses and if one of them has expired, then the number of domains and users allowed for that license will be deducted from the total number of allowed domains and users. No error message will be displayed if the usage is still limited within the total domains and users allowed for the remaining license(s).

An alert will be displayed at the top of the interface on the day when all the license(s) have expired. An example of the message is shown below.

Your subscription has expired, your account will be purged in 60 days, including all domains and quarantined emails, which will be irretrievable. Until that your Spam filters are disabled.

Note: The period after which all domains and quarantined emails for your account that will be purged depends on the settings configured in CASG.

During the configured period after license expiry, your emails will continue to be delivered to your domain via CASG but without any spam filtering. During this period, you cannot add new domains and new users. Option to enable quarantine is also disabled and incoming Spam detection settings screen for every domain in your account will display that Quarantine is disabled. After the configured period, all domains and quarantined mails in CASG for your account will be purged.

Users of the account can use the service normally during this period. After the configured period, if a user tries to login with his/her credentials, 'Your login or password is incorrect' message will be displayed.

Administrators can upgrade or downgrade his/her account using Comodo Accounts Manager (CAM) at <https://accounts.comodo.com/account/login>. You can use the login details provided at the time of purchasing the service.

Note: Any license upgrade or downgrade for your account will not be effected immediately. However, the changes will be reflected in the interface after a certain period of time depending on the settings configured in CASG.

After downgrading your existing account or after a license has expired, if the number of domains and / or users is more than permitted, an upgrade subscription message will be displayed at the top of the CASG interface. Some examples of alert messages are shown below:

- When the domain limit is exceeded:

Your domain limit exceeded by 1. Please lower number of your domains or buy new subscription.

You will not be able to add new domains until some of the current domains are removed. CASG filter will continue to function and you can add new users.

- When the user limit is exceeded:

Your user limit exceeded by 2. Please lower number of your users or buy new subscription.

You will not be able to add new users until some of the current users are removed. CASG filter will continue to function and you can add new domains.

2 Getting Started

Once an account with Comodo for CASG has been created, the next step is configuring your mail server with the CASG service and setting up incoming and outgoing filtering. Click on the links below for more details.

- **Incoming Filtering Configuration**
 - **Configuring your mail server**
 - **Configuring MX record**
- **Outgoing Filtering Configuration**
 - **Per-user authentication**
 - **Outgoing Smarthot setup**

2.1 Incoming Filtering Configuration

This section explains how you have to configure your mail server and point your domain MX records to CASG service.

- **Configuring your mail server**
- **Configuring MX record**

2.1.1 Configuring Your Mail Server

Step 1: Disable Sender Policy Framework (SPF) check or add CASG service domain to SPF check whitelist.

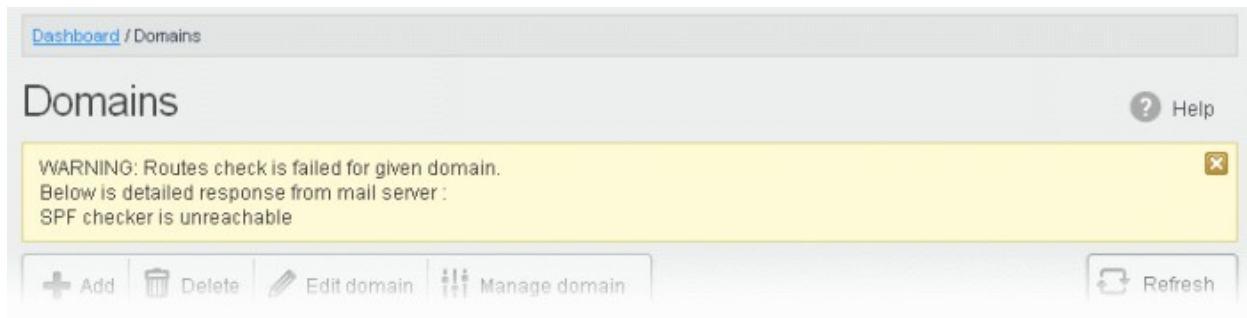
EU customers:

- mxpool1.spamgateway.comodo.com
- mxpool2.spamgateway.comodo.com

US customers:

- mxpool1.us.spamgateway.comodo.com
- mxpool2.us.spamgateway.comodo.com

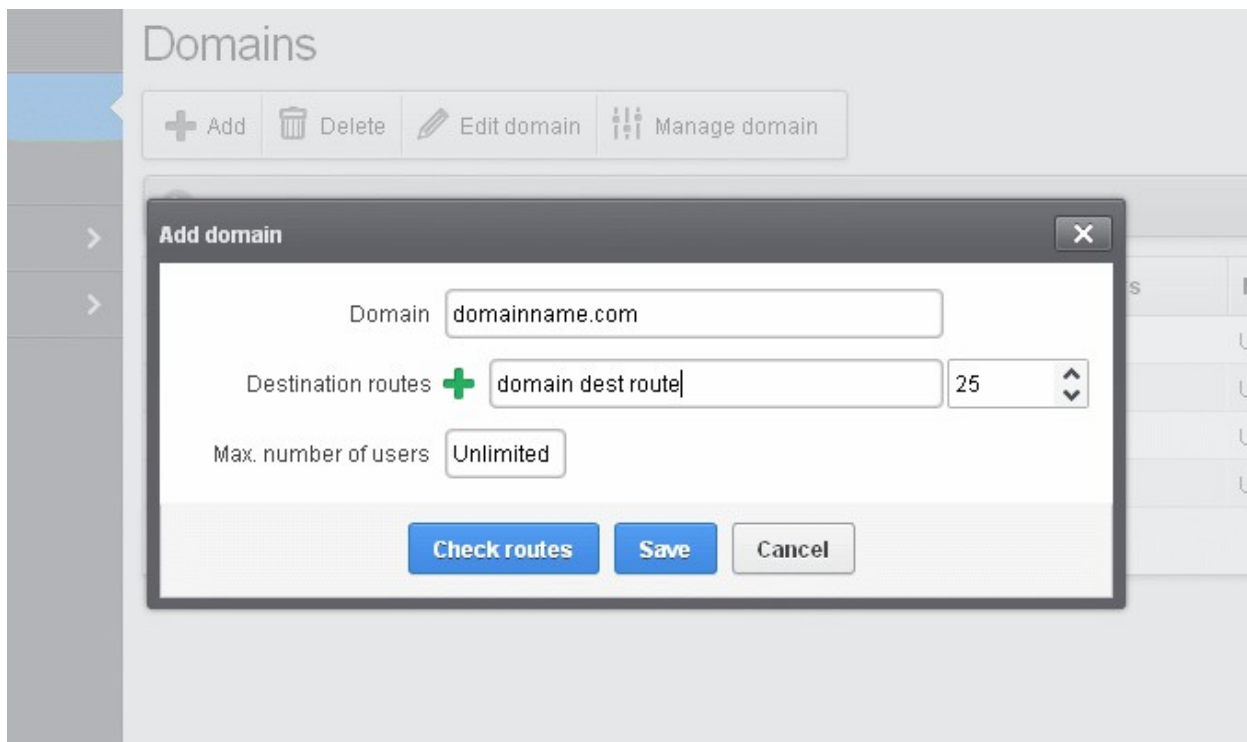
If the above step is not carried out, the following error message may appear while adding a domain.



Step 2: Add your domain to CASG service.

To add domain:

- **Login** to CASG system, go to **domain management** and **add domain**.



Step 3: Point mail server MX records to CASG service domain. See the next section 'Configuring MX Record' for more details.

2.1.2 Configuring MX Record

The next important step is to update the Mail Exchange (MX) records of your domain to point to the CASG service domain. Please ensure that you replace your old domain MX records with primary 'mxpool1.spamgateway.comodo.com' and secondary 'mxpool2.spamgateway.comodo.com'. If third-party MX servers are being used, then point the records to 'mxpool {1,2}.spamgateway.comodo.com'.

Background Note: The MX record is responsible for specifying the mail server to relay the incoming and outgoing email messages of a domain. A domain can have several MX records, each pointing to a mail server, with defined priority order. When an email is passed to/from your domain, the mail is handled by the first available mail server as per the priority. You can define new MX records or change the priority of them depending on how you want the mails to/from your domain has to be processed.

This section explains how to update your MX records so that all mails to/from your domain are passed through the

CASG spam filtering service. Click the following links for detailed explanations based on the DNS software/web hosting service you use.

- [Windows Server 2003/2008](#)
- [BIND \(and the "named" daemon\)](#)
- [Comodo DNS](#)
- [GoDaddy](#)
- [Enom](#)
- [Network Solutions](#)
- [Yahoo! SmallBusiness](#)
- [1and1](#)
- [4D Web Hosting](#)
- [DNS Park](#)
- [DreamHost](#)
- [DynDNS](#)
- [IX Web Hosting](#)
- [No-IP](#)
- [Cpanel](#)

2.1.2.1 Updating MX Records in Windows 2003/2008 Server

1. Open Control Panel by clicking Start > Control Panel and click 'Administrative Tools'.
2. Select 'DNS'.
3. Open the 'Forward Lookup Zones' folder.
4. To back up the current configuration, right-click the sub-folder for the mail domain you are configuring, select 'export' from the context sensitive menu and save the configuration in a safe location.
5. Open the zone/domain sub-folder for that mail domain.
6. Delete all the existing MX records in that zone/domain.
7. Enter a new record for primary mail server with a lowest priority number and enter its FQDN value as mxpool1.spamgateway.comodo.com and click 'OK'.
8. Enter a new record for secondary mail server with the next lowest priority number and enter its FQDN value as mxpool2.spamgateway.comodo.com and click 'OK'.
9. Right-click the zone/domain folder and select 'Properties' from the pop-up menu.
10. Select the 'Start of Authority (SOA)' tab, click the 'Increment' button and click 'oK'.

2.1.2.2 Updating MX Records on a host using BIND (and the 'named' daemon)

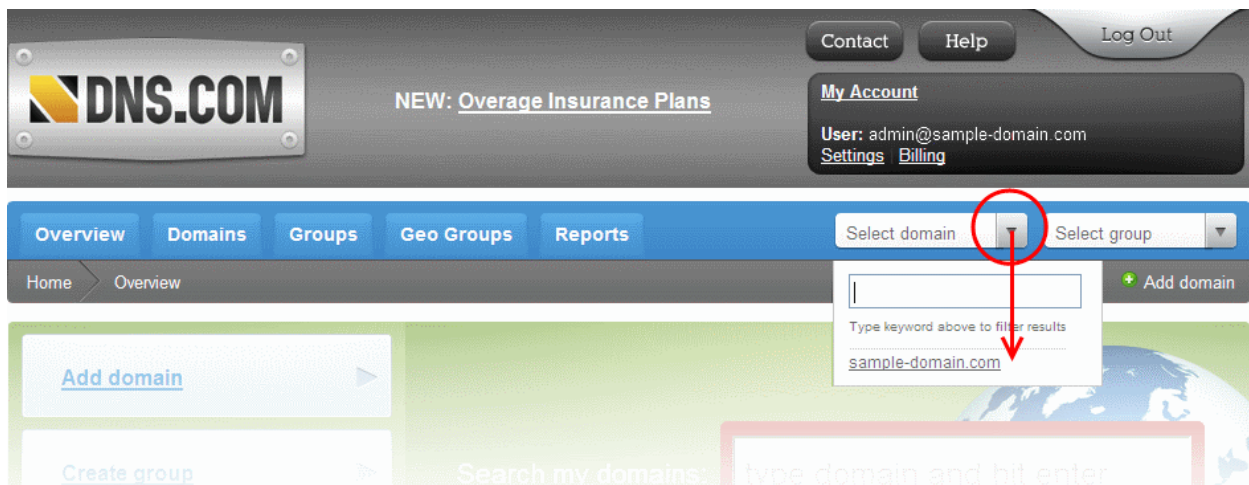
1. Make a backup copy of the zone file (or named.conf) that you intend to edit for MX record updates.
2. Open the Zone file for the mail domain you are configuring (or go to the part of named.conf being used for that zone)
3. Delete all the existing "MX" lines for that domain.
4. Enter a new "IN MX" record with the lowest preference value and enter the host name as "

mxpool1.spamgateway.comodo.com" for the primary mail server.

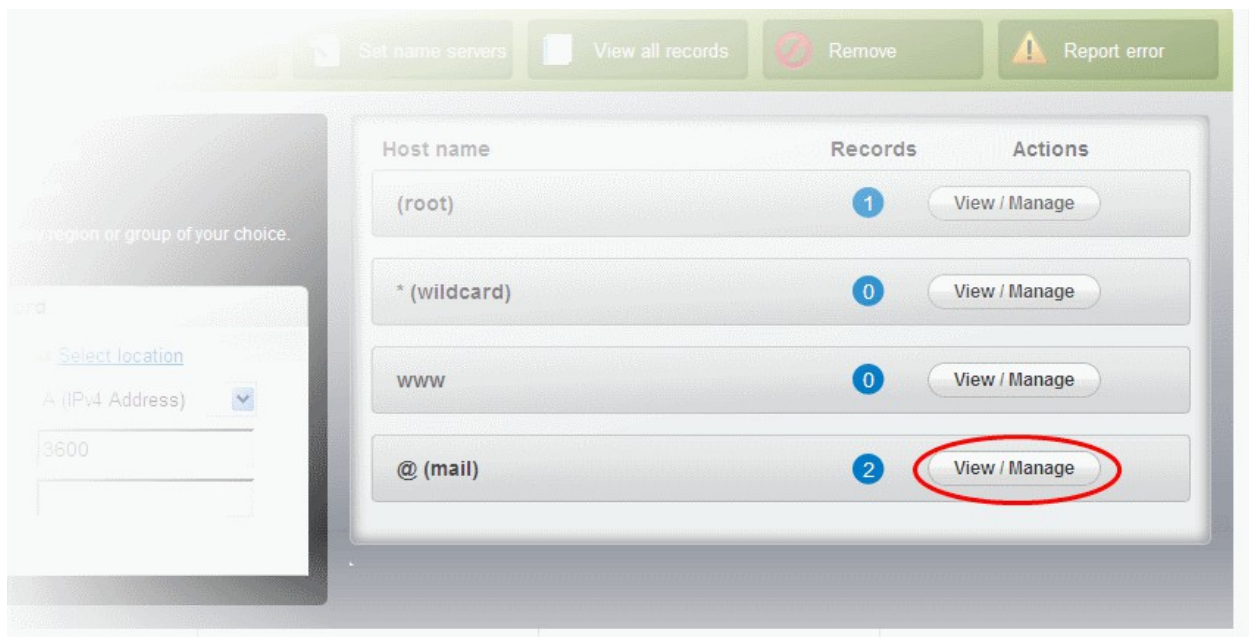
5. Enter a new "IN MX" record with the next lowest preference value and enter the host name as "mxpool2.spamgateway.comodo.com" for the secondary mail server.
6. Find the "@ IN SOA" record and increment the serial number (on the second line of the record).
7. Save the file and check it with named-checkconf.
8. Restart the 'named' daemon.

2.1.2.3 Updating MX Records for Comodo DNS

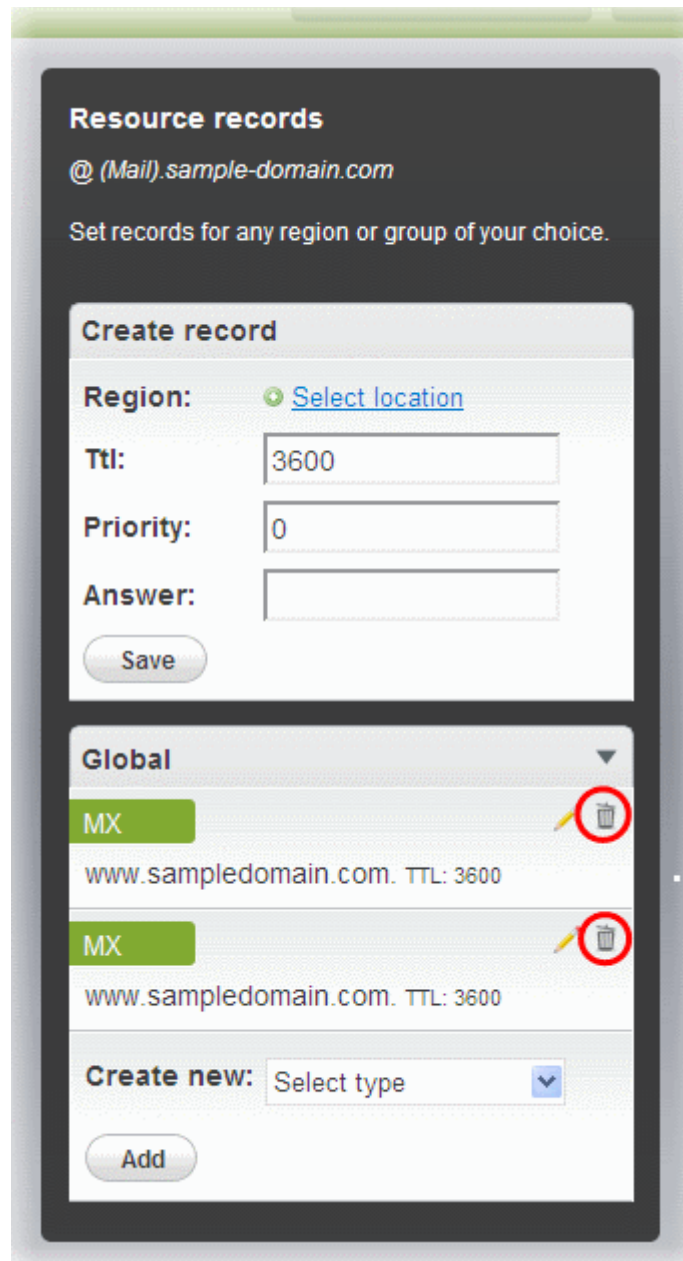
1. Log in to DNS.com administrative console at <https://dns.com/login/> by entering your login email address and password.
2. Select the domain for which you want to update the MX records, from the "Select domain" drop down menu.



3. Click the "View / Manage" button beside the row labeled "@ (mail)".



The existing MX records will be displayed at the left hand side pane.



4. Delete the existing records by clicking the trash can icons.
5. Set the primary mail server. Under 'Create Record':
 - Enter TTL as 3600 (secs)
 - Enter "1" in the 'Priority' field to set higher priority for the primary server
 - Enter " mxpool1.spamgateway.comodo.com" in the 'Answer' field
 - Click 'Save'
6. Again click the "View / Manage" button beside the row labeled "@ (mail)" and set the secondary mail server. Under 'Create Record':
 - Enter TTL as 3600 (secs)
 - Enter "2" in the 'Priority' field to set lower priority for the secondary server
 - Enter " mxpool2.spamgateway.comodo.com" in the 'Answer' field.
 - Click 'Save'

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

Setup should now be complete and mail filtering effected on all configured domains. If you experience problems, please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready. We have experienced technicians on hand to help troubleshoot any configuration issues.

2.1.2.4 Updating MX Records for GoDaddy

1. Log in to GoDaddy administrative console at <http://www.godaddy.com>, by entering your customer number or login name, entering your password, and clicking the 'Secure Login' button.
2. Click 'My Domains' from the 'Domains' drop-down menu.



3. Select the domain for which you want to update the MX records, from the 'Domain Name' column.
4. Click 'Total DNS Control and MX Records' from the Details page.



5. Delete the existing MX records by clicking the 'X' buttons.



Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Click the 'Edit' button beside each and set the priority with higher numbers like 10, 20 and so on. You can delete these records at a later time after your changes have taken effect.

6. Click 'Add New MX Record'. The interface for adding a new MX record will appear.

MX (Mail Exchangers)

To create a new MX record for your domain; enter the priority value (0 - 9999) and complete the Host Name, "Goes To" IP Address, and TTL Value fields; then click "Continue."

Note: The "Host Name" should be defined as your domain name (i.e., "domainnamegoeshere.com") or "@" (Entering "@" will automatically insert your domain name as the host name for the MX Record). If the MX Record is for the domain "www.domainnamegoeshere.com," the host name should be entered as "www."

Priority: 1

Host Name: @

Enter Goes To Address: my_domain_.net.psmtip.com

TTL: 1 Hour

OK Cancel

To set the primary server:

- Enter "1" in the 'Priority' field.
- Enter "@" in the Host Name field.
- In the 'Enter Goes To Address' field, enter " mxpool1.spamgateway.comodo.com".
- Select '1 week' from the TTL drop-down.
- Click 'OK'.

To set the secondary server:

- Click 'Add New MX Record' again. The interface for adding a new MX record will appear.
- Enter "2" in the 'Priority' field.
- Enter "@" in the Host Name field.
- In the 'Enter Goes To Address' field, enter " mxpool2.spamgateway.comodo.com".
- Select '1 week' from the TTL drop-down.
- Click 'OK'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.5 Updating MX Records for Enom

1. Log in to Enom administrative console at <https://www.enom.com/login.aspx> by entering your 'Login ID', 'Password' and clicking 'Login'.
2. Click the 'Domains' tab and select 'My Domain Names'. 'Manage Domains' page will be opened
3. Choose the domain for which the MX records are to be updated.
4. Select the + icon under the 'Total DNS Control' list in the 'Domain Details' panel. A sub-list will appear.
5. Click 'Total DNS Control And MX Records'. The 'Manage MX Records and DNS Zone File panel' will appear.
6. Click 'Launch Total DNS Control Manager'. The 'DNS Manager' interface will appear.
7. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Click the 'Edit' button beside each and set the priority with higher numbers like 10, 20 and so on. You can delete these records at a later time after your changes have taken effect.

- Click 'Add New MX Record'. The 'MX (Mail Exchangers) Record Wizard' will appear.

To set the primary server:

- Enter "1" in the 'Priority Value' field.
- Enter "@" in the Enter a Host Name field.
- In the 'Enter Goes To Address' field, enter " mxpool1.spamgateway.comodo.com".
- Select '1 week' from the TTL drop-down.
- Click 'Add'.

To set the secondary server:

- Enter "2" in the 'Priority Value' field.
- Enter "@" in the Enter a Host Name field.
- In the 'Enter Goes To Address' field, enter " mxpool2.spamgateway.comodo.com".
- Select '1 week' from the TTL drop-down.
- Click 'Add'.

- Click 'Continue'. The 'DNS Manager main page' will reappear when you've finished.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.6 Updating MX Records for Network Solutions

- Log in to Network Solutions administrative console at <https://www.networksolutions.com/manage-it/index.jsp> by entering your 'User ID', 'Password', selecting 'Manage All Services' from 'Log-in to' drop-down and clicking 'Login'.
- Click 'Edit DNS' under 'DNS Settings'. (If this is the first time you are editing the DNS settings, then click 'Custom DNS Setting'). The 'Edit DNS' interface will appear.
- Click 'Continue' in the 'DNS Manager-Advanced Tools'. The 'DNS Manager - Advanced Tools' interface will appear.
- Click Add/Edit in the 'Mail Servers' panel. The 'Mail Servers' table will be displayed.
- Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'Mail Servers' table to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

- Update the 'Mail Servers' table with the information in the following table.

Priority	Mail Server
1	mxpool1.spamgateway.comodo.com
2	mxpool2.spamgateway.comodo.com

- Click 'Save'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.7 Updating MX Records for Yahoo! Small Business

- Log in to Yahoo! Small Business administrative console at https://login.yahoo.com/config/login_verify2

by entering your 'Yahoo ID', 'Password' and clicking 'Sign In'.

2. Click 'Domain' from the tool bar.
3. Click 'Manage Advanced DNS Settings'.
4. Click 'Change MX Records'.
5. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

6. Enter the MX record for primary email server as " mxpool1.spamgateway.comodo.com" in the first open text box.
7. Set the priority for the primary email server as "1"
8. Enter the MX record for secondary email server as " mxpool2.spamgateway.comodo.com" in the second open text box.
9. Set the priority for the secondary email server as "2"
10. Click 'Submit'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.8 Updating MX Records for 1and1

1. Log in to 1and1 administrative console at <http://www.1and1.com/login> by entering your 'Customer ID' (Account Number or Domain name), 'Password' and clicking 'Login'.
2. Click 'Administration' tab
3. Click 'Domains'. The 'Domain Overview' page will appear.
4. Choose the domain for which the MX records are to be updated.
5. Select 'Edit DNS Settings' from the DNS menu.
6. Click 'Advanced DNS Settings' and choose 'Other mail server' from the options.
7. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

8. Enter the MX 1/Prio and MX 2/Prio fields with the following information.

MX 1/Prio	mxpool1.spamgateway.comodo.com
MX 2/Prio	mxpool2.spamgateway.comodo.com

9. Click 'OK'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.9 Updating MX Records for 4D Web Hosting

1. Log in to your 4D Web Hosting administrative console at <https://members.4dwebhosting.com/> by entering your 'Username', 'Password' and clicking 'Login'.
2. Click 'Configure'.
3. Click 'MX Records' from the Configuration options.
4. Replace the top two records with the following:

Primary	mxpool1.spamgateway.comodo.com
Secondary	mxpool2.spamgateway.comodo.com

5. Click 'Update MX Records'.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.10 Updating MX Records for DNS Park

1. Log in to DNS Park administrative console at <https://www.dnspark.net/signin.php>.
2. Click 'DNS Hosting' from the left hand side navigation.
3. Choose the domain for which the MX records are to be updated.
4. Click 'Mail Records (MX)'.
5. Under 'MX Resource records',
 - Replace the hostname at 1st priority row with " mxpool1.spamgateway.comodo.com" and click 'Update'
 - Replace the hostname at 2nd priority row with " mxpool2.spamgateway.comodo.com" and click 'Update'
6. Delete other existing MX records.

Tip: If you do not want to delete these records at this time, you can do it later, after your changes have taken effect.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.11 Updating MX Records for DreamHost

1. Log in to DreamHost administrative control panel at <https://panel.dreamhost.com/> by entering your email address/Web ID and Web panel password.
2. Click 'Mail' from the left hand side navigation and select 'MX' from the options.
3. Click 'Edit' beside the domain name for which the MX records are to be updated.
4. Delete all existing MX records under 'Custom MX Records'.
5. In the first two text boxes, enter:
 - " mxpool1.spamgateway.comodo.com"
 - " mxpool2.spamgateway.comodo.com"
6. Click 'Update your custom MX records now!'

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.12 Updating MX Records for DynDNS

1. Log in to DynDNS administrative console at <https://account.dyn.com/entrance/> by entering your Username and password.
2. Click 'My Services'.
3. Click 'Custom DNS' beside the domain for which the MX records are to be updated, under 'Zone Level Services'.
4. Select all the entries under 'Mail eXchanger Records' and click 'Delete MX'.
5. Click 'Add New MX'.
6. Set the primary mail server:
 - Enter " mxpool1.spamgateway.comodo.com"
 - Select '5' for preference to set higher priority for the primary server
 - Click 'Modify MX'
 - Click 'Return to...'
7. Set the secondary mail server
 - Enter " mxpool2.spamgateway.comodo.com"
 - Select '10' for preference to set lower priority for the secondary server
 - Click 'Modify MX'
 - Click 'Return to...'

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.13 Updating MX Records for IX Web Hosting

1. Log in to IX Web Hosting administrative control panel at <https://manage.ixwebhosting.com/index.php> by entering your login email address and password.
2. Click 'Manage' under 'Hosting Account'.
3. Choose the domain for which the MX records are to be updated.
4. Disable the existing MX records by clicking the 'On' button.
5. Click 'Edit' next to 'DNS Configuration'.
6. Delete the existing MX records.

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

7. Click 'Add DNS MX Record'.
8. Enter the primary and secondary mail servers one by one as given in the table below. Click 'Submit' after entering each record.

Name	Data	Data (Second box)
Leave Blank	1	mxpool1.spamgateway.comodo.com
Leave Blank	2	mxpool2.spamgateway.comodo.com

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.14 Updating MX Records for No-IP

1. Log in to No-IP administrative console at <https://www.no-ip.com/login/> by entering your login email address and password.
2. Click 'Host/Redirects' from the left hand side navigation.
3. Click 'Modify' beside the domain name for which the MX records are to be updated.
4. Navigate to 'Mail Options' section at the bottom of the page
5. Replace the MX record entry at the first field with " mxpool1.spamgateway.comodo.com"
6. Replace the MX record entry at the second field with " mxpool2.spamgateway.comodo.com"
7. Delete the other MX records.

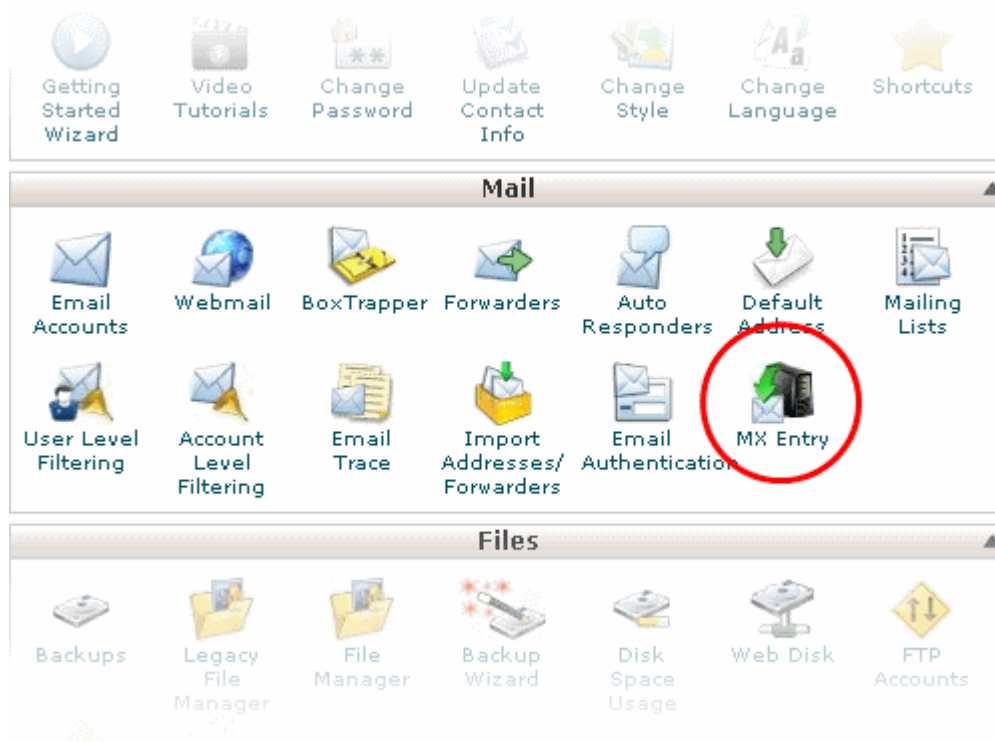
Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Edit the 'MX Records to set the priority with higher numbers like 10, 20 and so on for the existing records. You can delete these records at a later time after your changes have taken effect.

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.1.2.15 Updating MX Records in CPanel

This section explains how to update MX records for your domain if you or your web hosting service provider use CPanel as webhosting control interface.

1. Login to your administrative console. CPanel will be opened.
2. Click 'MX Entry' icon under 'Mail'



The MX Entry Maintenance panel will be opened.

3. Select the domain for which the MX record has to be changed from the Domains area.
4. Ensure that 'Local Mail Exchanger' option is selected under 'Email Routing'. If not, select the option and

click the 'Change' button.

Domain

Domain: mydomain.com

Email Routing

Automatically Detect Configuration (recommended) [more >](#)
 Local Mail Exchanger [more >](#)
 Backup Mail Exchanger [more >](#)
 Remote Mail Exchanger [more >](#)

Change

*Current setting is shown in **bold**.*

⚠ Warning: Setting the wrong option here can break receiving mail on your server. If you are at all unsure about which option to select contact your system administrator.

Add New Record

Priority:

Destination:

Add New Record

Priority:

Destination:

Add New Record

MX Records


PRIORITY	DESTINATION	ACTIONS
0	mydomain.com	Edit Delete

Home ▪ Trademarks ▪ Help ▪ Documentation ▪ Contact ▪ Logout

5. Delete the entries under 'MX Records' by clicking the 'Delete' links

Tip: If you do not want to delete the existing records at this moment, you can set them with lower priority. Click 'Edit' and set the priority with higher numbers like 10, 20 and so on. You can delete these records at a later time after your changes have taken effect.

6. Set the primary mail server under 'Add New Record'
 - Enter '0' in Priority field
 - Enter " mxpool1.spamgateway.comodo.com" in the Destination field
 - Click 'Add New record'. The new MX Record pointing to CASG service will be added

 Warning: Setting the wrong option here can break receiving mail on your server. If you are at all unsure about which option to select contact your system administrator.

Add New Record

Priority: ✓

Destination: ✓

MX Records

PRIORITY	DESTINATION	ACTIONS
0	mxsrv1.spamgateway.comodo.com	Edit Delete

7. Set the secondary mail server under 'Add New Record'

- Enter '1' in Priority field
- Enter " mxpool2.spamgateway.comodo.com" in the Destination field
- Click 'Add New record'. The new MX Record pointing to CASG service will be added

Priority:

Destination:

MX Records

PRIORITY	DESTINATION	ACTIONS
0	mxsrv1.spamgateway.comodo.com	Edit Delete
1	mxsrv2.spamgateway.comodo.com	Edit Delete
10	mydomain.com	Edit Delete

Home ▪ Trademarks ▪ Help ▪ Documentation ▪ Contact ▪ Logout

The MX records for your domain are updated now. But it may take up to 48 hours for the changes to take effect.

2.2 Outgoing Filtering Configuration

CASG allows you to configure outgoing filter that is independent of incoming email filtering. You can set up outgoing email filter for each user or if that is too cumbersome, you can set up the filtering server as a smarthost. Click the the following links for more details.

- [Per-user authentication](#)
- [Outgoing Smarthost setup](#)

Note: You can use only one of the methods, [Per-user authentication](#) or [Outgoing Smarthost setup](#), for outgoing email filtering.

2.2.1 Per-User Authentication

To set up outgoing filtering for a user, make sure that the user is a valid outgoing user. This can be done in the **Outgoing** section of the **Manage Domain** interface. You can also configure outgoing user to represent an IP address and anybody from this configured IP can send mail. To add an outgoing user, click 'Users' and 'Add' in the 'Outgoing users' interface. You can also import users from CSV file or from Incoming users. See the section **Users** to know how to configure an outgoing user.

2.2.2 Outgoing Smarthost setup

If you use a dynamic IP or you are unable to get the proper PTR records set up then you might need to consider using a smarthost. In this case all outgoing messages would be sent to CASG mailserver and the actual recipient would be contacted by CASG mailserver itself. Please note that for smarthost option, email user authorization should be handled on your side, either by IP address or by using SMTP AUTH.

A smarthost allows an SMTP server to route email to an intermediate mail server. This can ease mail server management.

This enables you to route messages over a connection that may be more direct or less costly than other routes. The smart host is similar to the route domain option for remote domains. The difference is that, after a smart host is designated, all outgoing messages are routed to that server. With a route domain, only messages for the remote domain are routed to a specific server. If you set up a smart host, you can still designate a different route for a remote domain. The route domain setting overrides the smart host setting.

You can route all incoming / outgoing messages for remote domains through a smarthost instead of sending them directly to the domain to reduce e-mail spam from the recipient's mail server via the default SMTP port.

- [Configuring QMail](#)
- [Configuring PostFix](#)
- [Configuring Sendmail](#)
- [Configuring Exchange 2000/2003](#)
- [Configuring Exchange 2007/2010](#)
- [Configuring Exim](#)
 - [Configuring Exim / cPanel](#)
 - [Configuring Exim / Directadmin](#)

2.2.2.1 Configuring QMail to use a Smarthost

Routing all mails to a smarthost

The file where SMARTHOST relating to smarthost settings are kept is named `smtproutes` and is usually found in `/var/qmail/control/`. We use the hostname ' `mxpool1.spamgateway.comodo.com`' on port 587 as outgoing server:

```
echo: mxpool1.spamgateway.comodo.com:587" > /var/qmail/control/smtproutes
```

This command will set qmail that all your mails will be routed to `mxpool1.spamgateway.comodo.com:587` (**will remove other existing lines**).

Routing all mails for a specific domain to a smarthost :

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

```
echo "example.com: mxpool1.spamgateway.comodo.com:587" >> /var/qmail/control/smtproutes
```

This will route outgoing email to "example.com" via the smarthost. (rest of the lines will be kept).

2.2.2.2 Configuring PostFix to use a Smarthost

Routing all mails to a smarthost :

These instructions assume the **postfix**config files live in **/etc/postfix/main.cf**

In **/etc/postfix/main.cf** add the line:

```
relayhost = mxpool1.spamgateway.comodo.com:587
```

Routing all mails for a specific domain to a smarthost :

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

Add a line to **/etc/postfix/transport**:

```
example.com smtp: mxpool1.spamgateway.comodo.com:587
```

generate a postmap file :

```
postmap hash:/etc/postfix/transport
```

To use the transport file, add or edit a line in **/etc/postfix/main.cf**:

```
transport_maps = hash:/etc/postfix/transport
```

Restart Postfix and all mail. The mail for selected domains should go through the Smarthost.

2.2.2.3 Configuring Sendmail to use a Smarthost

Routing all mails to a smarthost :

Edit **/etc/sendmail.cf** and add the following line:

```
DSmxpool1.spamgateway.comodo.com
```

Restart Sendmail.

2.2.2.4 Configuring Exchange 2000/2003 to use a Smarthost

Routing all mails to a smarthost :

- In the Exchange System Manager, expand the Administrative Groups container.
- Expand the desired administrative group, and expand the Routing Groups container.
- Expand the routing group you need to work with, right-click the Connectors folder and select 'New'.
- Select SMTP Connector.
- On the 'General' tab, enter a name to identify the connector.
- Change 'Select Forward All Mail Through this Connect To The Following Smart Hosts' then enter one of the following URLs:
 - EU Customers – Enter mxpool1.spamgateway.comodo.com
 - US Customers – Enter mxpool1.us.spamgateway.comodo.com
- Default SMTP Server -> Properties -> Delivery Tab -> Outbound Connections -> TCP Port set to 587.

Routing all mails for a specific domain to a smarthost :

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

Do all steps mentioned **above** and continue on with the following:

- Under Local Bridgeheads, click 'Add' and select the SMTP server that will become the SMTP bridgehead for its routing group.
- On the 'Address Space' tab, click Add select SMTP and click 'OK'.
- In the E-Mail Domain box add the name of the remote location's e-mail domain (e.g., **example.com**), and click 'OK'.
- Click 'OK' three times to exit the SMTP connector configuration.
- Restart the Microsoft Exchange Routing Engine service and the SMTP service.

2.2.2.5 Configuring Exchange 2007/2010 to use a Smarthost

Routing all mails to a smarthost :

A Send Connector must already have been created and configured correctly on the Hub Transport server.

- Open Exchange Management Console.
- Click on the '+' next to Organization Configuration.
- Select Hub Transport and select the 'Send Connectors' tab.
- Right-click on the existing Send Connector, select 'Properties' and go to the 'Network' tab.
- Select "Route mail through the following smart hosts:" and click 'Add'.
- EU Customers – Enter mxpool1.spamgateway.comodo.com (you need to use port 587).
- US Customers – Enter mxpool1.us.spamgateway.comodo.com (you need to use port 587).

If you have more than one Smarthost, repeat the previous two steps.

The changes to the Send Connector will take effect immediately without you having to reboot the server or restart any services.

In order to change the port to 587 you will have to issue the following command in the Exchange Powershell Console:

```
Set-SendConnector -identity "NAME OF CONNECTOR" -Port:587
```

Restart the transport service.

Routing all mails to a smarthost with Username Authentication:

A Send Connector must already have been created and configured correctly on the Hub Transport server.

- Open Exchange Management Console.
- Click on the + next to Organization Configuration.
- Select Hub Transport and select the 'Send Connectors' tab.
- Right-click on the existing Send Connector, select 'Properties' and go to the 'Network' tab.
- Select "Route mail through the following smart hosts:" and click 'Add'.
- Enter **mxpool1.spamgateway.comodo.com**, **mxpool2.spamgateway.comodo.com** in the FQDN section.
- Click 'Change' under the smart-host authentication.
- Select '**Basic Authentication**' and tick the TLS box .
- Add your newly created username and password.
- Click 'OK '.

The changes to the Send Connector will take effect immediately without you having to reboot the server or restart any services.

In order to change the port to 587 you will have to issue the following command in the Exchange Powershell Console:

```
Set-SendConnector -identity "NAME OF CONNECTOR" -Port:587
```

Restart the transport service.

2.2.2.6 Configuring Exim to use a Smarthost

Routing all mails to a smarthost :

To configure the mailserver Exim, edit your Exim configuration file (e.g. `/etc/exim/exim.conf`).

Add in the routers section (after **begin routers**):

```
spamgateway_smarthost_router:  
  driver = manualroute  
  transport = spamgateway_smarthost_transport  
  route_list = $domain mxpool1.spamgateway.comodo.com::587  
  no_more
```

Make sure the local mail route is before smarthost, if you don't want local mail to be forwarded. Add in the transports section (after **begin transports**):

```
spamgateway_smarthost_transport:  
  driver = smtp  
  hosts_require_tls = *
```

Routing all mails for a specific domain to a smarthost:

Note: The information below relates to a very specific customer requirement and is not recommended for most deployments. A configuration like this can cause problems which will be hard to troubleshoot. Unless you are sure you need to use this setup, please explore the other available options for routing mail.

Put the domain in place of the \$domain value in the route_list (above). For multiple domains you can use:

```
route_list = domain.example.com mxpool1.spamgateway.comodo.com::587 ;
domain.example.org mxpool1.spamgateway.comodo.com::587
```

Restart Exim for the changes to take effect.

2.2.2.6.1 Configuring Exim / cPanel to use a Smarthost

Routing all mails to a smarthost :

Go to the "Exim Configuration Editor" in WHM. Choose "Advanced Editor". Add in the routers section (after **begin routers**, and after the **democheck:** router block):

```
smarthost_dkim:
  driver = manualroute
  domains = !+local_domains
  require_files = "+/var/cpanel/domain_keys/private/${sender_address_domain}"
  transport = remote_smtp_smart_dkim
  route_list = $domain mxpool1.spamgateway.comodo.com::587

smarthost_regular:
  driver = manualroute
  domains = !+local_domains
  transport = remote_smtp_smart_regular
  route_list = $domain mxpool1.spamgateway.comodo.com::587
```

Then add in the transports section (after begin transports):

```
remote_smtp_smart_dkim:
  driver = smtp
  hosts_require_tls = *
  interface = ${if exists {/etc/mailips}}{${lookup{$sender_address_domain}
lsearch*/etc/mailips}{$value}{}}{}}
  helo_data = ${if exists {/etc/mailhelo}}{${lookup{$sender_address_domain}
lsearch*/etc/mailhelo}{$value}{$primary_hostname}}{$primary_hostname}}
  dkim_domain = $sender_address_domain
  dkim_selector = default
  dkim_private_key = "/var/cpanel/domain_keys/private/${dkim_domain}"
  dkim_canon = relaxed

remote_smtp_smart_regular:
  driver = smtp
  hosts_require_tls = *
  interface = ${if exists {/etc/mailips}}{${lookup{$sender_address_domain}
lsearch*/etc/mailips}{$value}{}}{}}
  helo_data = ${if exists {/etc/mailhelo}}{${lookup{$sender_address_domain}
lsearch*/etc/mailhelo}{$value}{$primary_hostname}}{$primary_hostname}}
  dkim_domain = $sender_address_domain
  dkim_selector = default
  dkim_private_key = "/var/cpanel/domain_keys/private/${dkim_domain}"
  dkim_canon = relaxed
```

Save the configuration. All the outgoing mail will be relayed through the filterserver and accept original and DKIM

signed emails.

Routing all mails to a smarthost with SMTP Authentication:

- Go to the "Exim Configuration Editor" in WHM.
- Choose "Advanced Editor". do not include "**begin authenticators**".
- Otherwise, simply append our 4 lines and leave out our "**begin authenticators**".

```
begin authenticators

spamgateway_login:
driver = plaintext
public_name = LOGIN
client_send = : username@example.com : yourUserPassword
```

Add a Router in the Router Configuration Box.

```
send_via_spamgateway:
driver = manualroute
domains = ! +local_domains
transport = spamgateway_smtp
route_list = "* mxpool1.spamgateway.comodo.com::587 byname"
host_find_failed = defer
no_more
```

Add a Transport to the Transport Configuration Box.

```
spamgateway_smtp:
driver = smtp
hosts = mxpool1.spamgateway.comodo.com
hosts_require_auth = mxpool1.spamgateway.comodo.com
hosts_require_tls = mxpool1.spamgateway.comodo.com
```

Restart Exim.

Extra: Routing all mails for a specific domain to a smarthost with individual outgoing accounts:

To be able to set custom settings/limits for outgoing users, use the information above (Routing with SMTP Authentication) with a small change. Use this:

```
client_send = : ${extract{user}}{${
{lookup{$sender_address_domain}lsearch{/etc/exim_spamgateway}}}} :
                ${extract{pass}}{${
{lookup{$sender_address_domain}lsearch{/etc/exim_spamgateway}}}}
```

instead of the **client_send** in the previous example.

To create a file called **/etc/exim_spamgateway** with the following structure, use this :

```
domain1.com:    user=user@domain1.com    pass=abc
domain2.com:    user=user@domain2.com    pass=xyz
```

Extra: Limiting Outgoing for certain domains

This option can be combined with the individual accounts configuration to restrict outgoing only to specific domains. You can add the following entry (underneath domains) in the router :

```
senders = ^.*@domain1.com : ^.*@domain2.com
```

2.2.2.6.2 Configuring Exim / Directadmin to use a Smarthost

- Edit your Exim configuration file (e.g. /etc/exim.conf).
- Add in the routers section (after begin routers):

```
spamgateway_smarthost_router:  
  driver = manualroute  
  domains = ! +local_domains  
  ignore_target_hosts = 127.0.0.0/8  
  condition = "${perl{check_limits}}"  
  transport = spamgateway_smarthost_transport  
  route_list = $domain mxpool1.spamgateway.comodo.com::587  
  no_more
```

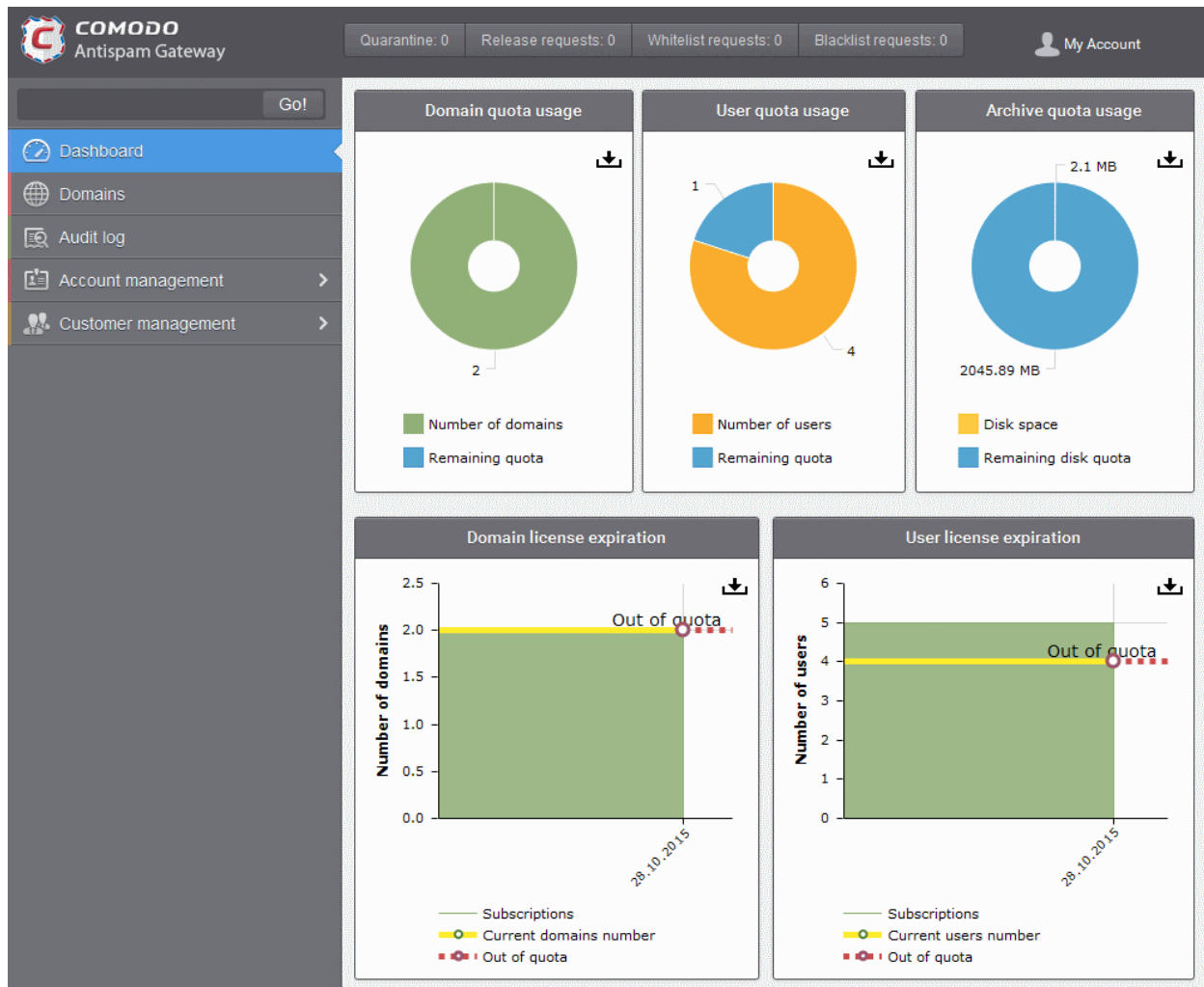
- This replaces the existing "lookuphost:" router which should be commented.
- Add in the transports section (after begin transports):

```
spamgateway_smarthost_transport:  
  driver = smtp  
  hosts_require_tls = *
```

Restart Exim.

3 The Administrative Interface

The Administrative Console is the nerve center of Comodo Antispam Gateway (CASG), allowing administrators to add domains, add administrators and users, manage accounts and more.




Once logged-in, the administrator can navigate to different areas of the console by clicking the tabs at the left hand side.

Main Functional Areas

- **Dashboard** - Allows administrator to view graphical summaries of domain quota usage, user quota usage, archive quota usage, details of domain and user license expiration. See **The Dashboard Area** for more details.
- **Domains** - Provides a snapshot of domains in CASG for your account and serves as a launchpad for adding, deleting, editing and managing domains. In this area the administrators can set filters, view quarantined mails, set email restrictions. The administrator can also view the log record of actions such as accepting whitelist request, accepting blacklist request and so on. See **Domain Management** for more details.
- **Audit Log** - Allows administrators with appropriate privileges to view a record of actions initiated by users and administrators for all domains belonging to an account. See **Audit Log** for more details.
- **Account Management** - Enables the administrator to add other administrators, delete or edit existing administrators. Currently logged in administrator also can change his/her password, manage their subscription to periodical domain and quarantine summary reports in this area. An administrator also can create user and administrator groups and permissions can be configured for these groups. Users and administrators then can be added to these groups that will impose a common permission policy for them. The administrators can also view a user history for *all* domains within a particular date range. See **Account Management** for more details.
- **Customer Management** - Enables the administrator to view the details of the customer such as name, maximum number of users, maximum number of domains, incoming archive space, license expiration date

and whether the customer is enabled or not. Also the administrator can manage the subscription of periodical domain and quarantine summary reports for the customer, configure email template settings for the messages sent from CASG. See **Customer Management** for more details.

Clicking the support.comodo.com link at the bottom of interface takes you to the Comodo support web page, an online knowledge base and support ticketing system. The fastest way to get further assistance in case you find any problem using CASG.

Various interfaces displays a help button  at the top right side of the interface. Clicking on this help button will take you to the respective help page of CASG online help guide for more detailed explanation.

3.1 Logging-in to the Administrative Interface

You can login into your CASG account using any internet browser. Login at the following URLs:

EU Customers - <https://antispamgateway.comodo.com/admin/login.zul>

US Customers - <https://us.antispamgateway.comodo.com/admin/login.zul>

A screenshot of the 'Administrative Interface' login form. The form has a blue header with a user icon and the text 'Administrative Interface'. Below the header, there are two input fields: 'Username' and 'Password'. Below the 'Password' field is a blue 'Login' button.

- Login to the interface with your CASG username and password.

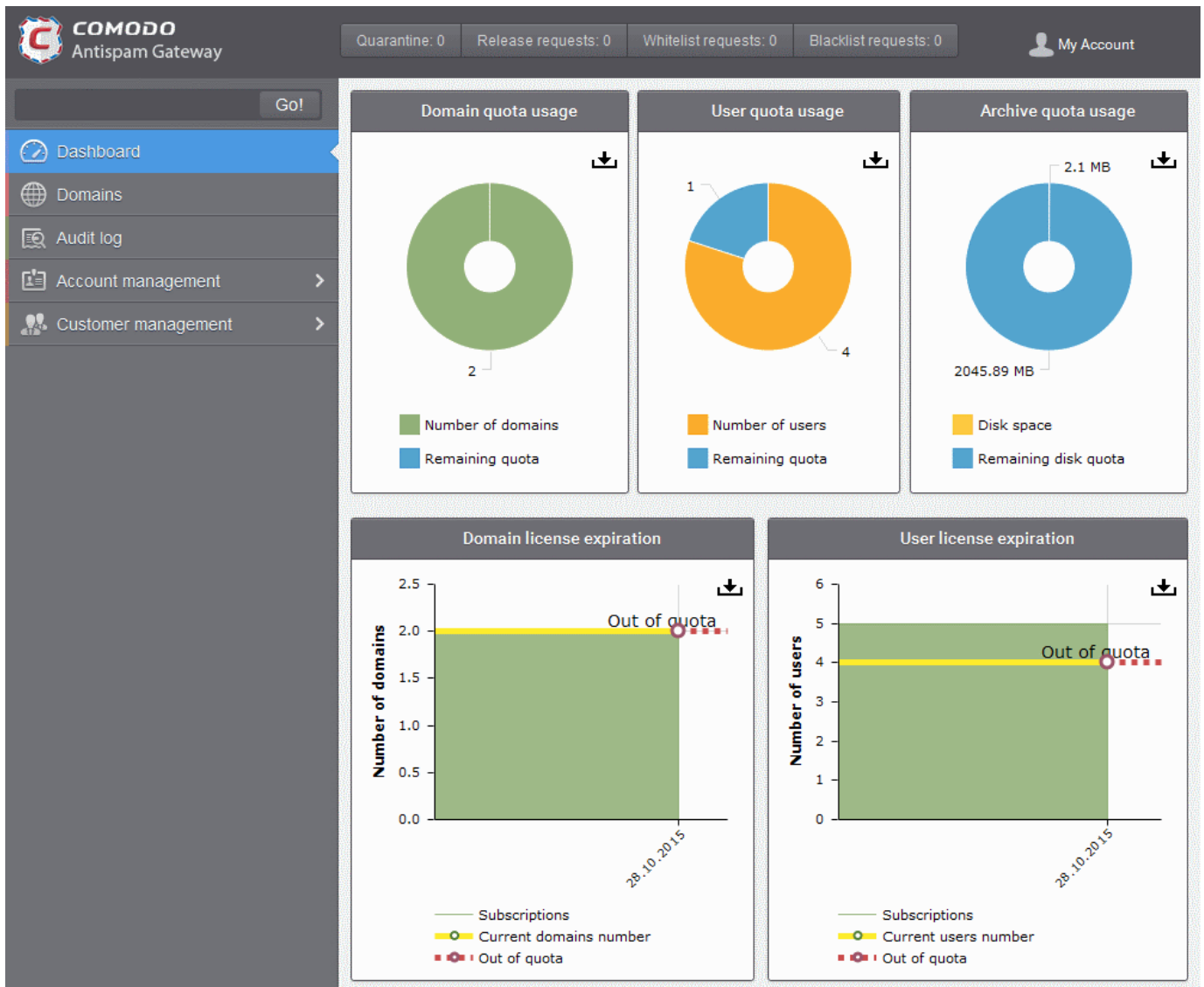
In order to ensure safety, CASG will lock the account if the login attempts fail for more than three attempts due to incorrect Username or Password. To unlock the account the administrator can contact their Comodo Account Manager.

The threshold number of unsuccessful login attempts before locking the account can also be customized by contacting the Comodo Account Manager.

Note: You can login to the interface using either the credentials created via CAM account or the administrative credentials created via the CASG interface. If you login using the CAM account credentials, an additional feature 'Login to my Comodo account' will be available in the Account management area through which you can manage your account such as subscribe for more licenses.

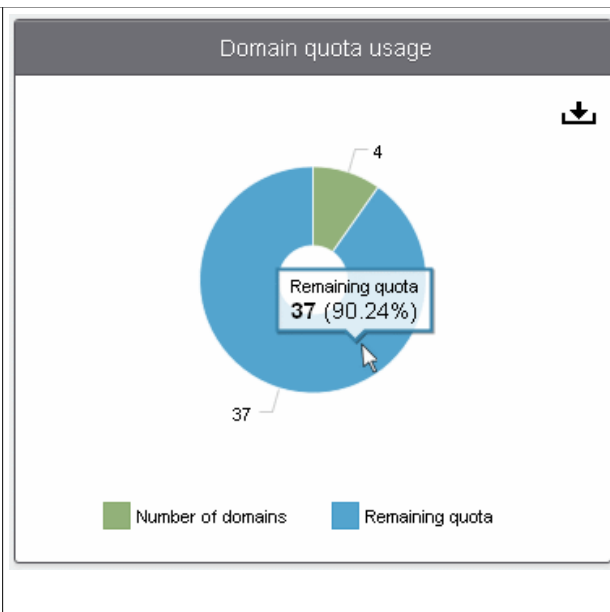
3.2 The Dashboard Area

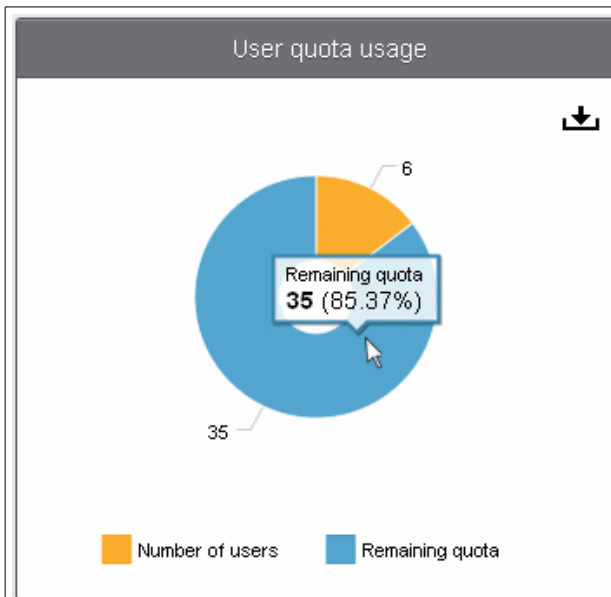
The Dashboard displays a snapshot summary of domain, user and archive quota usage as pie charts and domain and user license expiration as graphs. Administrators can download the pie charts and graphs as image or pdf files by clicking the download icon at the top right side of each item.



Domain Quota Usage

The 'Domain quota usage' pie chart provides the details of number of used and remaining domains for the account. Hovering the mouse cursor or clicking over a sector displays a call-out providing respective details. Clicking on a legend turns on / off respective metric on the chart.



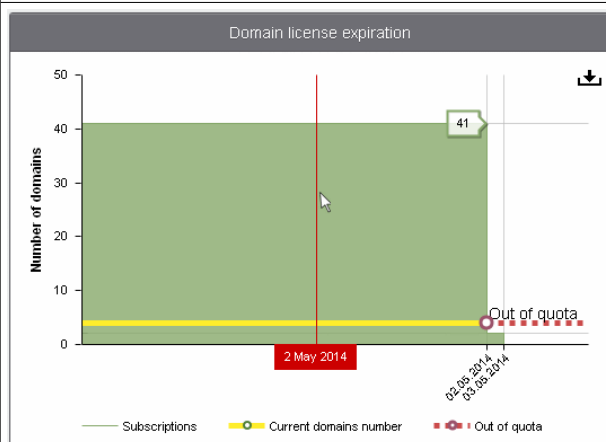
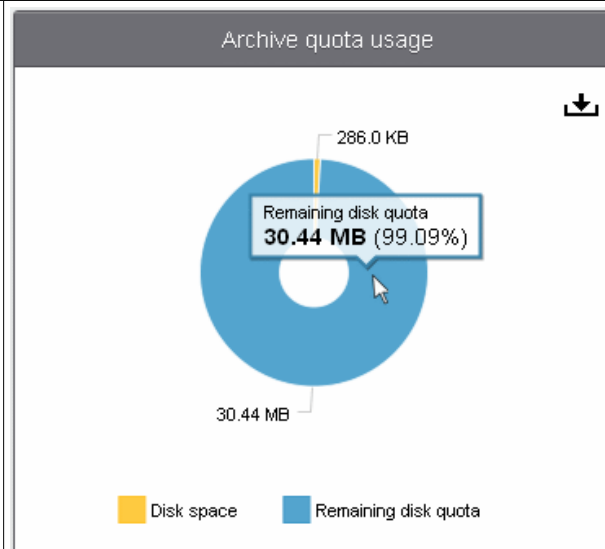


User Quota Usage

The 'User quota usage' pie chart provides the details of number of used and remaining users for the account. Hovering the mouse cursor or clicking over a sector displays a call-out providing respective details. Clicking on a legend turns on / off respective metric on the chart.

Archive Quota Usage

The 'Archive quota usage' pie chart provides the details of used and remaining archive space for incoming mails for the account. Hovering the mouse cursor or clicking over a sector displays a call-out providing respective details. Clicking on a legend turns on / off respective metric on the chart.

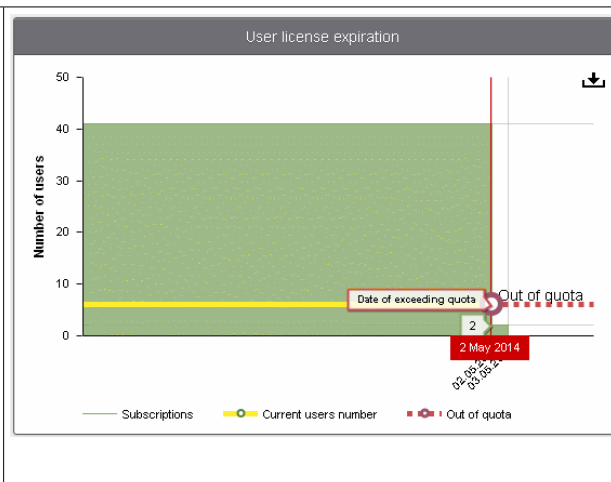


Domain License Expiration

The 'Domain license expiration' graph provides at-a-glance summary of domains that can be added for the account and their licenses expiry dates. The number of domains that is allowed for the account is displayed in X axis and the Y axis indicates the dates when the licenses for these domains are set to expire. Hovering the mouse cursor over any part of the graph displays when the current license is set to expire. It also displays if any license has expired. The yellow line indicates the total number of domains added for the account. Out of quota indicates the date the domains added for the account exceeds for a license.

User License Expiration

The 'User license expiration' graph provides at-a-glance summary of users that can be added for the account and their license expiry dates. The number of users that is allowed for the account is displayed in X axis and the Y axis indicates the dates when the subscriptions for these users are set to expire. Hovering the mouse cursor over any part of the graph displays when the current subscription is set to expire. It also displays if any subscription has expired. The yellow line indicates the total number of users added for the account. Out of quota indicates the date the users added for the account exceeds for a license.



3.2.1 Domain Management

The 'Domains' area of the interface allows administrators to perform domain management tasks such as adding, deleting editing and managing a domain. Various settings such as email size restrictions and extensions of attached files in emails can be configured for any listed domain. The interface also allows administrators to view logs of changes such as whitelist a recipient, blacklist a recipient and so on for all the domains in the account.

Tip: CASG also periodically generates Domains reports containing a summary of all the mail activities for the domain. The reports are sent to the administrators through email. Administrators can configure for such reports through **Dashboard > Account Management > Admin > Add Administrators** or **Edit Administrators**. Refer to **CASG Reports - An Overview** for more details.

The screenshot shows the 'Domains' management page. At the top, there are status indicators: Quarantine: 4, Release requests: 0, Whitelist requests: 0, Blacklist requests: 0. The left sidebar contains navigation options: Dashboard, Domains (selected), Audit log, Account management, and Customer management. The main content area shows a table of domains with the following data:

Domains	Aliases	Number of users	Max. number of users
docteamcasg.comodo.od.ua		4	Unlimited
dsg-arch-qa.comodo.od.ua		0	Unlimited

At the bottom of the table, there is a pagination control showing '1 / 1' and '[1 - 2 / 2]', and a 'Per page' dropdown set to 15.

The following section provides more information on **Domains**.

3.2.1.1 Domains

As the name suggests, the The 'Domains' area of the interface allows administrators to perform domain management tasks such as adding, deleting, editing a domain. Various settings such as email size restrictions and extensions of attached files in emails can be configured for any listed domain.

- Click the Domains tab in the left hand side navigation to open the Domains area.

Quarantine: 4 | Release requests: 0 | Whitelist requests: 0 | Blacklist requests: 0 | My Account

Dashboard / Domains

Domains

Filters

Domains	Aliases	Number of users	Max. number of users
<input type="checkbox"/> docteamcasg.comodo.od.ua		4	Unlimited
<input type="checkbox"/> dsg-arch-qa.comodo.od.ua		0	Unlimited

/ 1 | [1 - 2 / 2] | Per page 15

Having Trouble? Support is here to help. Open a Ticket at support.comodo.com or call 1.888.COMODO (256.2608)

The list of domains that are configured will be displayed.

Sorting the Entries

Clicking the domain column heading switches the sorting of the entries based on the ascending/descending order of the entries.

Using Filter options to search particular domain(s)

Click anywhere on the Filters tab to open the filters area.

Dashboard / Domains

Domains

Filters

Domain contains

Domains	Aliases	Number of users	Max. number of users
<input type="checkbox"/> docteamcasg.comodo.od.ua		4	Unlimited
<input type="checkbox"/> dsg-arch-qa.comodo.od.ua		0	Unlimited

/ 1 | [1 - 2 / 2] | Per page 15

You can add more filters by clicking  for narrowing down your search.

Dashboard / Domains

Domains

[+ Add](#)
[Delete](#)
[Edit domain](#)
[Manage domain](#)
[Refresh](#)

Filters

- Domain contains
- Domain equals
- Alias contains
- Domain starts with

Apply filter

<input type="checkbox"/> Domains	<input type="checkbox"/> Aliases	Number of users	Max. number of users
<input type="checkbox"/> example.domain.com		2	Unlimited
<input type="checkbox"/> example1.domain.com		0	Unlimited

You can remove a filter by clicking the icon beside it.

Available filters are:

- **Domain:** Will execute a search of domain names according to the text in the text box (column 3) and the condition selected in column 2.
- **Aliases:** Will execute a search of domain alias names according to the text in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following filters are available in the second drop-down:

- **Equals:** Displays the domain or alias name that was entered in full in the text box.
- **Contains:** Displays all domain or alias name(s) that contains the words entered in the text box.
- **Not Contains:** Displays all domain or alias name(s) that does not contain the words entered in the text box.
- **Starts With:** Displays all domain or alias name(s) that starts with the words entered in the text box.
- **Not Equals:** Displays all domain or alias name(s), except the one entered in the text box.
- **Ends With:** Displays all the domain or alias name(s) that ends with the words entered in the text box.

Click 'Apply Filter' after selecting the filters.

Click anywhere on the Filters tab to close the filters area.

Click the button to display all the domains.

Note: To display all the domains after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Click the following links to know how to:

- [Add a domain](#)
- [Delete a domain](#)
- [Edit a domain](#)
- [Manage a domain](#)

3.2.1.1.1 Adding Domains

From this interface, administrators with appropriate privileges can add domains, configure the number of users for each domain and the destination routes for respective domains. The number of domains that you can add depends on the plan that you have subscribed.

To add a domain

- Click the 'Add' button in the Domains interface



The 'Add domain' dialog will open.

Add domain

Domain

Destination routes + : 25

Timezone : (GMT +00:00)GMT

Domain user limit Unlimited

Check routes Save Cancel

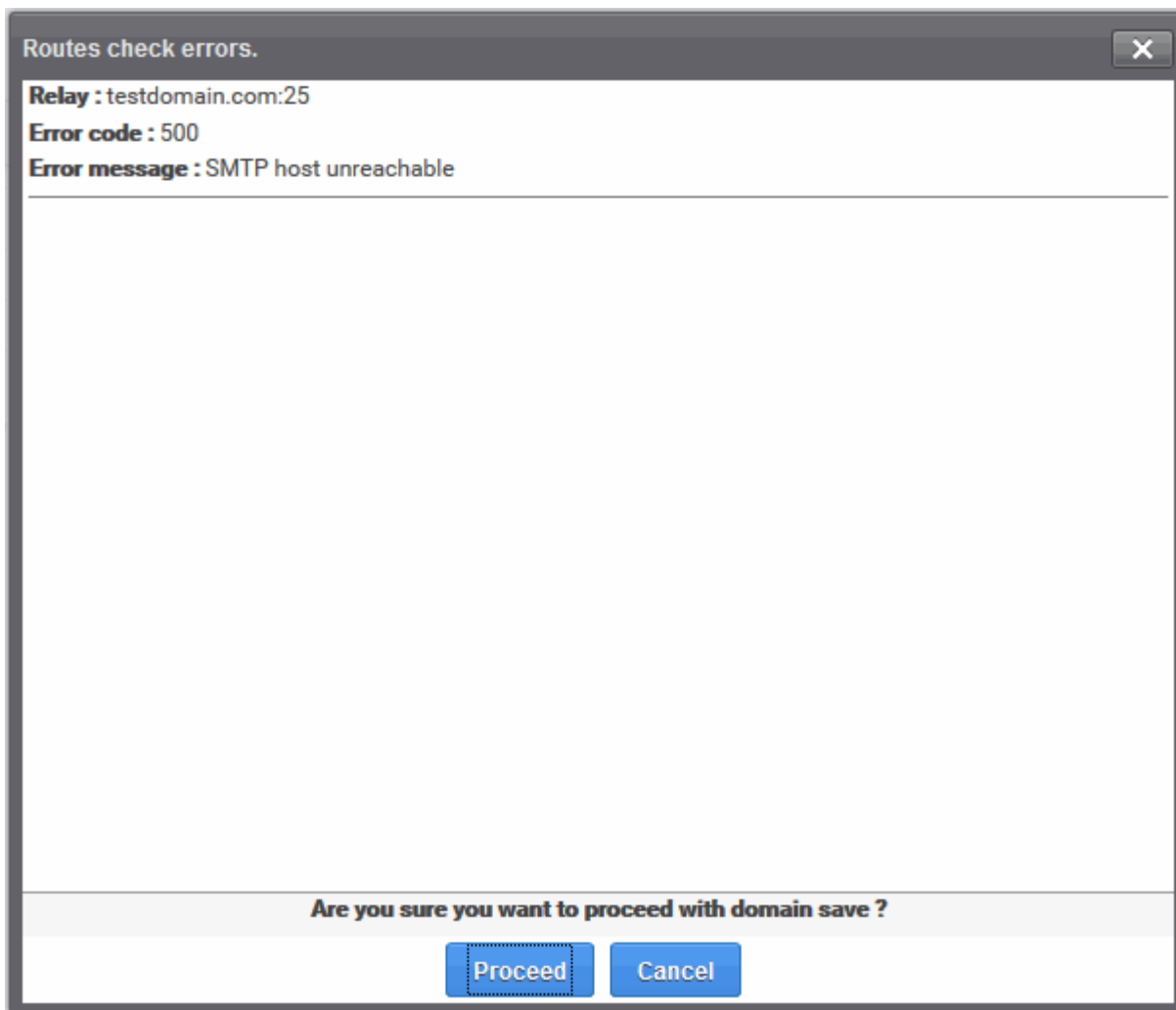
- Enter a valid domain name in the 'Domain' field.
- Enter the final mail server destination route in the 'Destination routes' field. This is where the mails will be delivered from CASG after appropriate filtering of mails. The default port is 25.
- If you want additional routes to be included for the filtered mails to be delivered in case of failure of the first route, click + beside the 'Destination routes' field to add more alternative destination routes.

The screenshot shows a dialog box titled "Add domain" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Domain:** A text input field containing "testdomain.com".
- Destination routes:** A list of two entries. The first entry is "mail.testdomain.com" with a green plus icon to its left and a dropdown menu showing "25". The second entry is "mail1.testdomain.com" with a red minus icon to its left and a dropdown menu showing "25".
- Timezone:** A dropdown menu showing "(GMT +01:00)Poland".
- Domain user limit:** A text input field containing "Unlimited".

At the bottom of the dialog, there are three buttons: "Check routes" (blue), "Save" (blue), and "Cancel" (grey).

- The 'Timezone' drop-down allows you to choose the zone for the domain. CASG will use the selected time-zone for events which concern that domain. Specifically, the quarantine list, archive list, log search, reports and report subscriptions.
- Click the 'Check routes' button to let CASG automatically get the destination routes information from DNS. If the result contains mxpool1.spamgateway.comodo.com then it means that DNS MX record was already updated to work with Antispam Gateway server and you must fill 'Destination routes' field with your real MX record, for example mail.exempldomain.com.
- Enter the maximum numbers of users that can be added for this domain in the 'Domain user limit' field. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license. The maximum number of users for a selected domain can also be configured in the **Domain Settings** area.
- The domain entered in the 'Destination routes' field is checked by Comodo Gateway diagnostic tool to assure the destination route is entered by administrator correctly.



- Click 'Proceed' to save a domain.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field, but CASG checks if the total number of users for all domains is within your license limit.

- Click 'Save' to add the configured domains.

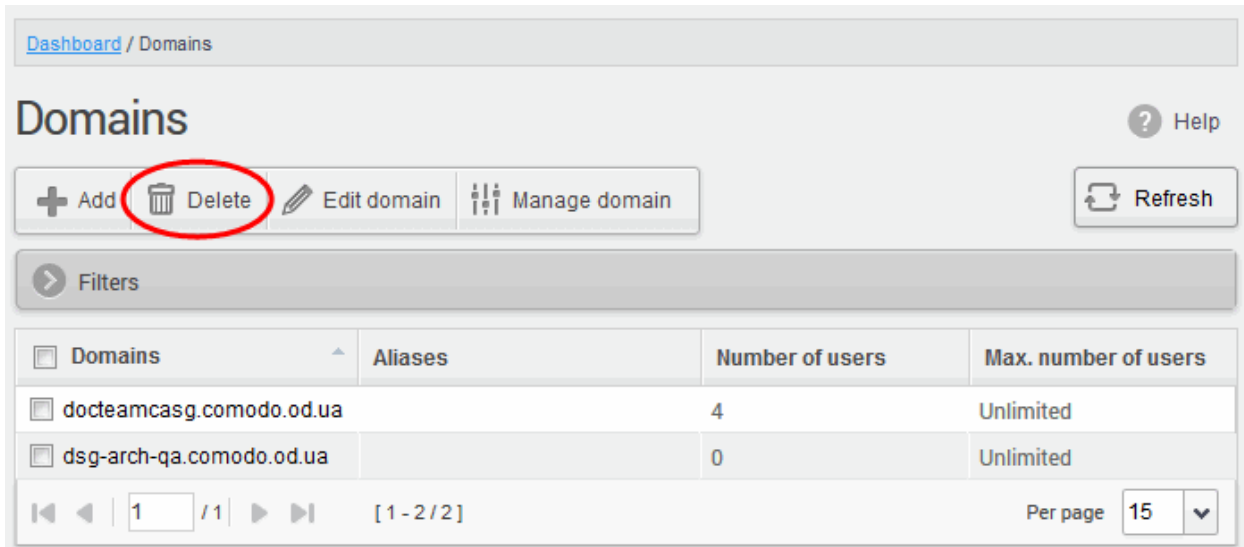
Note: When you create a new domain, email addresses 'abuse@addeddomain' and 'postmaster@addeddomain' will be added by default in Recipient Whitelist. [Click here](#) for more details.

3.2.1.1.2 Deleting Domains

If you want to delete a domain for which emails are being routed via CASG, this can be done in this interface.

To delete a domain

- Select the domain(s) that you want to delete from the interface.



Dashboard / Domains

Domains

Help

+ Add **Delete** Edit domain Manage domain Refresh

Filters

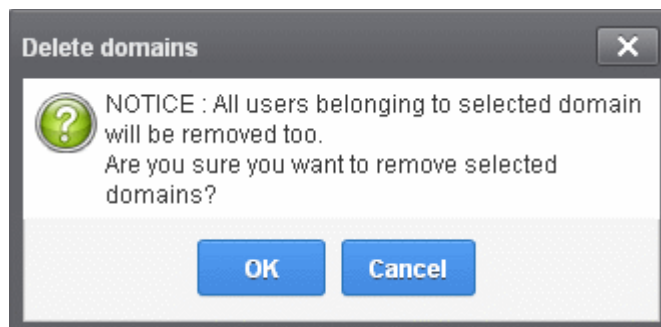
<input type="checkbox"/> Domains	Aliases	Number of users	Max. number of users
<input type="checkbox"/> docteamcasg.comodo.od.ua		4	Unlimited
<input type="checkbox"/> ds-g-arch-qa.comodo.od.ua		0	Unlimited

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

- Click the "Delete" button

Tip: You can select multiple domains to delete by pressing and holding the Shift or Ctrl keys.

A notice will be displayed warning you that the users belonging to the selected domains to be deleted will also be removed.



- Click 'OK' to confirm.

The selected domain(s) will be deleted.

3.2.1.1.3 Editing Domains

You can change the destination routes of a configured domain and check routes for the edited domain. Please note that the name of the domain cannot be edited.

To edit a domain

- Select the domain that you want to edit from the interface.

Dashboard / Domains

Domains ? Help

Filters

<input type="checkbox"/> Domains	Aliases	Number of users	Max. number of users
<input type="checkbox"/>	docteamcasg.comodo.od.ua	4	Unlimited
<input type="checkbox"/>	dsg-arch-qa.comodo.od.ua	0	Unlimited

/ 1 [1 - 2 / 2]
Per page

- Click the 'Edit domain' button

The Edit domain dialog will be displayed. Please note that the domain name is not editable.

Edit domain ✕

Domain

Destination routes +

Max. number of users

From here you can add another destination route, change the primary destination route or delete additional destination routes and reconfigure the maximum number of users for that domain.

- Click in the 'Destination route' field to edit it.
- Click + beside the 'Destination routes' field to add more alternative destination routes.

Edit domain ✕

Domain

Destination routes +

-

Max. number of users

- Click - to remove alternative destination routes.

- Click the 'Check routes' button to let CASG automatically get the destination routes information from DNS. If the result contains mxpool1.spamgateway.comodo.com then it means that DNS MX record was already updated to work with Antispam Gateway server and you must fill 'Destination routes' field with your real MX record, for example mail.testdomain.com.
- If required, edit the maximum of number of users that can be added for this domain in the 'Max. number of users' field. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license.
- The domain entered in the 'Destination routes' field is checked by Comodo Gateway diagnostic tool to assure the destination route is entered by administrator correctly.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field, but CASG checks if the total number of users for all domains is within your license limit.

- Click 'Save' to confirm the changes.

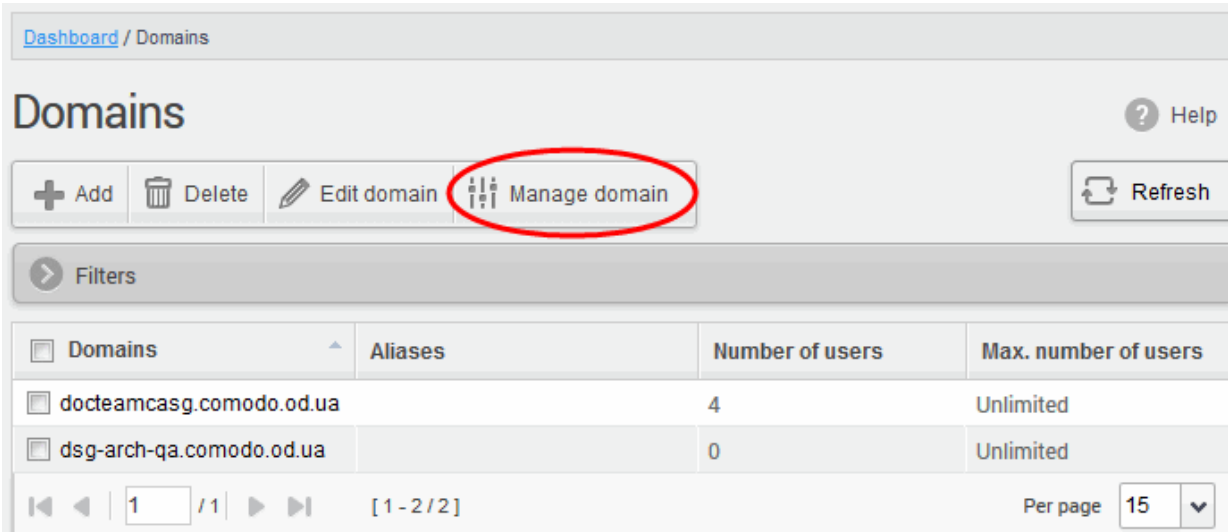
3.2.1.1.4 Managing Domain

In this area, an administrator can configure various settings for a selected domain. This interface allows the administrator to view quarantined mails, set email restrictions, add users as recipient whitelist or blacklist, add new users and view log reports for the domain.

This section is divided into seven main subsections namely, Domain dashboard, Incoming, Outgoing, Email management, Audit log, Domain Rules and Account management. Click on the respective tab to expand or close the subsection in the left hand side navigation.

To manage a domain

- Select the domain that you want to manage from the interface and click the 'Manage Domain' button.
- or
- Click on the domain name in the 'Domains' column.
- or
- Right-click on the domain name in the 'Domains' column to open in a new tab or window.



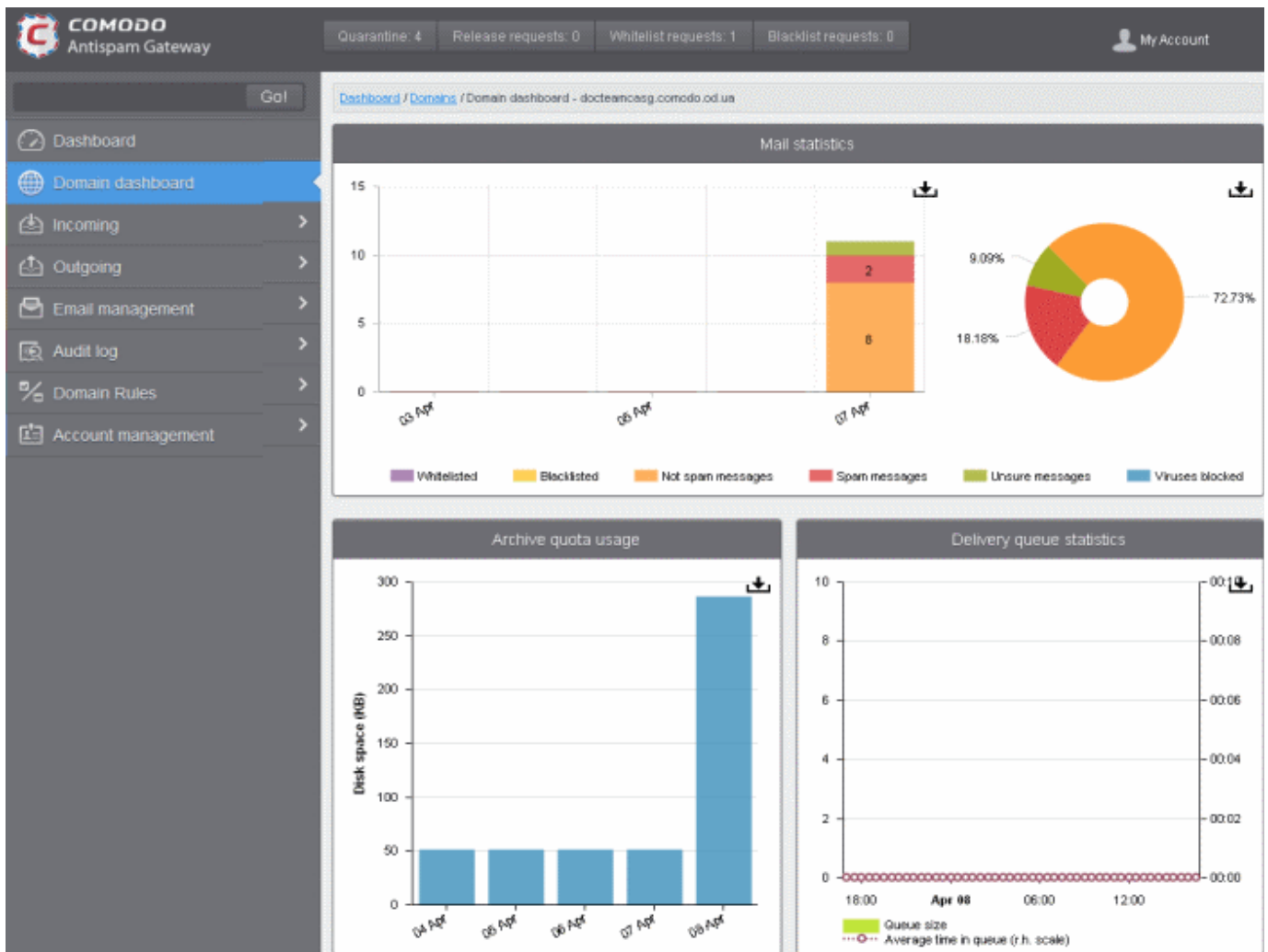
The screenshot shows the 'Domains' management interface. At the top, there is a breadcrumb 'Dashboard / Domains' and a 'Help' icon. Below the title 'Domains', there are several action buttons: '+ Add', 'Delete', 'Edit domain', and 'Manage domain' (which is circled in red). A 'Refresh' button is also present. Below the buttons is a 'Filters' section. The main content is a table with the following data:

<input type="checkbox"/> Domains	Aliases	Number of users	Max. number of users
<input type="checkbox"/>	docteamcasg.comodo.od.ua	4	Unlimited
<input type="checkbox"/>	dsg-arch-qa.comodo.od.ua	0	Unlimited

At the bottom of the table, there is a pagination control showing '1 / 1' and '[1 - 2 / 2]', and a 'Per page' dropdown set to '15'.

In the left hand side navigation, the configuration tabs for the selected domain will open. By default, the Domain

dashboard for the selected domain will be displayed. Click on the tabs in the left side to open the respective interfaces.



Click on the following links for more details on the subsections:

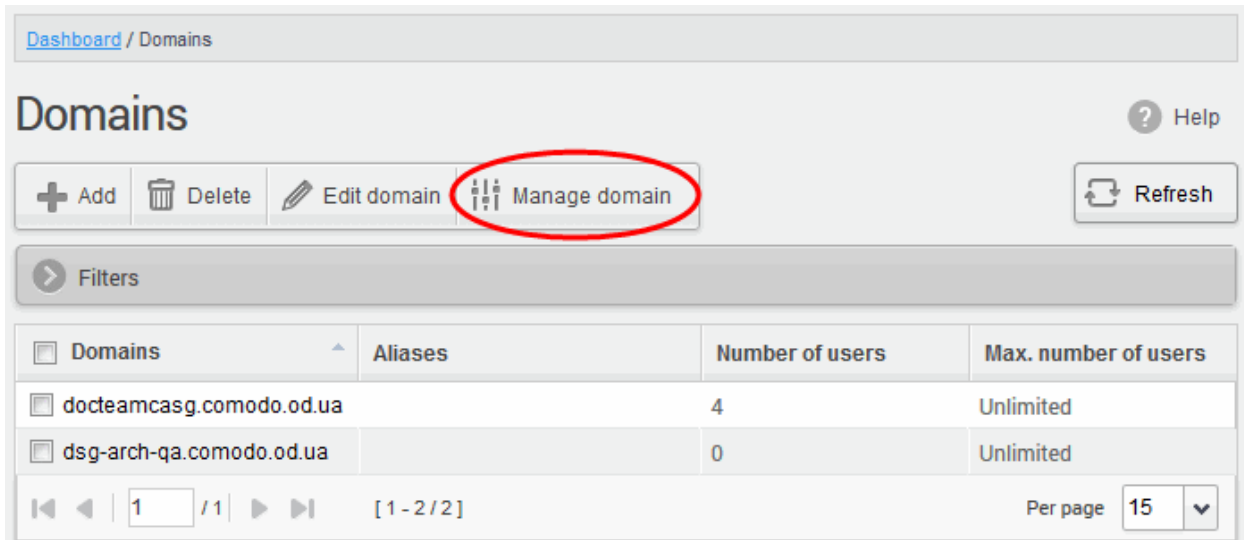
- [Domain Dashboard](#)
- [Incoming](#)
- [Outgoing](#)
- [Email Management](#)
- [Domain Audit Log](#)
- [Domain Rules](#)
- [Account Management](#)

3.2.1.1.4.1 Domain Dashboard

CASG provides a dashboard view of a selected domain for quick analysis of important statistics such as number of quarantined mails, release requests, whitelist requests, blacklist requests, incoming mails archive quota usage and more. Administrators can download the pie charts and graphs as image or pdf files by clicking the download icon at the top right side of each item. To open a domain dashboard, click Domains tab on the left hand side and then:

- Select the domain that you want to view its dashboard and click the 'Manage Domain' button.
- or

- Click on the domain name in the 'Domains' column.
- or
- Right-click on the domain name in the 'Domains' column to open in a new tab or window.



The dashboard of the selected domain will be displayed.

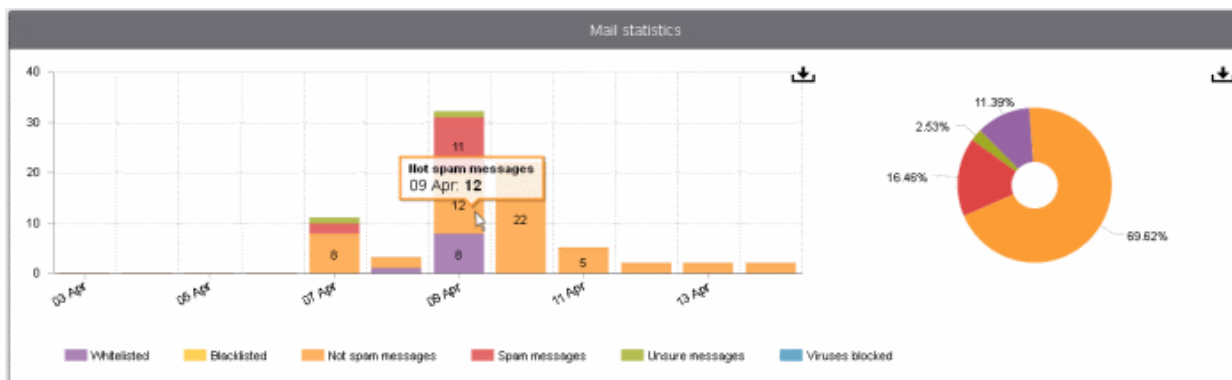


Clicking on the buttons at the top of the domain dashboard takes you to the respective interface:

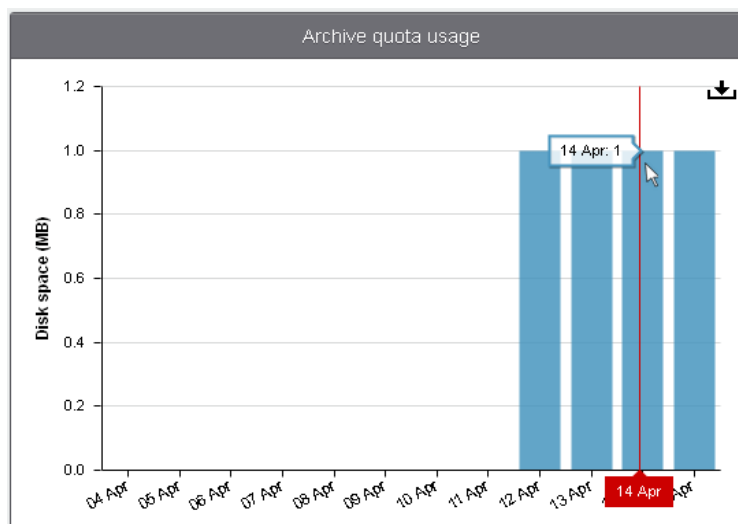
- **Quarantine** - Displays the quarantined mails of all users of the selected domain. Refer to the section **Quarantine** for more details.

- **Release requests** - Displays the requests from users of the selected domain for releasing quarantined mails. Refer to the section **Released Requests** for more details.
- **Whitelist requests** - Displays the requests from users of the selected domain for whitelisting the senders of quarantined mails. Refer to the section **Whitelisted Requests** for more details.
- **Blacklist requests** - Displays the requests from users of the selected domain for blacklisting the senders of quarantined mails. Refer to the section **Blacklisted Requests** for more details.

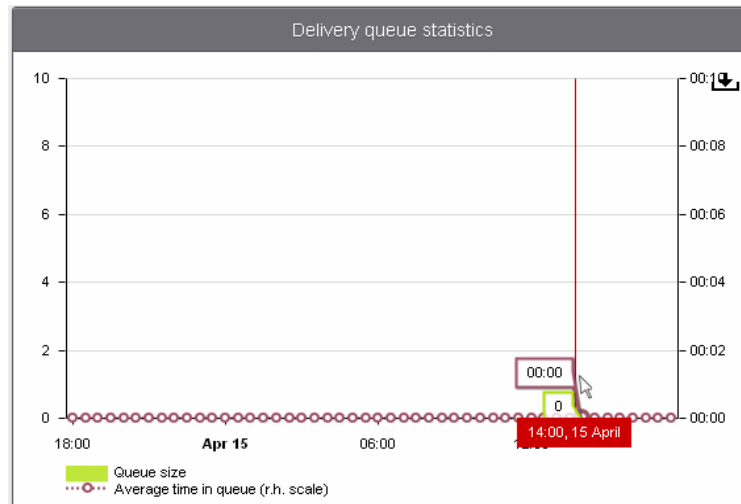
The Mails Statistics area provides a graphical as well as pie chart representation of the mails that were blocked, viruses blocked and more. Hovering the mouse cursor over a sector or graph displays a call-out providing respective details. Clicking on a legend turns on / off respective metric on the chart and graph.



The 'Archive quota usage' area provides details of the storage space used for archiving incoming mails. The graph shows the disk space used per day for the last two weeks. Hovering the mouse cursor over any part of the graph displays the details of the space used for the respective date. Refer to the section **Managing Archived Mails** for more details.

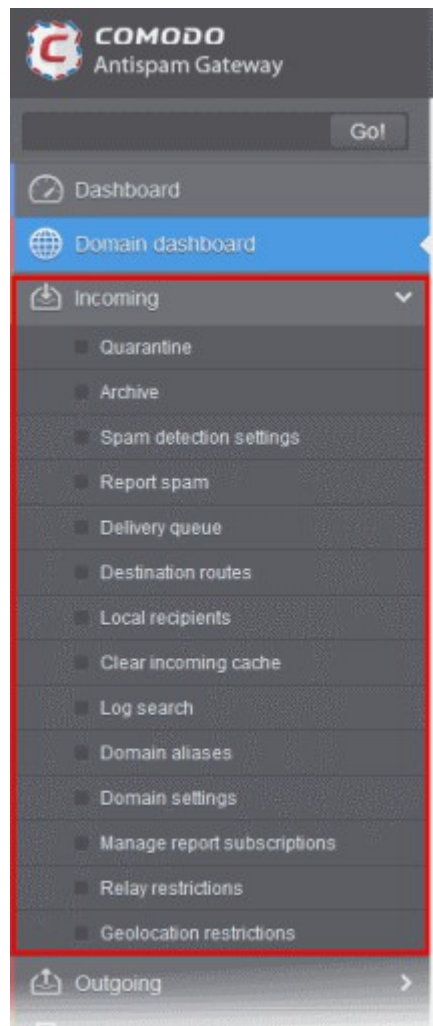


The 'Delivery queue statistics' area provides details of filtered mails that are queued in CASG servers for delivery at a later time. It also displays the average time of queued mails for the previous day in CASG servers before delivery. Refer to the section **Delivery Queue** for more details.



3.2.1.1.4.2 Incoming

The 'Incoming' area of the Manage Domain section allows you to view quarantined mails, configure incoming spam detection settings, set spam alert headings, add local email recipients and more.



Click the following links for more details:

- [Quarantine](#)
- [Managing Archived Mails](#)

- [Incoming Spam detection settings](#)
- [Report Spam](#)
- [Delivery Queue](#)
- [Destination Routes](#)
- [Local Recipients](#)
- [Clear Incoming Cache](#)
- [Log Search](#)
- [Domain Aliases](#)
- [Domain Settings](#)
- [Manage Report Subscriptions for Selected Domain](#)
- [Relay Restrictions](#)
- [Geolocation Restrictions](#)

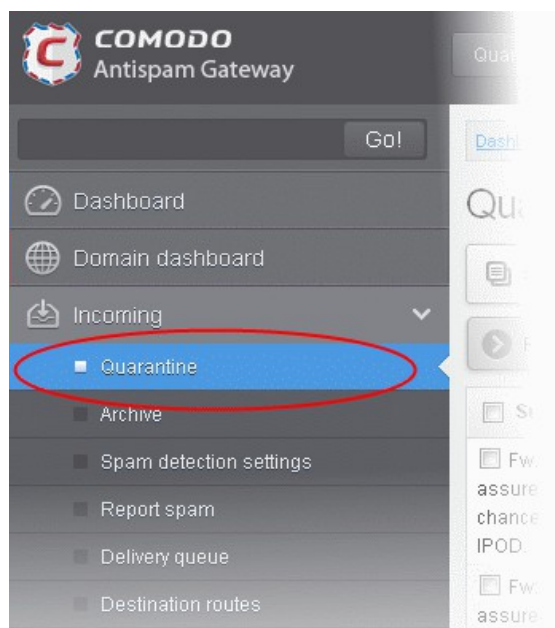
Quarantine

In this area, an administrator can view the list of all the quarantined emails and their headers, of all the users for the selected domain. The administrator can also choose to release quarantined emails to the intended recipient after ascertaining that particular email is not actually a spam. The administrator also can delete a selected or all the spam mails from this interface.

Tip: CASG also periodically generates Quarantine reports containing a summary of mails identified as spam or malicious that were moved to quarantine automatically. The reports are sent to the administrators through email. Administrators can configure for such reports through [Dashboard > Account Management > Admin > Add Administrators](#) or [Edit Administrators](#). Refer to [CASG Reports - An Overview](#) for more details.

To open the quarantined email interface:

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Quarantine' tab.



The quarantined email area of the selected domain will open:

Dashboard / Domains / Domain_dashboard - docteamcasq.comodo.od.ua / Quarantine

Quarantine ? Help

Show message Release Delete More actions Refresh

Filters

Subject	From	To	Recipient	Date (GMT+)	Reason	Size		Actions
<input type="checkbox"/> Spam email 1	admin <demo@csg.comodo.od.ua>	demo1@docteamcasq.com	demo1@docteamcasq.com	Oct 28, 2014 1:21:46 PM	spam External pattern match (Sanesecurity.Junk.:	168 bytes		
<input type="checkbox"/> Spam email 2	admin <demo@csg.comodo.od.ua>	demo2@docteamcasq.com	demo2@docteamcasq.com	Oct 28, 2014 1:21:19 PM	spam External pattern match (Sanesecurity.Junk.:	168 bytes		

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

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search quarantined emails

Click anywhere on the Filters tab to open the filters area.

Dashboard / Domains / Domain_dashboard - docteamcasq.comodo.od.ua / Quarantine

Quarantine ? Help

Show message Release Delete More actions Refresh

Filters

+ Subject contains Apply filter

Subject	From	To	Recipient	Date (GMT+)	Reason	Size		Actions
					spam			

You can add more filters by clicking + for narrowing down your search.

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Subject:** Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From:** Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To:** Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size (KB):** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions are available:

- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

If 'Size' is selected, the following conditions are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box
- Click 'Apply Filter' after selecting the filters.
- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all the quarantined emails.

Note: To display all the quarantined emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

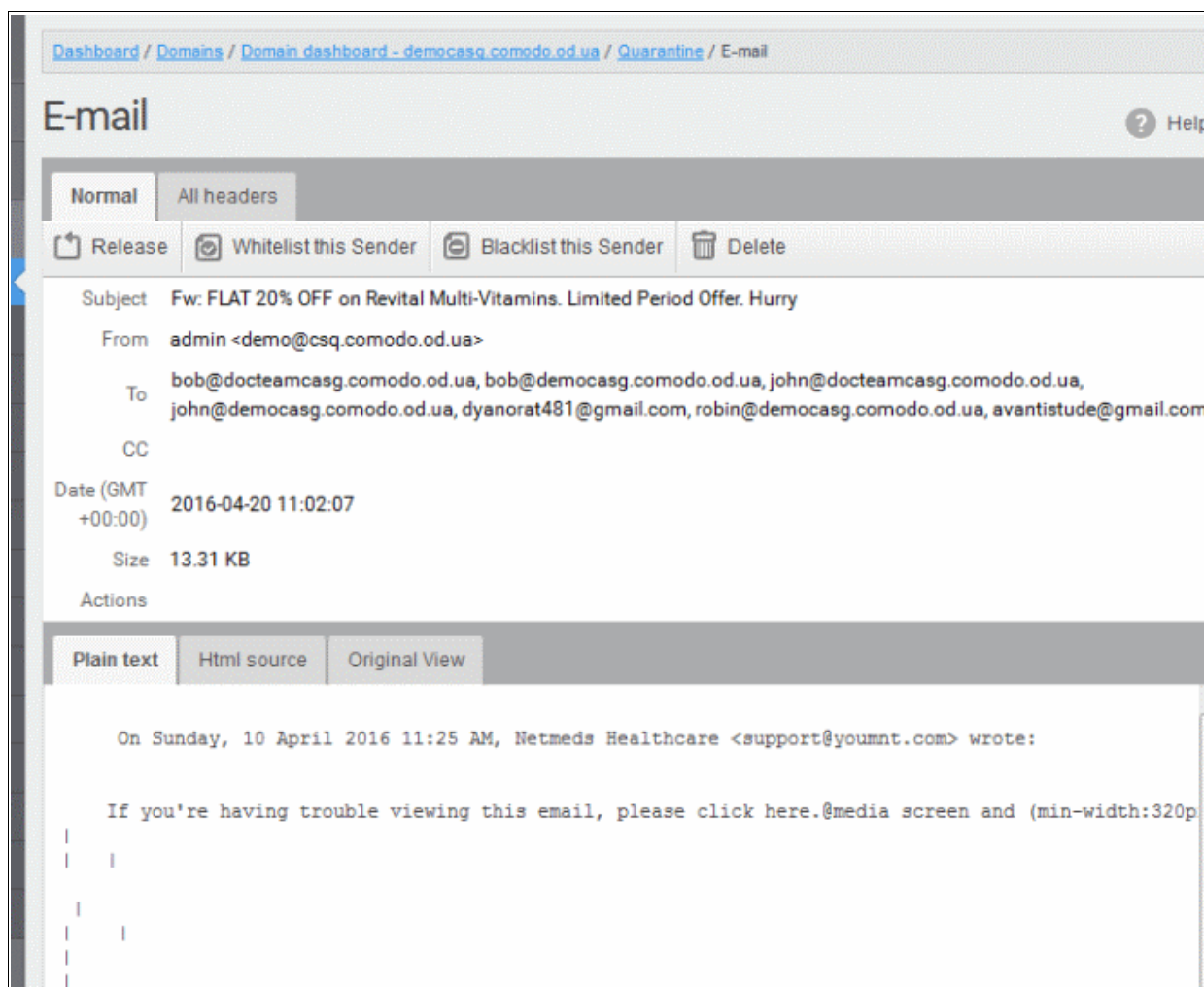
Viewing Details of Quarantined Mails

The details like subject, sender, recipient, date and size of the mails added to the Quarantine can be viewed in two ways:

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

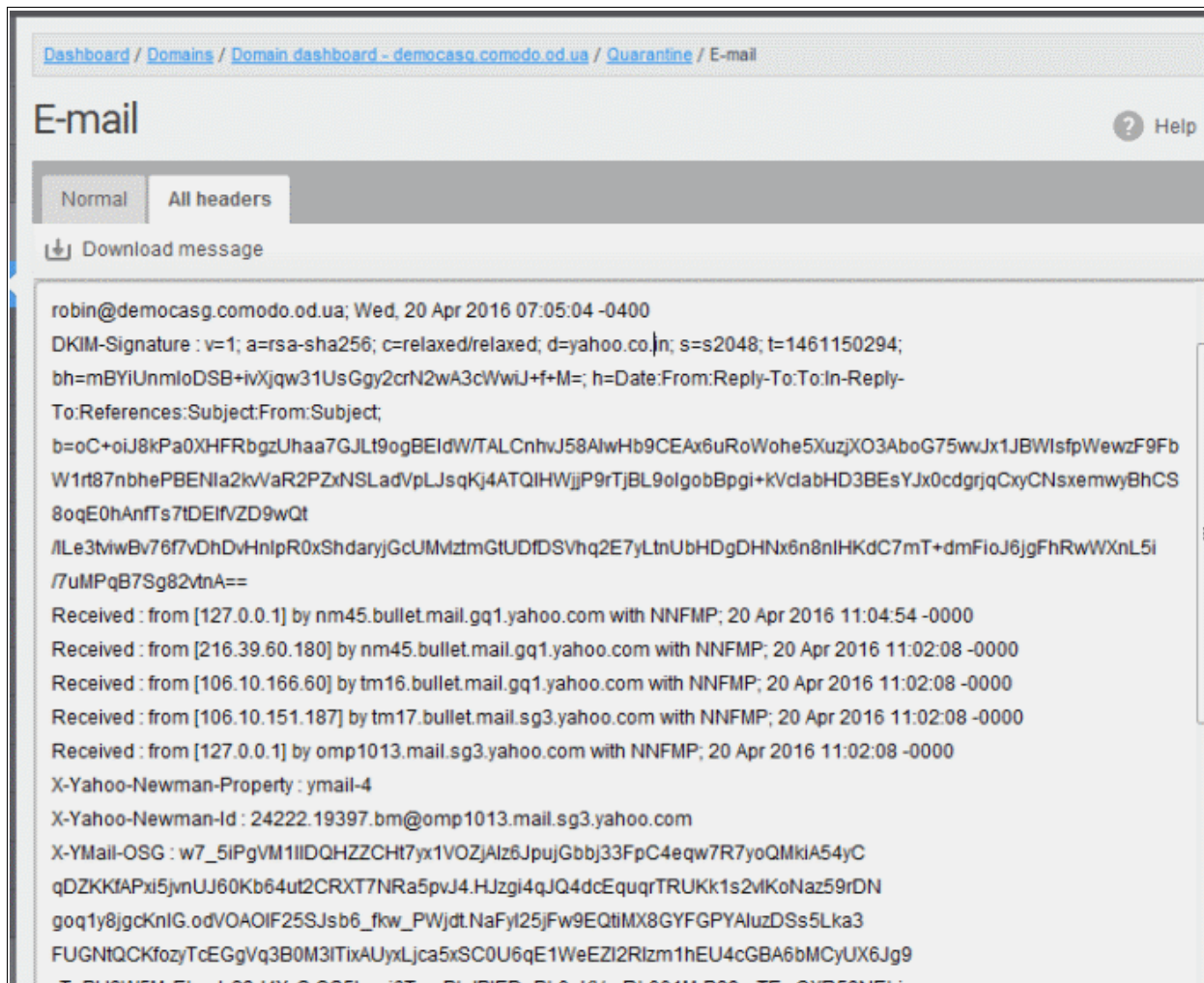
To view details of quarantined mails in the same CASG window:

- In the quarantined email area, 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 details of the selected email will be displayed.

To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient, click 'All headers' tab. 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.



Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either release the mail or delete it. Click the 'Whitelist this sender' tab to add the sender to **Sender Whitelist** if you desire or 'Blacklist this Sender' to add this sender to **Sender Blacklist**. Refer to the section **Whitelist / Blacklist** for more details.

To view the details of a quarantined mail in a new CASG window

- In the quarantined email area, select the mail that you want to view, right-click on the email link in the subject column and select to open in a new tab or new window.

Dashboard / Domains / Domain_dashboard - docteamcasg.comodo.od.ua / Quarantine

Quarantine

Help

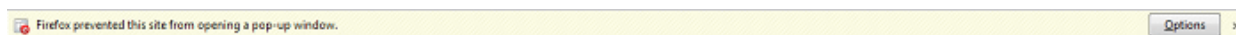
Show message Release Delete More actions Refresh

Filters

Subject	From	To	Recipient	Date (GMT+)	Reason	Size	Actions
<input checked="" type="checkbox"/> Spam email 1	admin <demo@csq.comodo.od.ua>	demo1@docteamcasg.com	demo1@docteamcasg.com	Oct 28, 2014 1:21:46 PM	spam External pattern match (Sanesecurity.Junk:..)	168 bytes	
<input type="checkbox"/> Spam		demo2@docteamcasg.com	demo2@docteamcasg.com	Oct 28, 2014 1:21:19 PM	spam External pattern match (Sanesecurity.Junk:..)	168 bytes	

Per page 15

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



Dashboard / Domains / Domain_dashboard - democaso.comodo.od.ua / Quarantine / E-mail

E-mail

Help

Normal All headers

Release Whitelist this Sender Blacklist this Sender Delete

Subject Spam email 1

From admin <demo@csq.comodo.od.ua>

To demo1@docteamcasg.com

CC

Date (GMT +00:00) 2016-04-20 11:02:07

Size 13.31 KB

Actions

Plain text Html source Original View

On Sunday, 10 April 2016 11:25 AM, Netmeds Healthcare <support@youmnt.com> wrote:

If you're having trouble viewing this email, please click here.@media screen and (min-width:320p

|

|

|

|

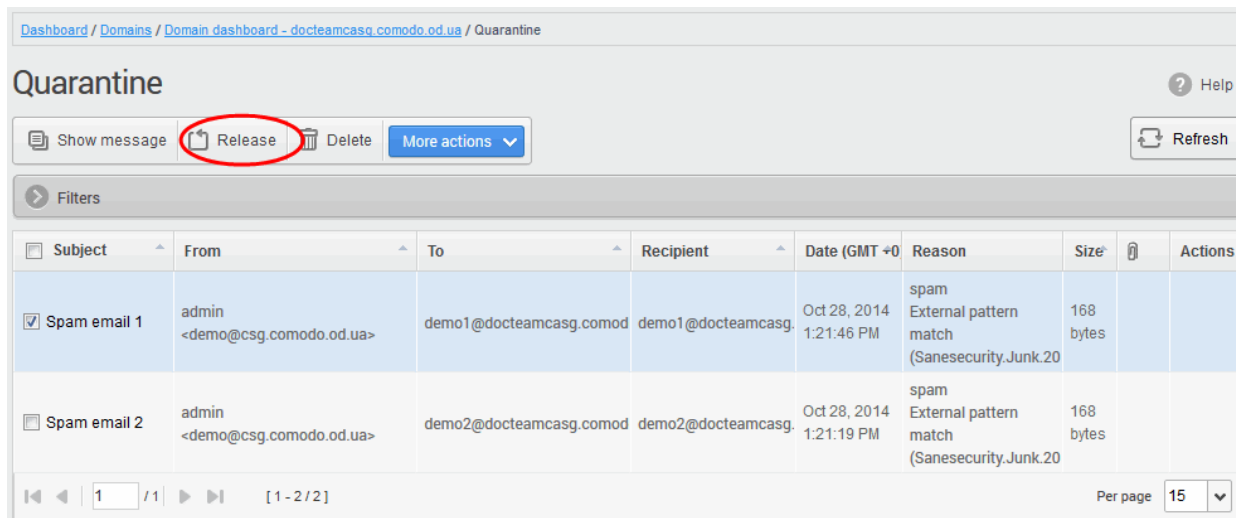
- 1800 103 0304

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

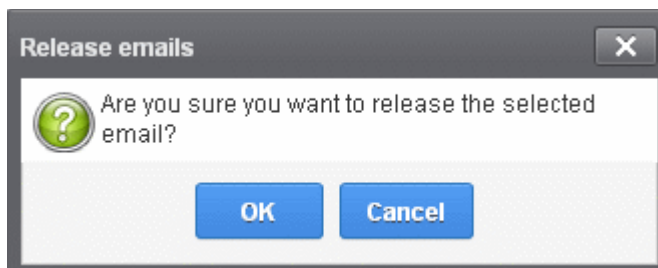
To release a quarantined mail:

After viewing the details and ensuring that the selected email is not a spam you can choose to release the mail to the recipient.

- Select the mail that you want to release and click the 'Release' button.



An alert will be displayed to confirm the release of selected email.



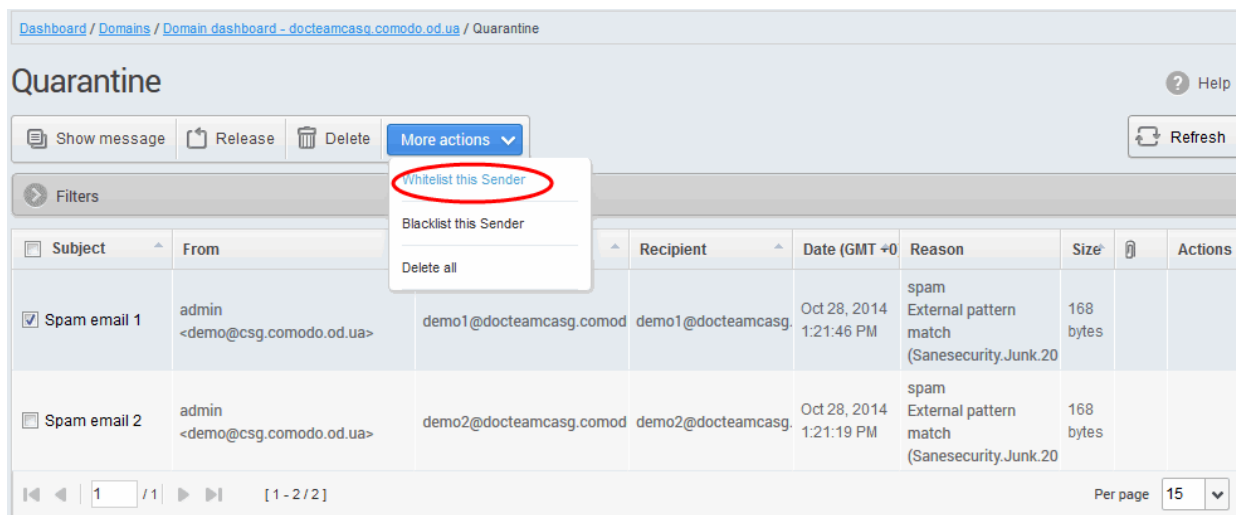
- Click 'OK' to confirm the release

The email will be released to the addressee and the mail will no longer be in the quarantined list.

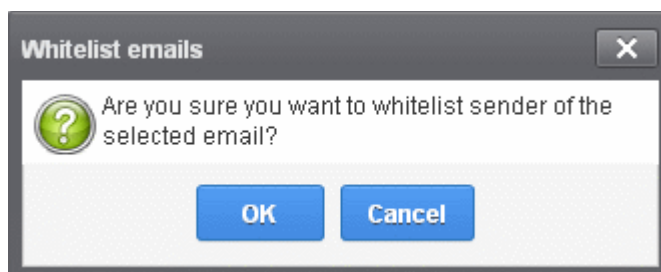
To add a sender to whitelist

After ascertaining that emails sent by particular senders are not spam, administrators can choose to add them to **Sender Whitelist** from this interface. Once added to whitelist, emails sent by these senders will not be quarantined.

- Select the mail that you want to add the sender to whitelist and then click 'More actions' > 'Whitelist this Sender'.



An alert will be displayed to confirm adding the sender to whitelist.

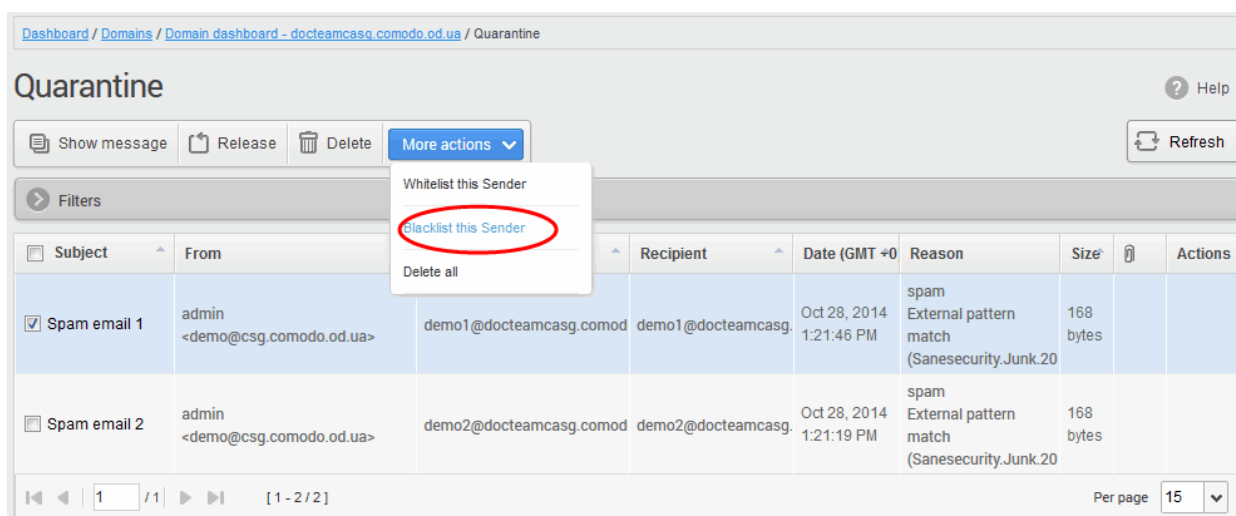


- Click 'OK' to confirm to add the sender to whitelist. Refer the section '**Sender Whitelist**' for more details.

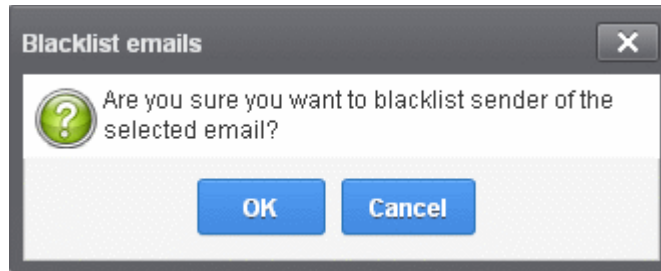
To add a sender to blacklist

Administrators can choose to add senders to '**Sender Blacklist**' from the Quarantine interface also. Once the selected senders are added to blacklist, all emails from them to the selected domain will be automatically blocked.

- Select the mail that you want to add the sender to blacklist and then click 'More actions' > 'Blacklist this Sender'.



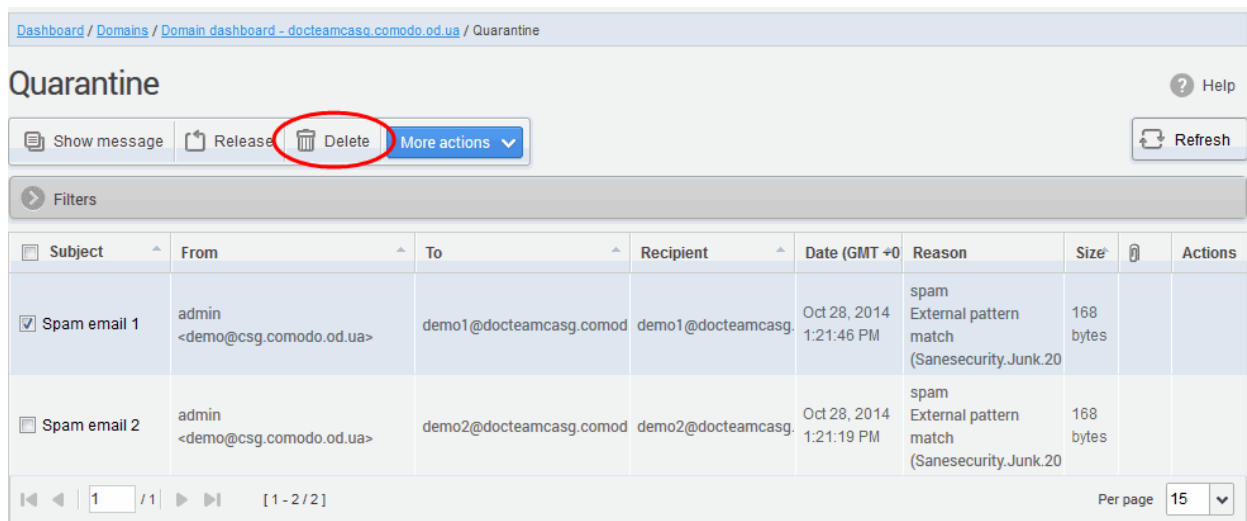
An alert will be displayed to confirm adding the sender to blacklist.



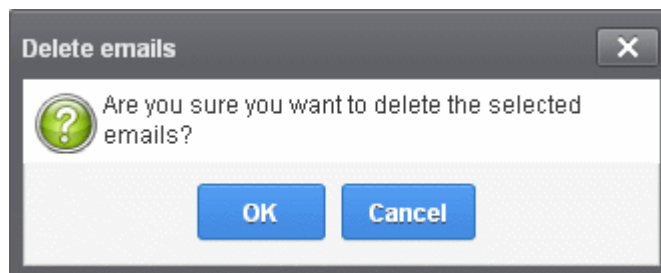
- Click 'OK' to confirm to add the sender to blacklist. Refer the section '**Sender Blacklist**' for more details.

To delete a quarantined mail:

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

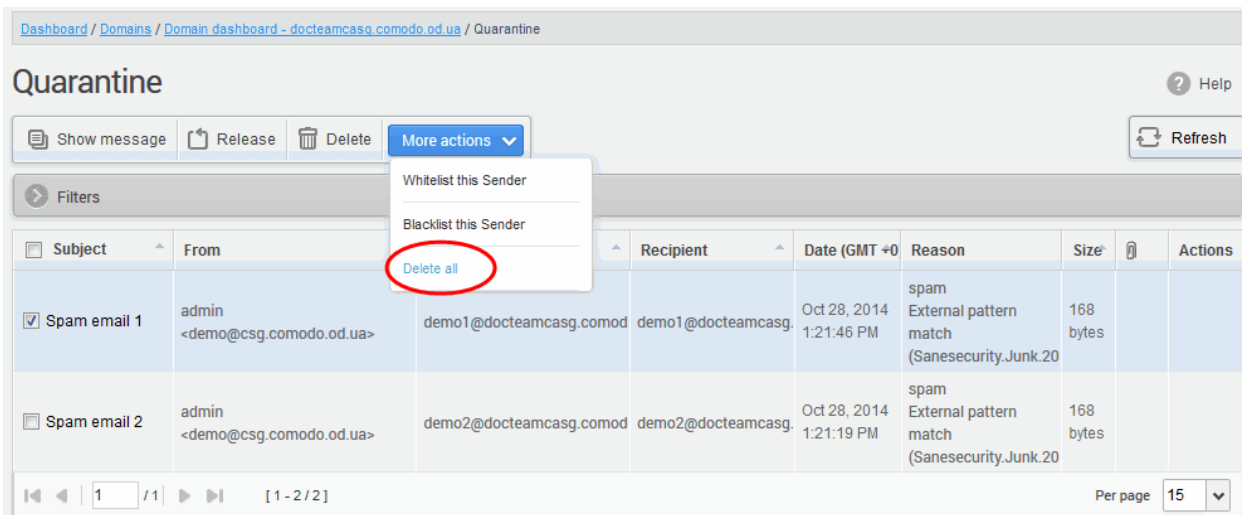


An alert will be displayed to confirm the deletion. Click 'OK' to delete the selection email.

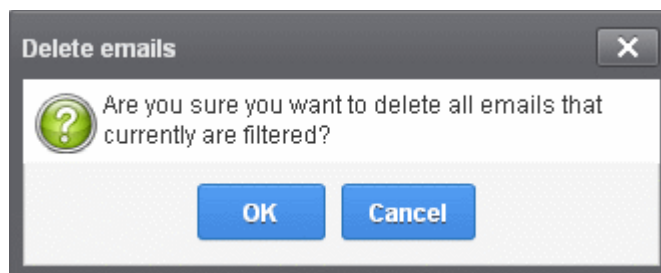


The selected mail will be deleted and will no longer be in the quarantined mail list.

- To delete all the quarantined mails, click 'More actions' > 'Delete all'.



An alert will be displayed to confirm the deletion. Click 'OK' to delete all quarantined emails.



All the quarantined emails for the selected domain will be deleted .

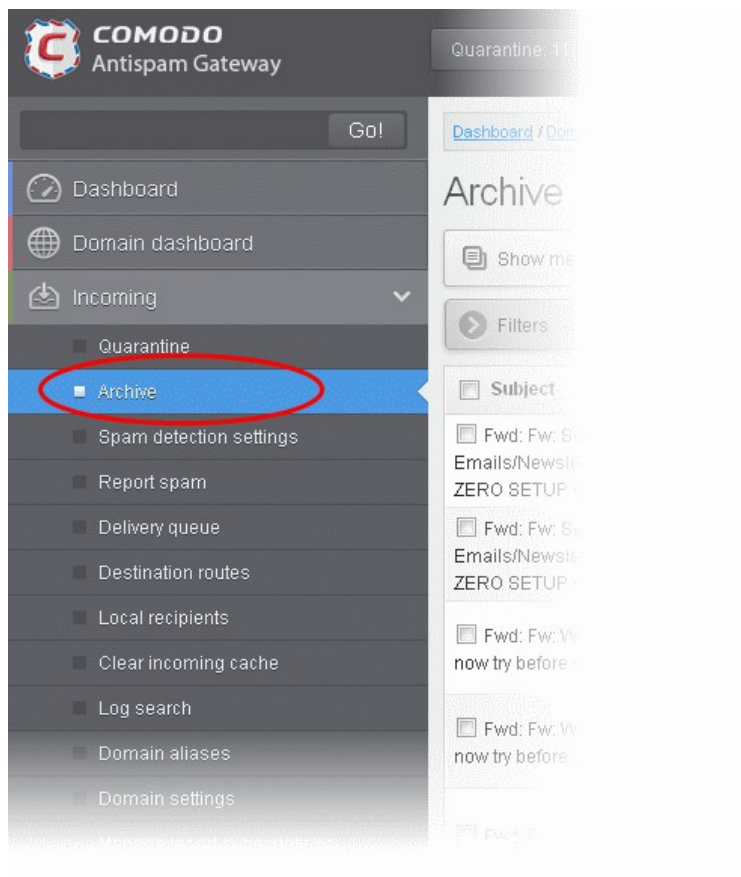
Managing Archived Mails

CASG is capable of storing a copy of all incoming mails for all domains belonging to an account. A customer can purchase the archive storage space via Comodo Accounts Manager (CAM).

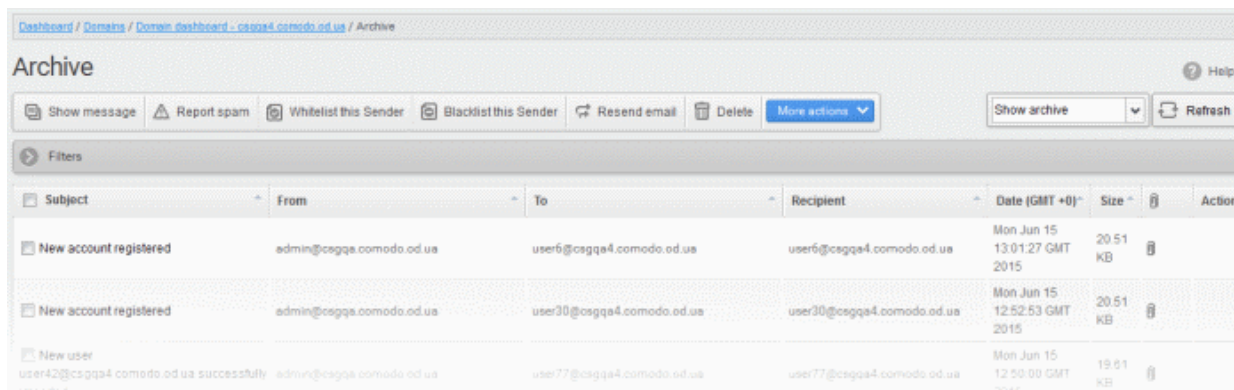
From the archived mails interface, an administrator with appropriate privileges can view details of the message, report spam, resend emails if required, retain messages from being removed, add the sender to **Domain Rules** and delete messages. The archived messages can be deleted manually or can be automated to be cleaned periodically. The settings for auto cleanup can be configured in the **Domains Settings** interface.

To open the archived email interface:

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Archive' tab.



The archived email area of the selected domain will open:

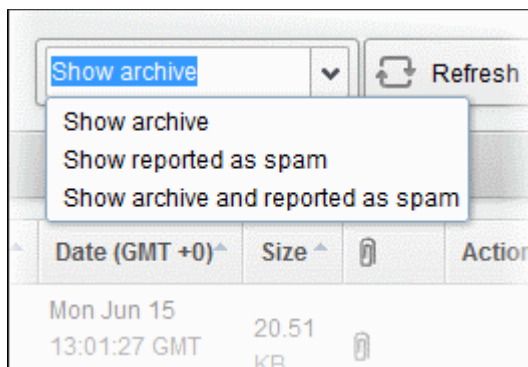


Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Page Filter

The page filter on the right side has three options:

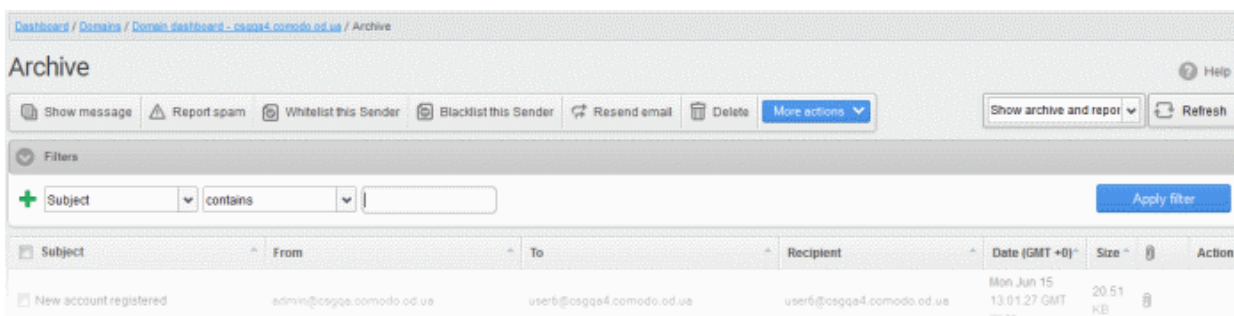


- **Show archive:** Lists only the archived mails
- **Show reported as spam:** Lists mails that are reported as spam
- **Show archive and reported as spam:** Lists both archived mails and mails that are reported as spam

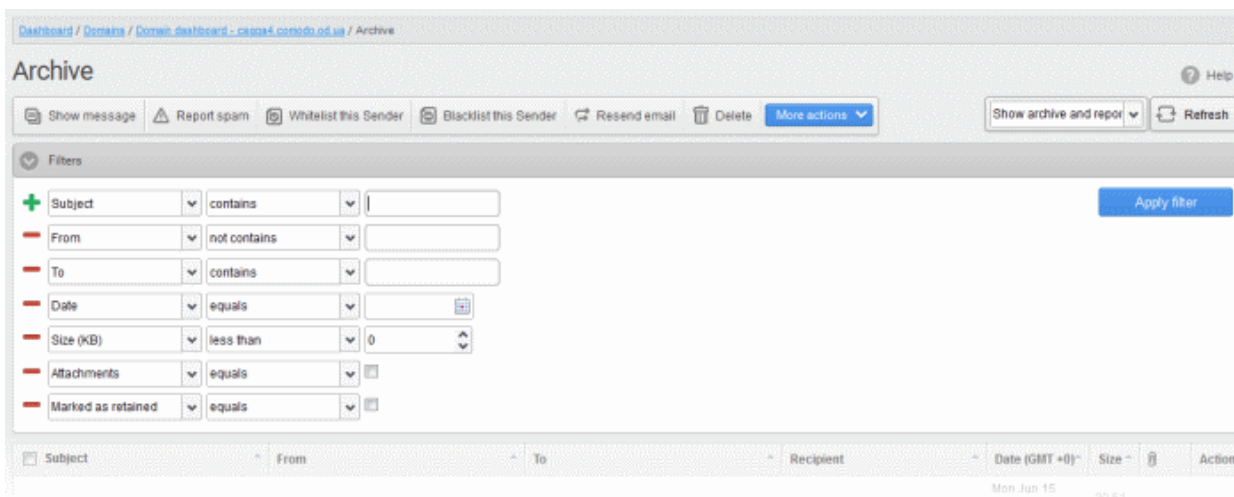
Select the option from the drop-down before using the filter option described below.

Using Filter option to search archived emails

Click anywhere on the Filters tab to open the filters area.



You can add more filters by clicking  for narrowing down your search.



You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Subject:** Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From:** Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To:** Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all archived mails that contain the words entered in the text box
- **Not Contains:** Displays all archived emails that don't contain the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size (KB):** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.
- **Attachments:** Will execute a search of mails according to the checkbox status (column 3) whether enabled or disabled. If enabled, all archived mails with attachments will be displayed.
- **Marked as retained:** Will execute a search of mails according to the checkbox status (column 3) whether enabled or disabled. If enabled, all archived mails that are marked as retained will be displayed.

If 'Date' is selected, the following conditions are available:

- **Equals:** Displays the archived emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the archived emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the archived emails with dates greater than the selected date in the third box from the calendar

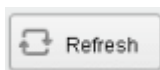
If 'Size' is selected, the following conditions are available:

- **Less than:** Displays the archived emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the archived emails with size greater than the selected or entered size in the third box

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.



Click the  button to display all the archived emails.

Note: To display all the archived emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing Details of Archived Mails

The details like subject, sender, recipient, date and size of the mails in the archive can be viewed in two ways:

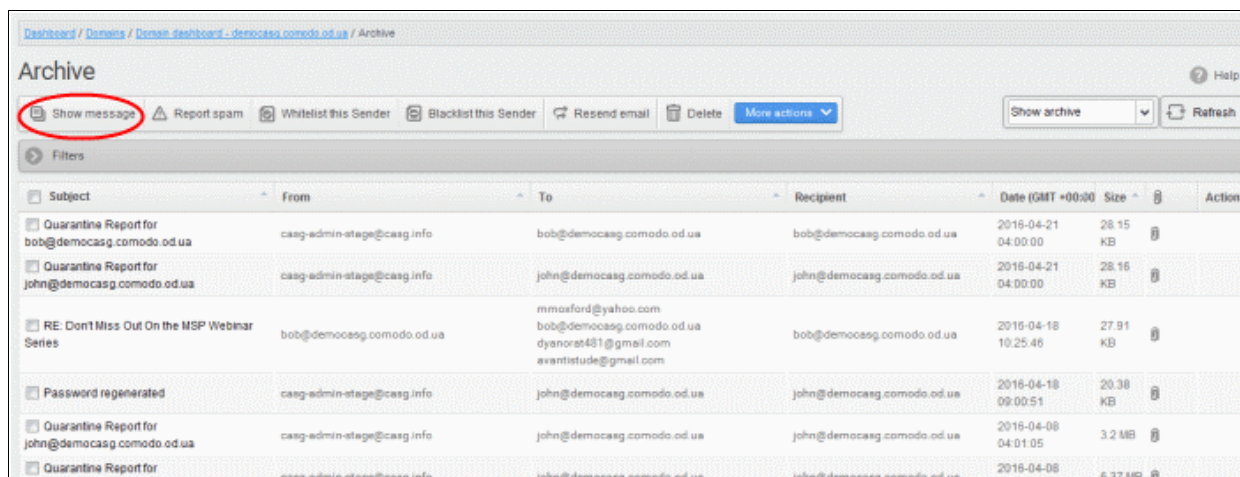
- **In the same CASG window**

- **In a new CASG window**

To view details of archived mails in the same CASG window:

- In the archived email area, 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.

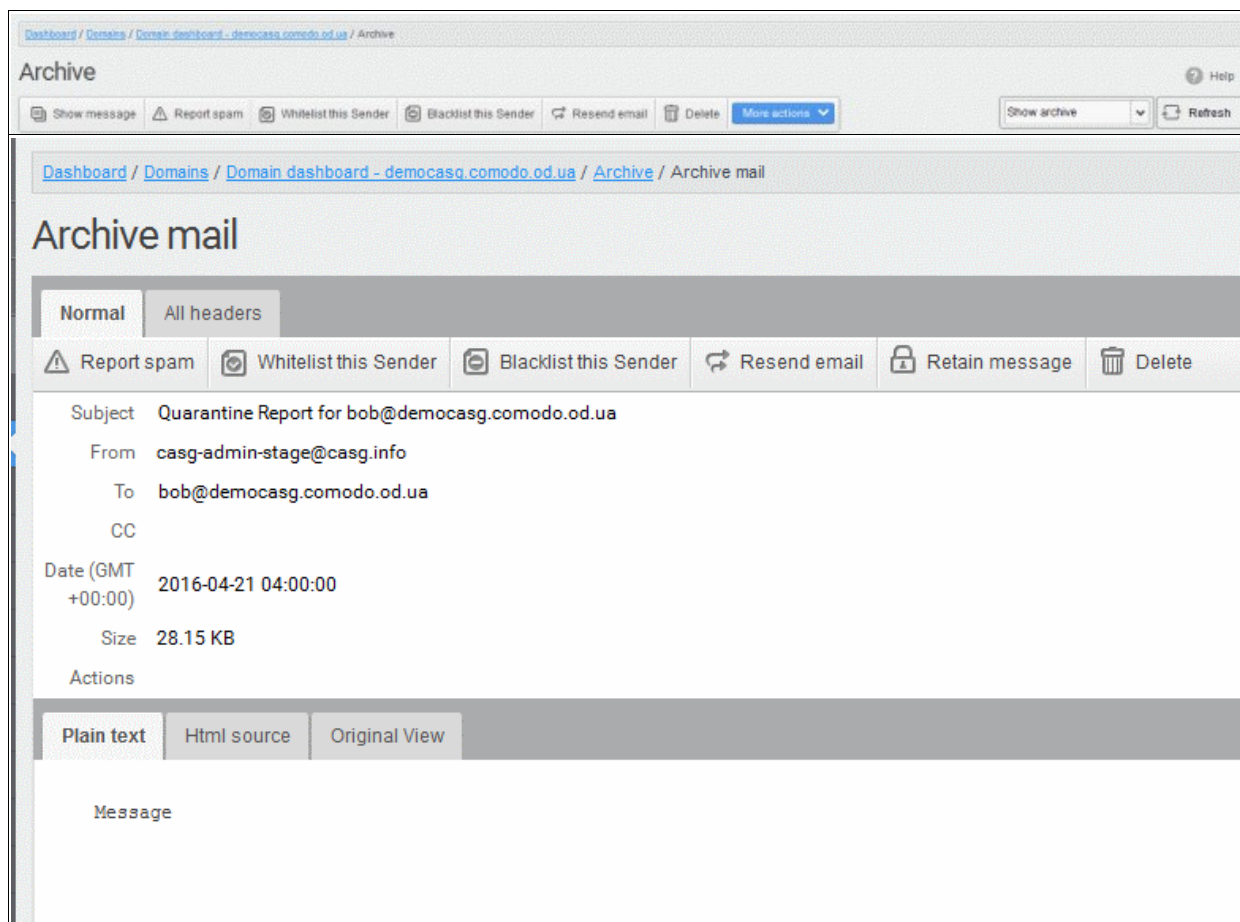
The details of the selected email will be displayed.



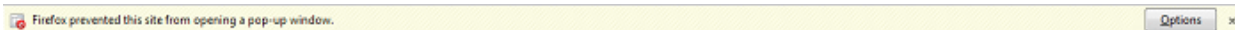
To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient, click 'All headers' tab. The headers give full details of the sender, route, recipient, sent date, mail type and so on.

To view the details of archived mails in a new CASG window

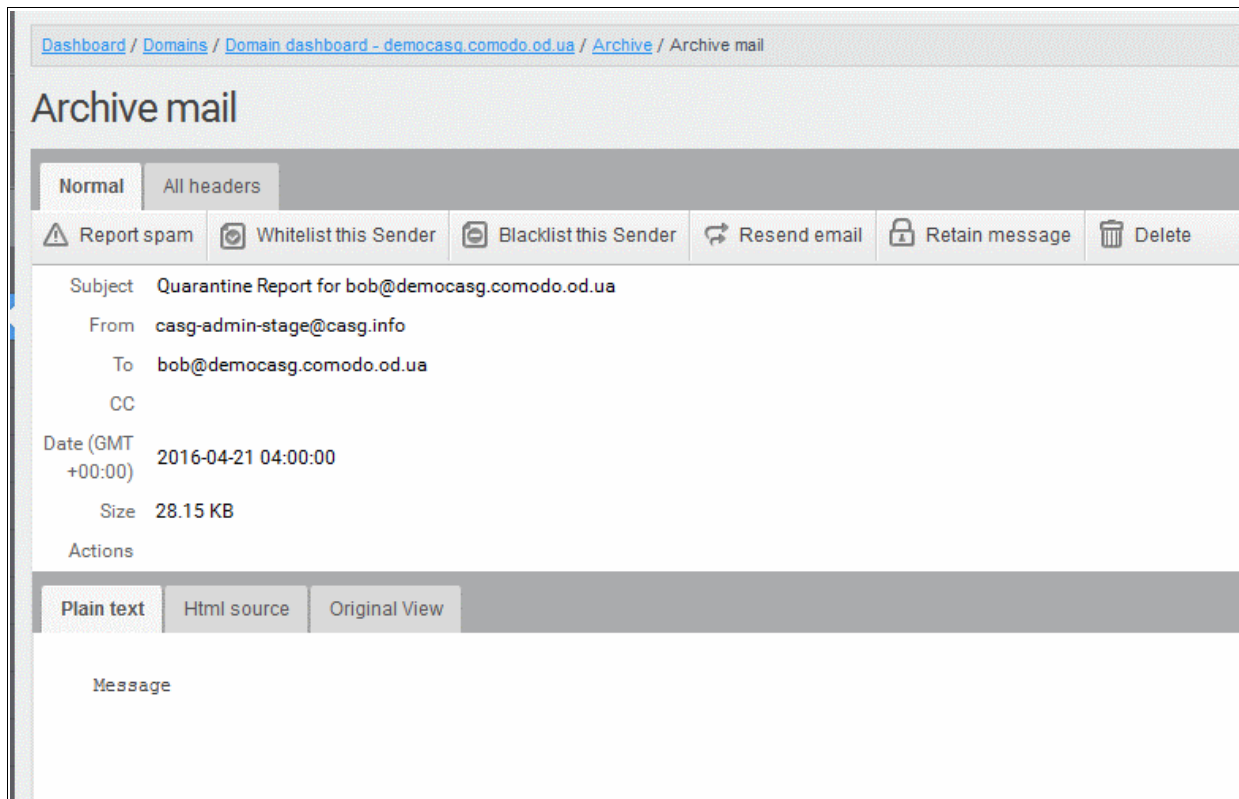
- In the archived email area, select the mail that you want to view, right-click on the email link in the subject column and select to open in a new tab or new window.



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



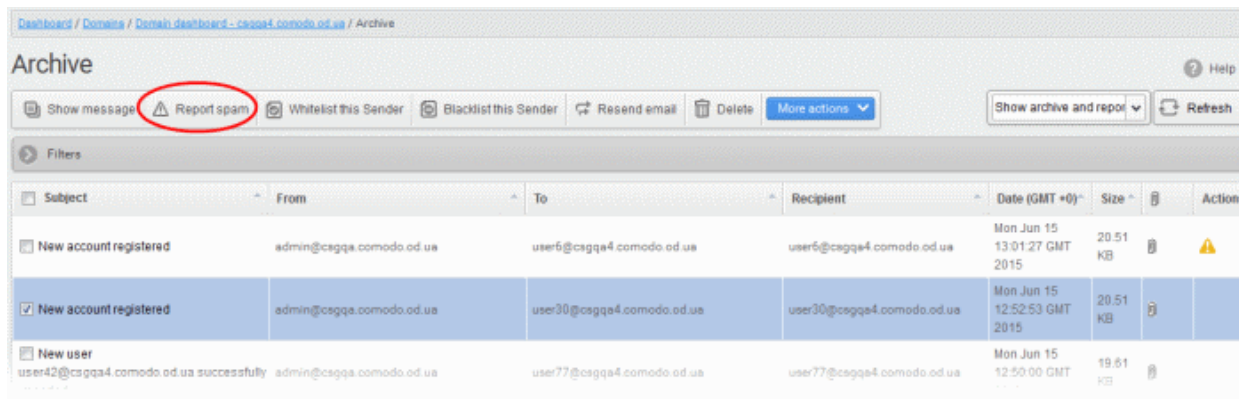
The details of the selected mail will be displayed in a new CASG window.



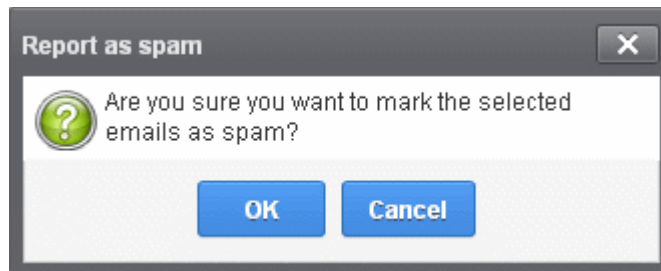
To report archived mails as spam

After viewing the details and ensuring that the selected email is a spam you can choose to report it as a spam.

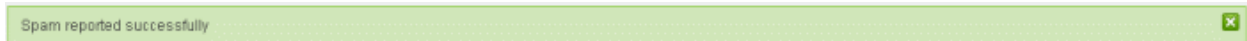
- Select the mail that you want to report as spam and click 'Report spam'.




An alert will be displayed to confirm selected email as spam.



- Click 'OK' to confirm.

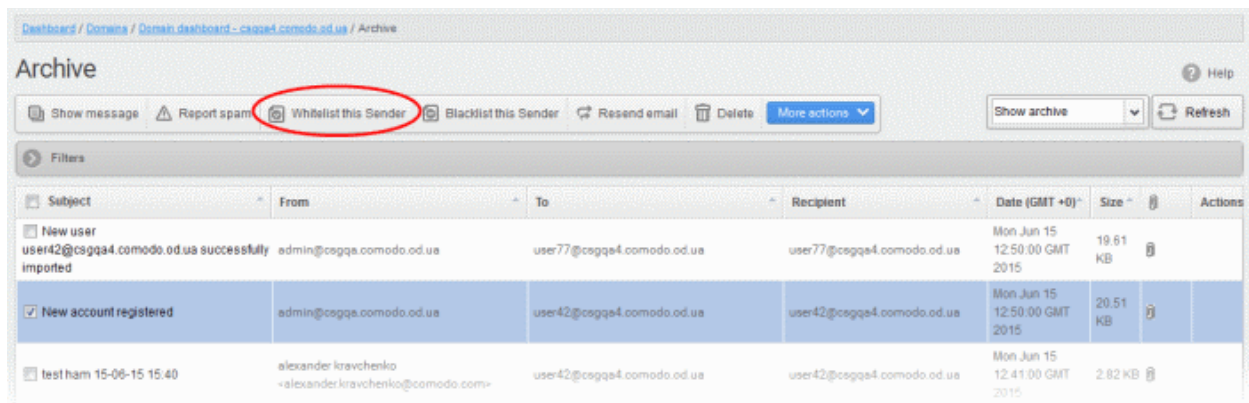


A success message will be displayed and the icon  indicating the email is reported as spam will be shown under the 'Actions' column. The mail will be forwarded to the spam email address displayed in the Incoming Spam Detection Settings interface for analysis by experts. Refer to the explanation under **Incoming Spam Detection Settings** for more details.

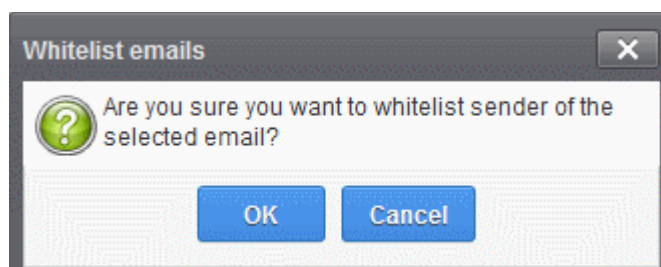
To add a sender to whitelist

Administrators can choose to add the email senders to 'Sender Whitelist' from this interface. Once added to whitelist, emails sent by these senders will not be quarantined.

- Select the mail that you want to add the sender to whitelist and then click 'Whitelist this Sender'



An alert will be displayed to confirm adding the sender to whitelist.

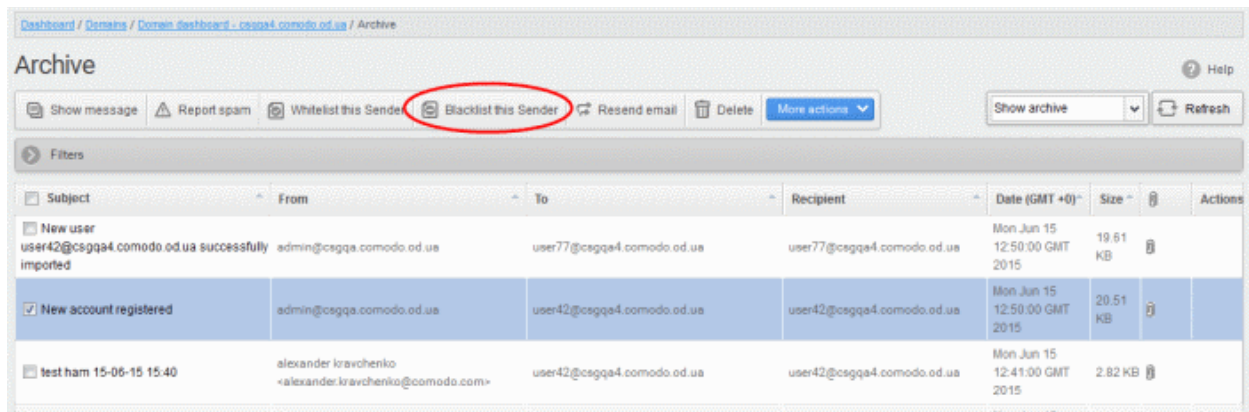


- Click 'OK' to confirm to add the sender to whitelist. Refer the section '**Sender Whitelist**' for more details.

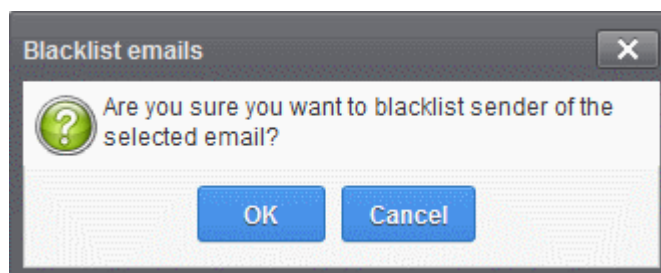
To add a sender to blacklist

Administrators can choose to add the email senders to '**Sender Blacklist**' from this interface. Once the selected senders are added to blacklist, all emails from them to the selected domain will be automatically blocked.

- Select the mail that you want to add the sender to blacklist and then click 'Blacklist this Sender'



An alert will be displayed to confirm adding the sender to blacklist.

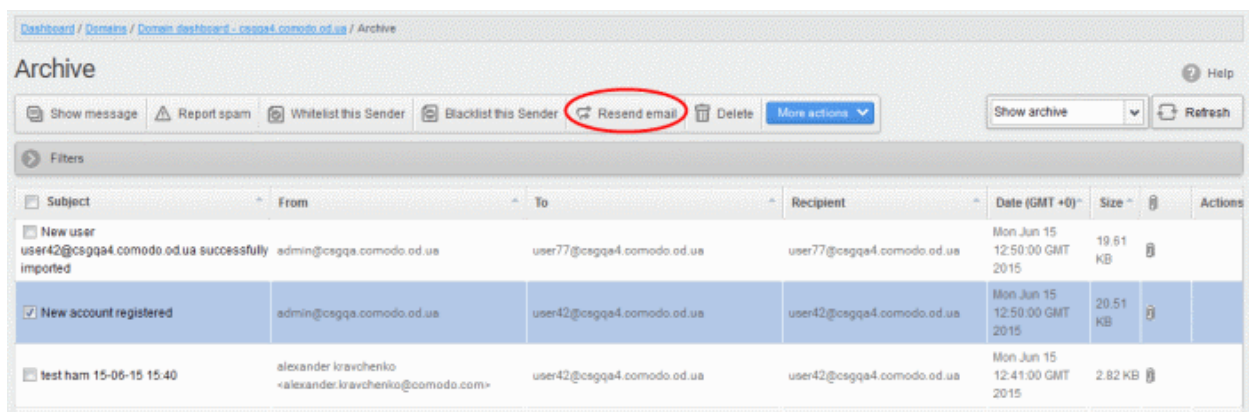


- Click 'OK' to confirm to add the sender to blacklist. Refer the section '**Sender Blacklist**' for more details.

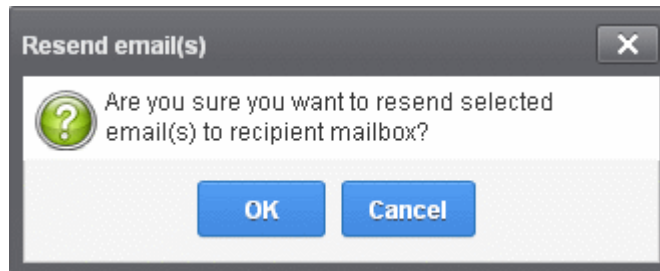
To resend emails from archive

The archived mails can be sent to the recipients if required. CASG will still retain a copy of mails in the archive even after they are sent.

- Select the mail that you want to resend and click 'Resend email'.

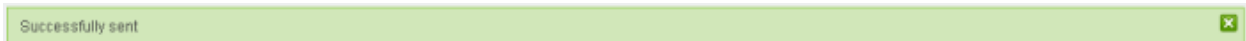


An alert will be displayed to confirm resending emails.



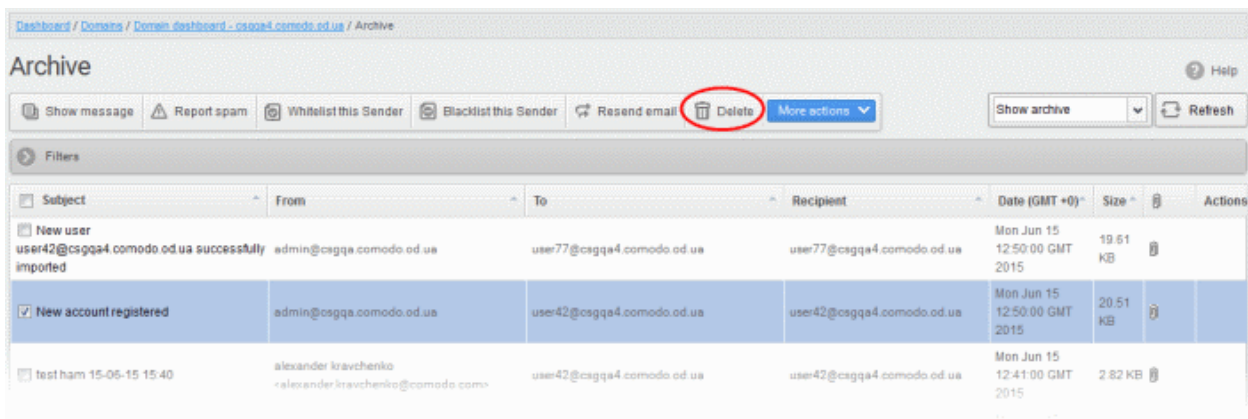
- Click 'OK' to confirm.

A success message will be displayed.

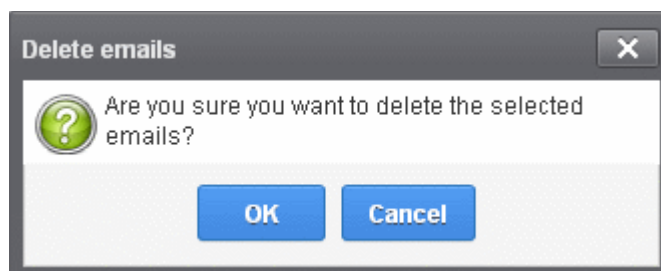


To delete archived mails

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



An alert will be displayed to confirm deletion.



- Click 'OK' to confirm.

The selected mail will be deleted and will no longer be in archive.

- To delete all the archived mails, click 'More actions' > 'Delete all'.

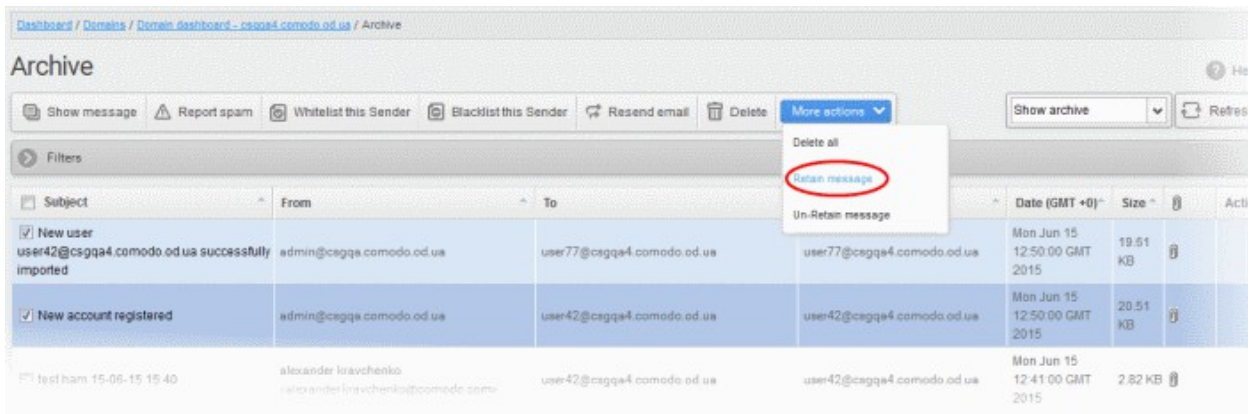


An alert will be displayed to confirm the deletion. Click 'OK' to delete all archived emails.

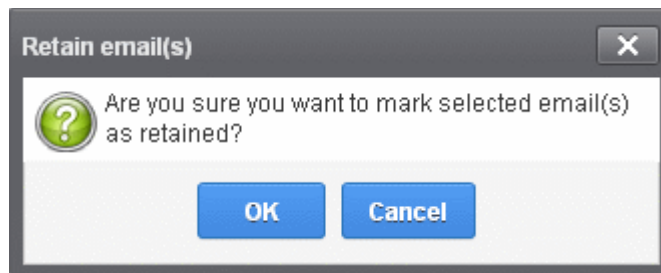
To exclude mails from auto-clean operations

CASG can be configured in the **Domain Settings** area to automatically purge emails from archive after the configured period. If administrators wants to retain email(s) from being cleared, then these mails can be marked as 'Retain message'.

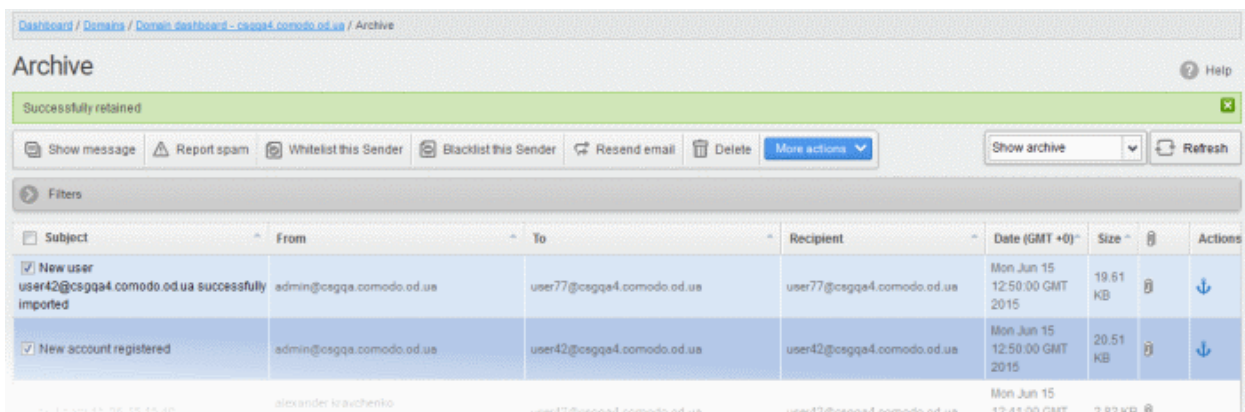
- Select the mail(s) that you want to retain and then click 'More actions' > 'Retain Message'.



An alert will be displayed to confirm retain selected email(s).

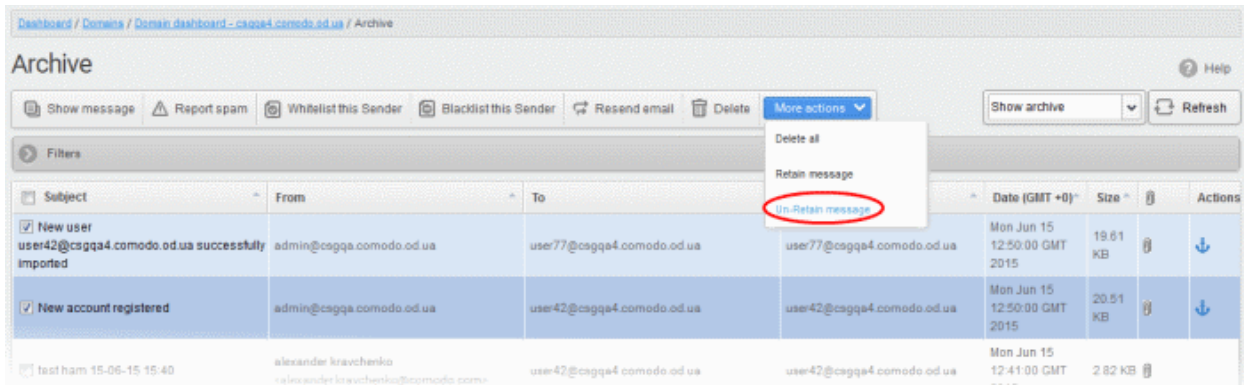


- Click 'OK' to confirm.

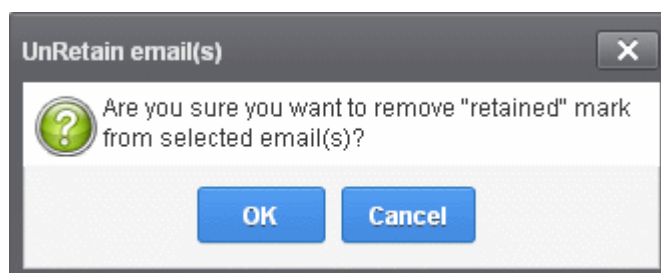


A confirmation dialog will be displayed and the retained messages are indicated by the anchor icons under the Actions column.

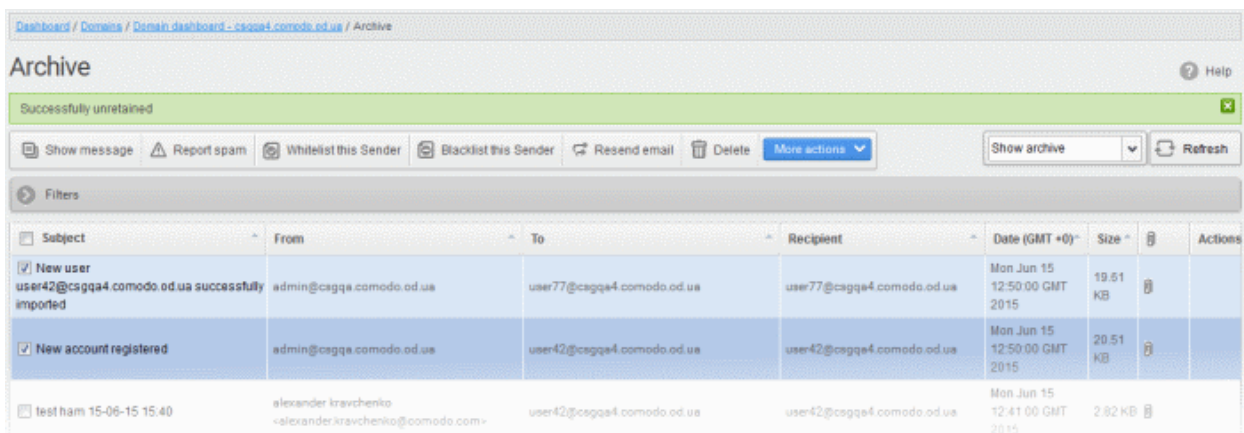
- To remove the retained status for a mail, select the retained message and then click 'More actions' > 'Un-Retain Message'.



An alert will be displayed to confirm selected email(s) from retain status.



- Click 'OK' to confirm.



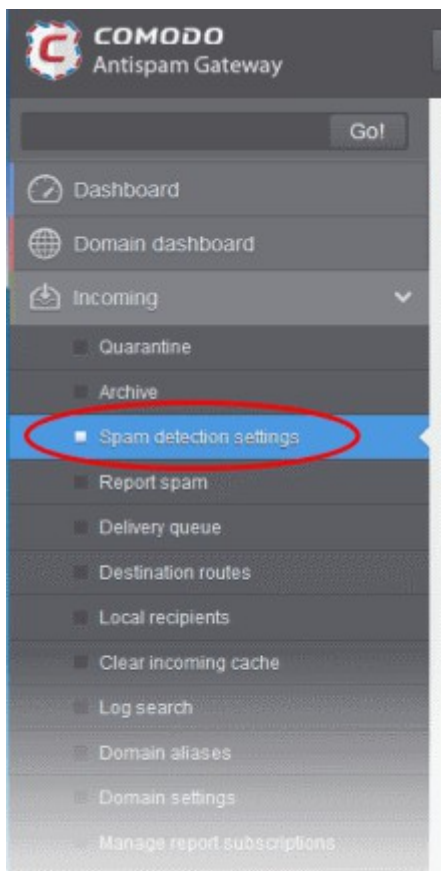
A confirmation dialog will be displayed and the anchor icons under the Actions column are no longer displayed indicating their unretained status.

Incoming Spam detection settings

The settings made in this interface determine what kind of mails should be classified as 'spam', 'probable' and 'safe'. CASG enforces several rules to mail envelope, header and content as the emails passes through its spam filters. Each of these rules depicts some typical spam attribute, which has a numeric value on the probability that the attribute suggests spam. A message's spam score depends on the result of weighted value of all the rules combined together. For example, if you set the spam threshold as 0.33, all mails that have a score of more than 0.33 will be treated as spam and quarantined. Please note that the highest spam threshold is 1 for CASG and the higher threshold you set, it is likely that more spam messages may be delivered to the recipients. Try the settings for a week or so and after analyzing how much spam messages are being delivered to the recipients without being filtered for the current settings, you have to reconfigure the spam threshold settings accordingly.

To configure incoming spam detection settings

- Click the 'Incoming' tab from the left hand side navigation to expand it and then click the 'Spam detection settings' tab.



The incoming spam detection settings interface for the selected domain will open:

The screenshot displays the 'Incoming Spam detection settings' configuration page. The settings are as follows:

- Quarantine enabled:
- Spam threshold:
- Probable spam threshold:
- Quarantine response:
- Days saved:
- Spam notation:
- Probable spam notation:
- Spam email:
- Suspicious attachment notation:
- Notify user about new quarantine message:

Buttons for 'Save' and 'Reset to default' are located at the bottom of the form.

- **Quarantine enabled** - Selecting this option will move the incoming emails detected as spam as per the '**Spam threshold setting**' to Quarantine. If this option is not enabled, emails that are detected as 'Spam' will not be quarantined but delivered to your email server with the subject line as set in the that you have set in **Probable Spam notation / Spam Notation** fields. Unsure messages that are identified as probable spam based on the '**Probable spam threshold setting**' are always sent to the recipient (and never quarantined) even if this option is enabled.
- **Days saved** - Enter the number of days that you want the mails to be retained in the quarantine.

The maximum number of days that can be set is 9999. The quarantined mails that are not checked, released or deleted within the stipulated days will be automatically deleted from the quarantine.

- **Spam threshold** - Enter any value between 0.1 and 1.0. All mails that are having a score value above that value will be identified as spam and quarantined automatically as explained **above**. Please note this value should be always higher than 'Probable spam threshold' value.
 - **Spam notation** - The prefix that will be appended to the subject line of all 'Spam' emails sent to users. For example, "<Spam> Order two Rolex watches and get a free carton of Viagra" - where <Spam> is the text entered in the 'Spam notation' field. Note - this only applies IF quarantine has been disabled (i.e. If the 'Quarantine Enabled' box is not checked).
 - **Probable spam threshold** - Enter any value between 0.0 and the value entered in **Spam threshold** field. All mails that are having a score value above that is set in this field will be identified as unsure mails and will be delivered to recipients with the subject line as set in the **Probable Spam notation / Spam Notation** field.
 - **Probable spam notation** - The prefix that will be appended to the subject line of all 'probable spam' emails sent to users. For example, "<Potentially Spam> Cheap deals on Dell computers" - where <Potentially Spam> is the text entered in the 'Probable spam notation' field.
 - **Quarantine response** - Choose the response to be sent by CASG to the SMTP server that delivered a message in the event that a mail is identified as spam.
 - Note - If you have enabled quarantine functionality, then spam/malicious mail will be quarantined (and not delivered to the recipient) regardless of your choice here. These options merely determine what message CASG will send back to the SMTP mail server. The available options are:
 - **Rejected** - Will inform the SMTP server that the email has been rejected by CASG and placed in quarantine.
 - **Accepted** - The email has passed the CASG spam filters and detected as a spam will be placed in quarantine in silent mode.
 - **Spam email** - Displays the email address to which the mails reported as spam from the 'Report Spam' interface and the 'Archive' interface will be forwarded. By default, mails reported as spam by the administrators will be forwarded to **spam@antispamgateway.comodo.com** for analysis by experts at Comodo. Once a reported mail is confirmed as spam, Comodo will update its mail filters to quarantine similar mails in future. Refer to the explanations under **Managing Archived Mails** and **Report Spam** for more details on forwarding the suspicious mails for analysis.
 - **Notify user about new quarantine message** - Select this option if you wish CASG to send a notification email to the intended recipient, if a spam email addressed to the recipient is intercepted by CASG and moved to Quarantine. The notification email will contain a link to the email and a link for the user to login to the CASG User interface.
 - The recipient will be able to click the link to directly read the email, without logging-in to CASG. The lifetime of the link is one day. If the user has not clicked the link within a day, the link will expire.
 - If the user needs to respond to or delete the quarantined email, the user can click the next link to login to CASG, view their quarantined mails and carry out their desired actions
 - **Suspicious attachment notation** - The prefix that will be appended to the subject line of all mails identified with suspicious attachments like malware and macros and forwarded to the recipient or to a different email address, as configured in the Domain Rules. Refer to the explanation under **Rules** in the section **Domain Rules** for more details. For example, "[Suspicious attachment] Your lucky draw" - where [Suspicious attachment] is the text entered in the 'Suspicious attachment notation' field.
- Click the 'Save' button for your settings to take effect.
 - To restore the settings to default, click 'Reset to Default'.

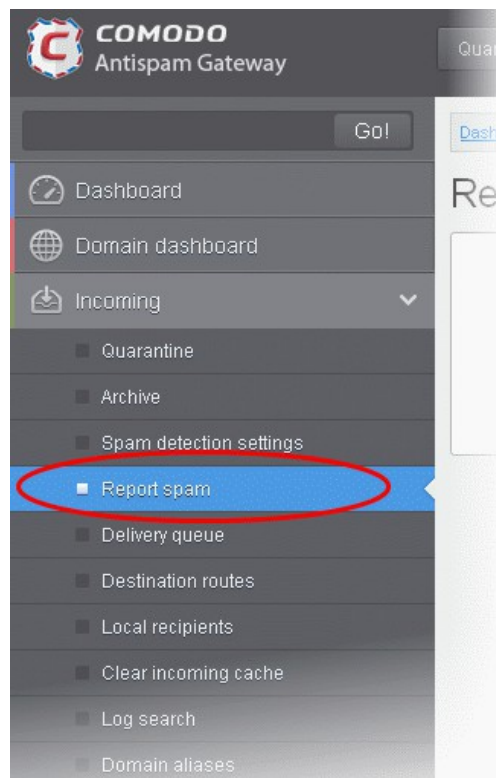
Report Spam

The 'Report Spam' feature allows 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. CASG accepts a range of different mail formats including .eml and .msg.

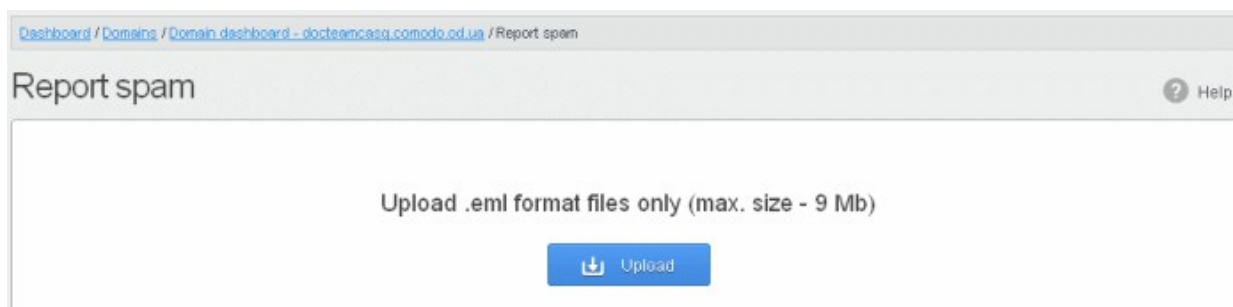
Users can also report spam by forwarding unsolicited messages to spam@antispamgateway.comodo.com.

To report a spam mail

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Report spam' tab.

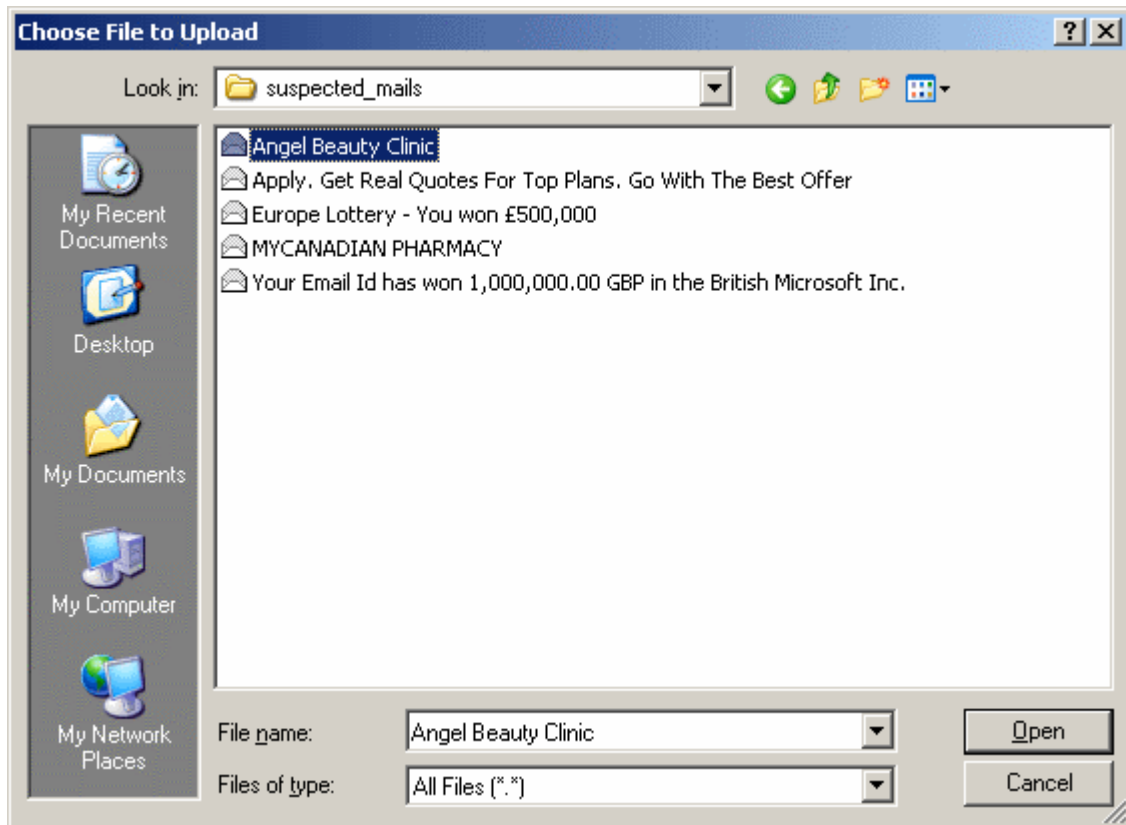


The Report Spam interface will open.

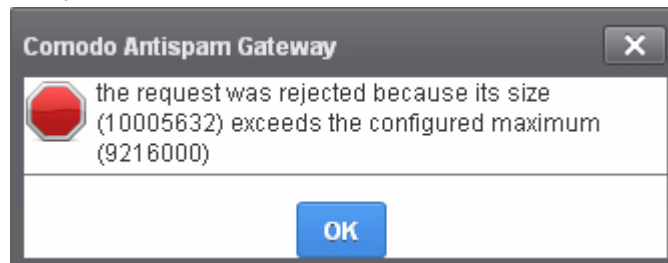


- Click the 'Upload' button

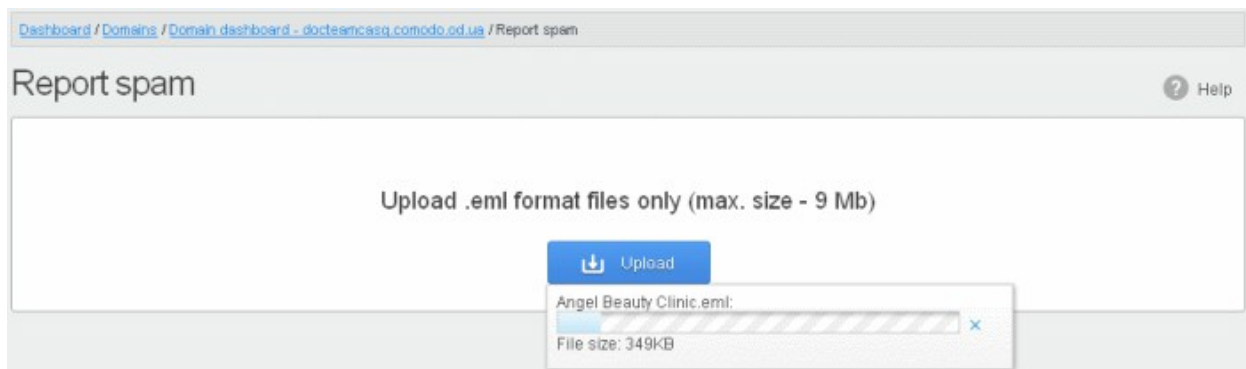
Navigate to the location where the suspected email(s) is/are stored in your system. Select the mail that you want to report as spam and click 'Open'. The maximum size of the file that can be uploaded is 9 MB.



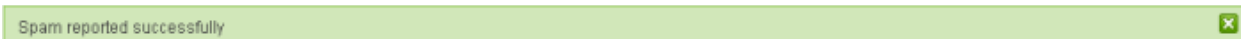
Note: Make sure to upload the file in email format only and size should not exceed 9 MB. Otherwise, the following warning message will be displayed.




The mail will be processed for uploading...



... and success message will be displayed.



- Click the  button to close the message.

Delivery Queue

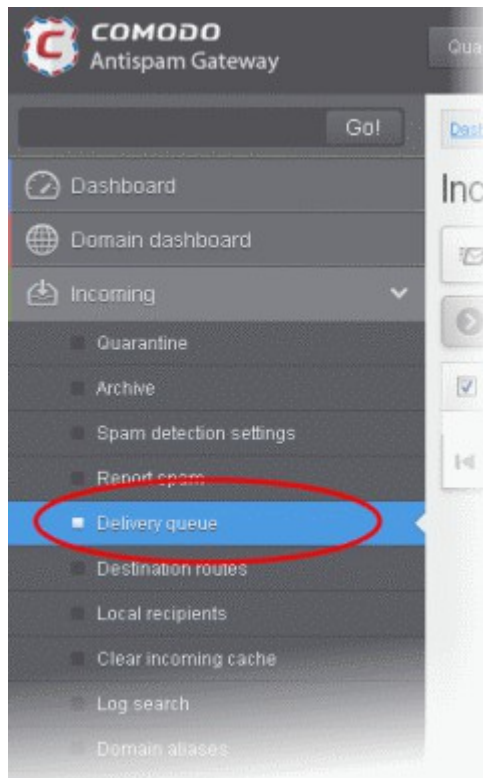
In general, emails are delivered to the destination server directly and not stored on the filtering machines. But whenever an email destination server for an account is temporarily unavailable, all filtered mails are queued in the CASG servers for delivery at a later time. Emails that are permanently rejected by the destination server with a 5xx error code will not be queued and rejected by the CASG system. The queued emails can be accessed in the CASG interface and from here they can be manually force retried for delivery.

The queued messages on CASG servers are automatically retried for delivery for up to a period that is set in 'Maximum days to retry' field in **domain settings** (for example, 4 days). The automatic retry schedule is given below:

- During the first two hours, the queued messages are retried for delivery at a fixed time interval of 15 minutes.
- During the next 14 hours, the queued messages are retried for delivery at a variable time interval starting from 15 minutes and multiplied by 1.5 with each attempted delivery. For example, after the first 15 minutes, the subsequent attempts will be after 22.5 minutes, 34 minutes and so on.
- From 16 hours since the delivery failure and up to 4 days, the queued messages are retried for delivery at a fixed time interval of every 6 hours.
- After a period of 4 days, all queued messages will be bounced to respective senders. The messages will be frozen if the bounce cannot be delivered immediately and retried for delivery at a fixed time interval of 3 days for the first 21 days. At the end of this period, delivery of messages will have failed permanently.

To manually force-deliver emails in queue

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Delivery queue' tab.



The Incoming Delivery Queue area of the selected domain will open:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Incoming delivery queue

Incoming delivery queue

Force retry Show headers Delivery diagnostic Alerts Refresh

Filters

Queue id	In queue	Sender	Recipient	Message size	Subject	Last action	Server name	Delay reasons
3jRwrD24WTz12LFC	52m	admin@antispamg;	john@docteamcasg	21577	New account registered	message_queue_ch	mta3.prod.casg	john@docteamcasg : connect to 91.196.95.19[91.19] Connection refused
3jRwrZ1qfHzHnm5	52m	admin@antispamg;	demo2@docteamcr	21585	New account registered	message_queue_ch	mta1.prod.casg	demo2@docteamcr : connect to 91.196.95.19[91.19] Connection refused
3jRwrY6XR0z12Lsf	52m	admin@antispamg;	bob@docteamcasg	21566	New account registered	message_queue_ch	mta3.prod.casg	bob@docteamcasg : connect to 91.196.95.19[91.19] Connection refused
3jRwrY0IY1zHnly	52m	admin@antispamg;	demo1@docteamcr	21586	New account registered	message_queue_ch	mta1.prod.casg	demo1@docteamcr : connect to 91.196.95.19[91.19] Connection refused
3jRvmH6LYpzHnn6	1h 41m	admin@antispamg;	john@docteamcasg	21576	New account registered	message_queue_ch	mta1.prod.casg	john@docteamcasg : connect to 91.196.95.19[91.19] Connection refused

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search queued emails

Click anywhere on the Filters tab to open the filters area.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Incoming delivery queue

Incoming delivery queue

Force retry Show headers Delivery diagnostic Alerts Refresh

Filters

+ Queue id contains Apply filter

Queue id	In queue	Sender	Recipient	Message size	Subject	Last action	Server name	Delay reasons
mm								

You can add more filters by clicking  for narrowing down your search.

Dashboard / Domains / Domain dashboard - docteamcsg.comodo.ed.ua / Incoming delivery queue

Incoming delivery queue

Force retry Show headers Delivery diagnostic Alerts Refresh

Filters

- Queue Id contains
- Queue name equals
- Sender not contains
- Recipient contains
- Message size less than 0
- Subject starts with
- Last action ends with
- Server name contains

Apply filter

Queue Id	In queue	Sender	Recipient	Message size	Subject	Last action	Server name	Delay reasons
3iCSnh0nV7>12l Ri		demo@csg.comod	demo1@docteamc	4752	Re: DQ demo 2	message_added	mta3.prod.casg	

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Queue ID:** Will execute a search of Queue ID according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Queue name:** Will execute a search of Queue name according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Recipient** - Will indicate the email address of the recipient that is in the delivery request.
- **Message size** - Will execute the message size settings according to the number selected in the 'Filters'.
- **Subject:** Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Last action:** Will execute a search of Last action according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Server name:** Will execute a search of Server name according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Delay reason** - Will indicate the reason an email is queued and cannot be delivered immediately.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all queued mails that contain the words entered in the text box
- **Equals:** Displays the queued emails that have the same words as entered in the text box
- **Not Equals:** Displays the queued emails that do not have the words entered in the text box
- **Not Contains:** Displays all queued emails that don't contain the words entered in the text box
- **Starts With:** Displays all queued mails that starts with the words entered in the text box.
- **Ends With:** Displays all queued mails that ends with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Sender:** Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Recipient:** Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.

- **Message size:** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Sender' and/or 'Recipient' option is selected, the following conditions are available:

- **Contains:** Displays all queued mails that contain the words entered in the text box
- **Not Contains:** Displays all queued emails that don't contain the words entered in the text box

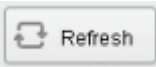
If 'Message Size' is selected, the following conditions are available:

- **Less than:** Displays the queued emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the queued emails with size greater than the selected or entered size in the third box

- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all the queued emails.

Note: To display all the queued emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

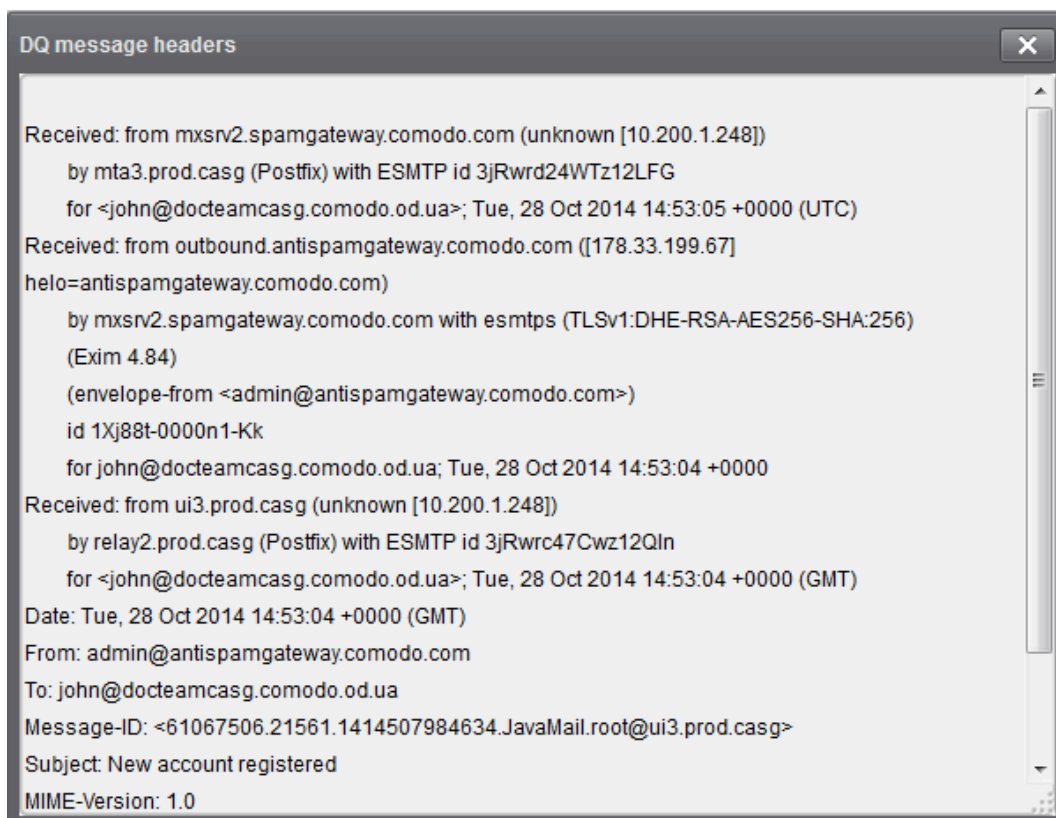
To force retry queued emails

- To force-deliver a single email manually, select an email from the delivery queue and click the 'Force retry' button.
- To force-deliver all email messages in the queue, select the checkbox beside 'Queue id' and click the 'Force retry' button.

Note: Frozen emails can't be force delivered from CASG interface.

To view headers queued emails

- Select an email from the delivery queue and click the 'Show headers' button.



To view diagnose routes availability of an email message in delivery queue

- Select an email from the delivery queue and click the 'Delivery diagnostic' button.

Mail delivery diagnostics ✕

MTA server availability
 [Relay : csg.comodo.od.ua:20]
 Error code : 500
 Error message : SMTP host unreachable
 No entries on your request

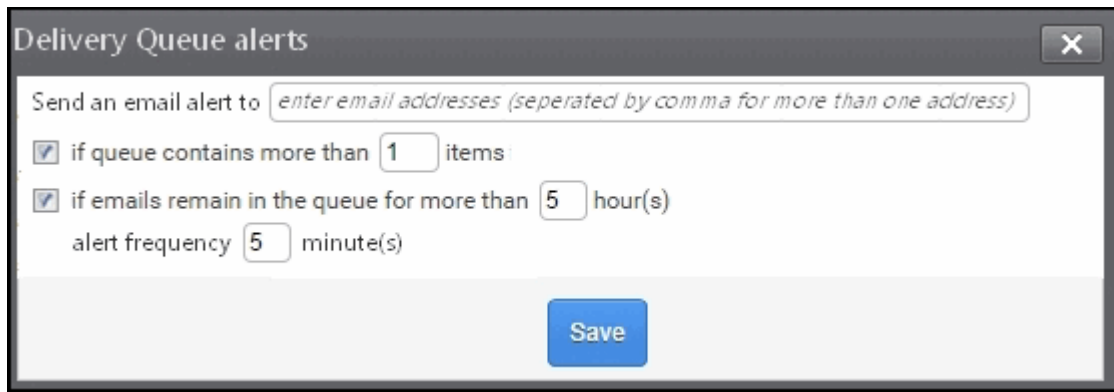
Log search (by queue ID)

[Host : 10.200.1.121]
 2014-10-28T15:38:37.045459+00:00 mta2 postfix/postfix: [Tue Oct 28 15:38:37 2014] [debug] GET
 "/log/3jRwrY6XRGz12Ls6".

[Host : 10.200.1.122]
 2014-10-28T14:53:01.920681+00:00 mta3 postfix.mta/smtpd[18514]: 3jRwrY6XRGz12Ls6:
 client=unknown[10.200.1.248]
 2014-10-28T14:53:01.921649+00:00 mta3 postfix.mta/cleanup[13104]: 3jRwrY6XRGz12Ls6: message-
 id=<891193322.21552.1414507981151.JavaMail.root@ui3.prod.casg>
 2014-10-28T14:53:01.921661+00:00 mta3 postfix.mta/cleanup[13104]: 3jRwrY6XRGz12Ls6:
 subject=New account registered
 2014-10-28T14:53:02.149219+00:00 mta3 postfix.mta/qmgr[26853]: 3jRwrY6XRGz12Ls6:
 from=<admin@antispamgateway.comodo.com>, size=21566, nrcpt=1 (queue active)
 2014-10-28T14:53:02.537662+00:00 mta3 postfix/relay/smtpd[28190]: 3iRwrY6XRGz12Ls6:

Alerts

The 'Alerts' area allows you to configure notification emails if there is a mail delivery delay. You will need to allow the alerting server to send you these alerts, so please add mxsrv10.antispamgateway.comodo.com [178.255.87.30] to your firewall/transport rules if necessary.



Send email alert to: Enter one or more email addresses as alert recipients.

You can specify 2 possible criteria that will trigger notifications:

1) *If queue contains more than n items:* Allows you to specify how many emails are queued before notifications are sent out.

2) *If email remains in the queue for more than n hour(s):* Will send notification mails when the oldest mail in the queue exceeds the age you specify (max age = 72 hours).

If you select both criteria, you will receive separate notifications for each trigger. If you uncheck both boxes, notifications will be cancelled.

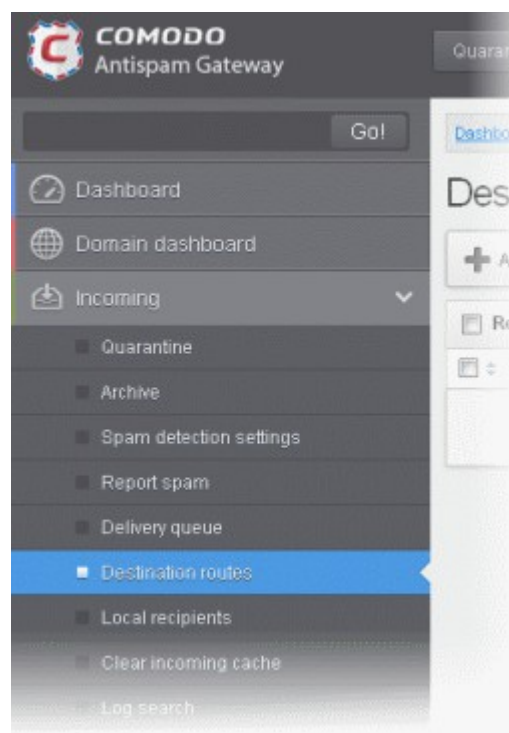
Alert frequency determines how often you will receive delivery delay notifications. Possible values are between 5-360 minutes.

Destination Routes

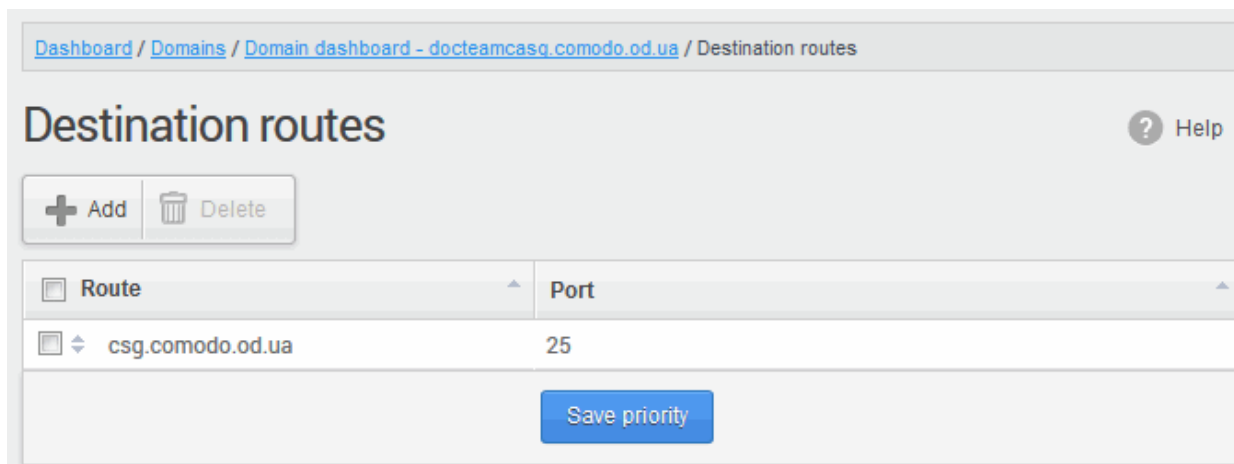
If there is a temporary problem with the primary email destination server, CASG will try to deliver the filtered mails to the next destination email server that is configured. If the failure is permanent, for example, unable to resolve hostname, CASG will try to deliver through the next alternative route.

To add additional destination routes

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Destination routes' tab.

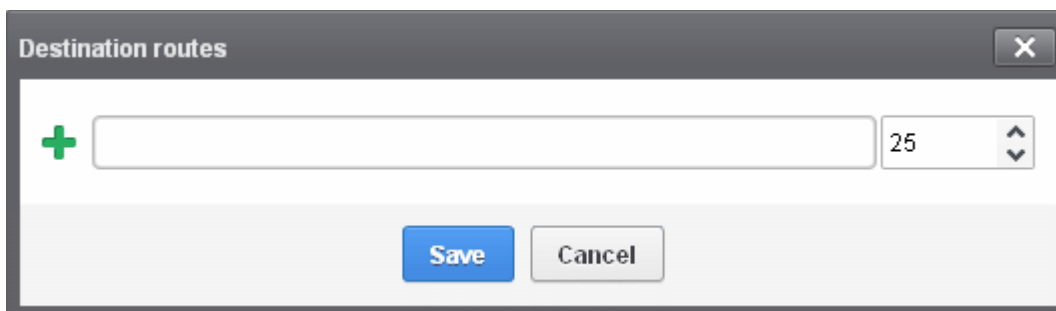


The 'Destination routes' area of the selected domain will open:

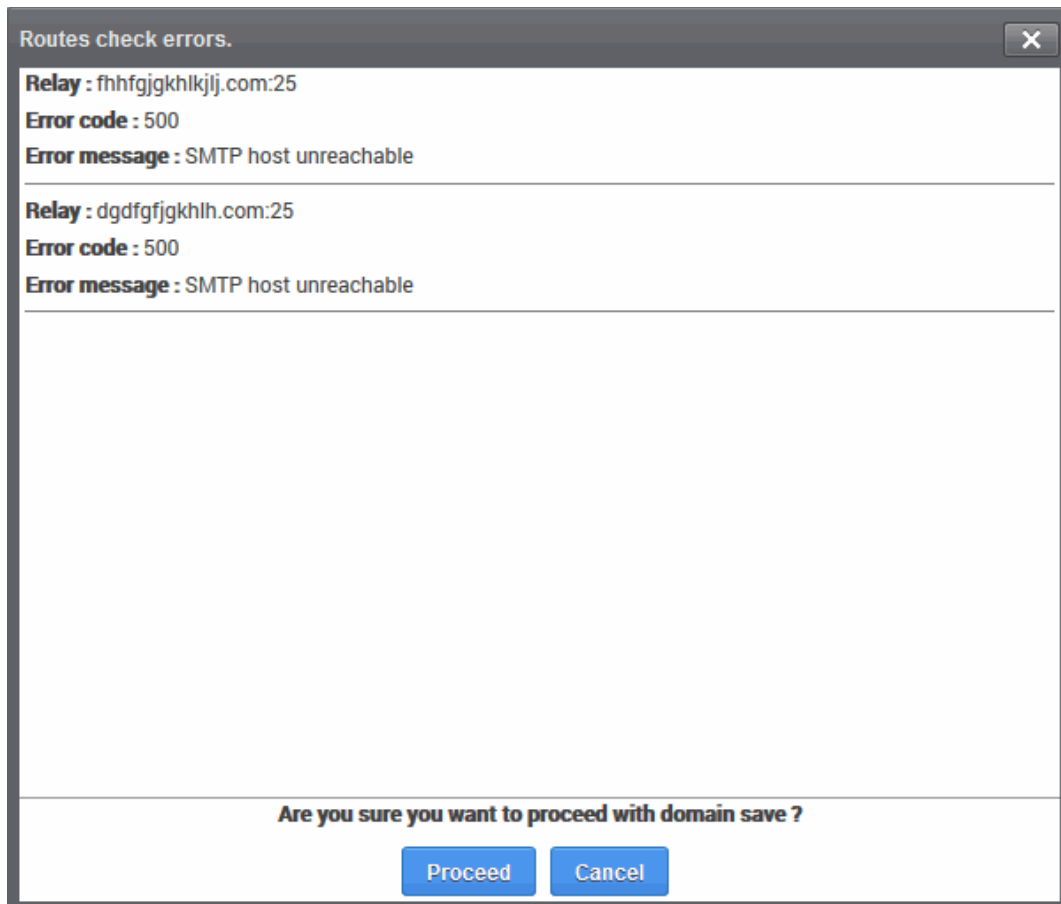


- Click the 'Add' button to add another alternative destination route

The 'Destination routes' dialog box will be displayed.

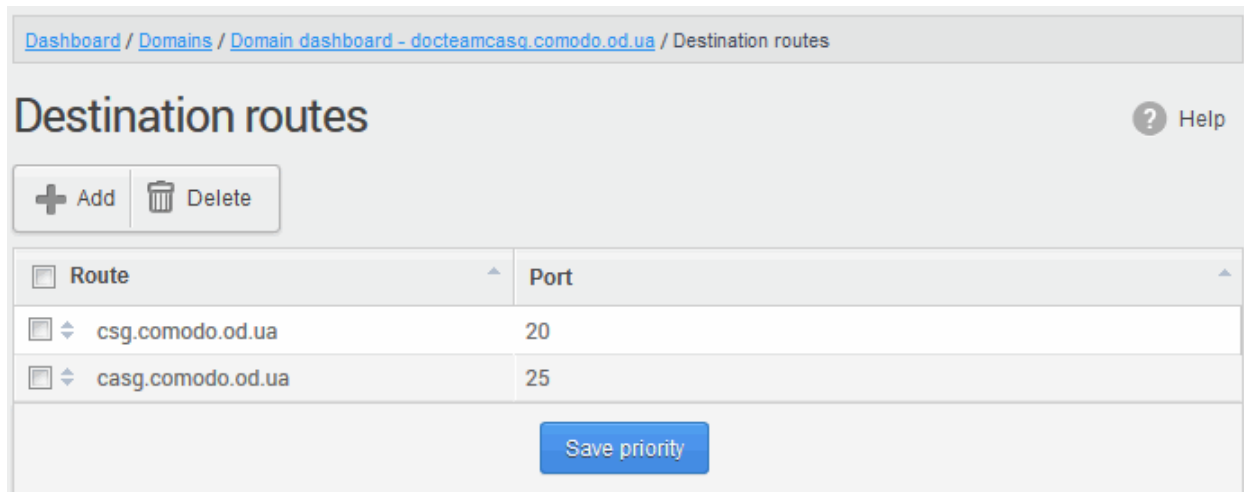


- Enter the alternative destination route and click the 'Save' button
- The domain entered in the 'Destination routes' field is checked by Comodo Gateway diagnostic tool to assure the destination route is entered by administrator correctly.



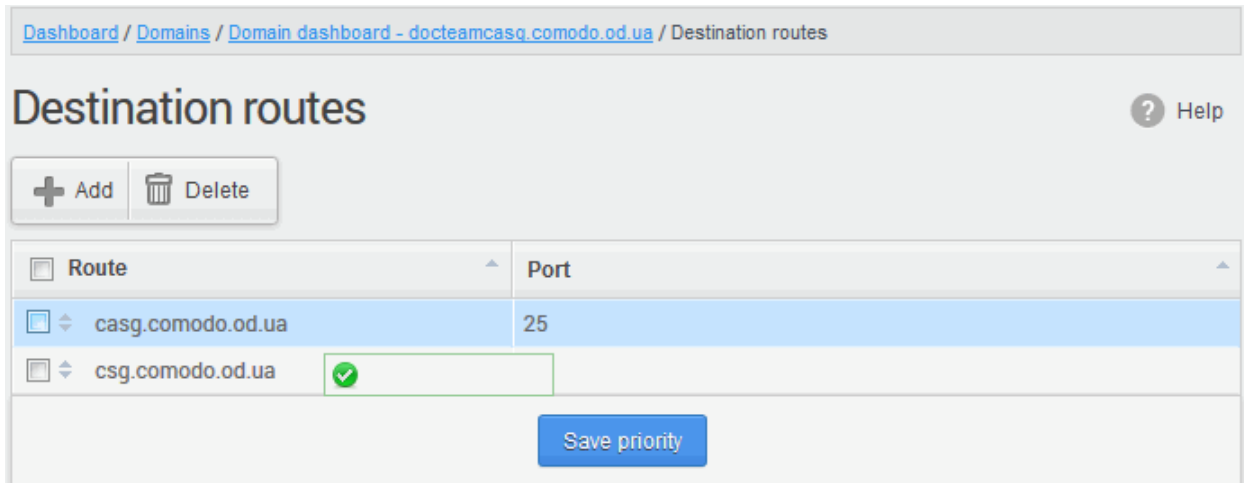
- Click 'Proceed' to save a domain.

The added route will be displayed in the list.



- If you want additional routes to be included, click **+** to add more alternative destination routes.

You can also prioritize the routes by dragging and dropping from the list.



- Click the 'Save priority' button to confirm the changes.

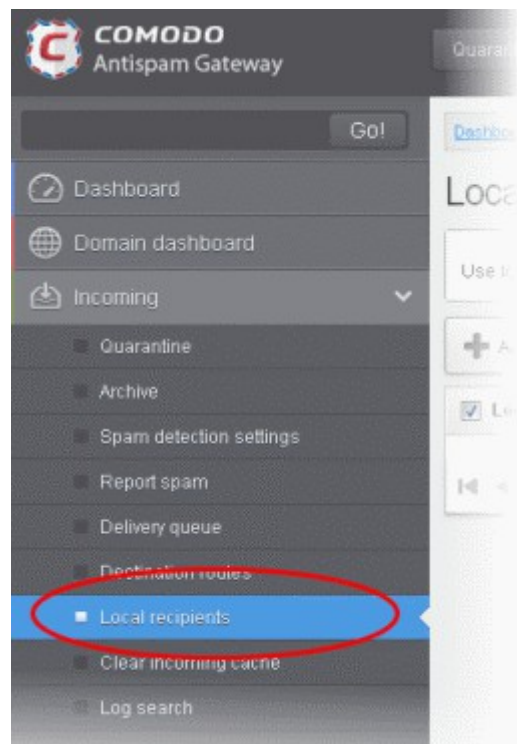
[Click here](#) for more details on how to check the routes.

Local Recipients

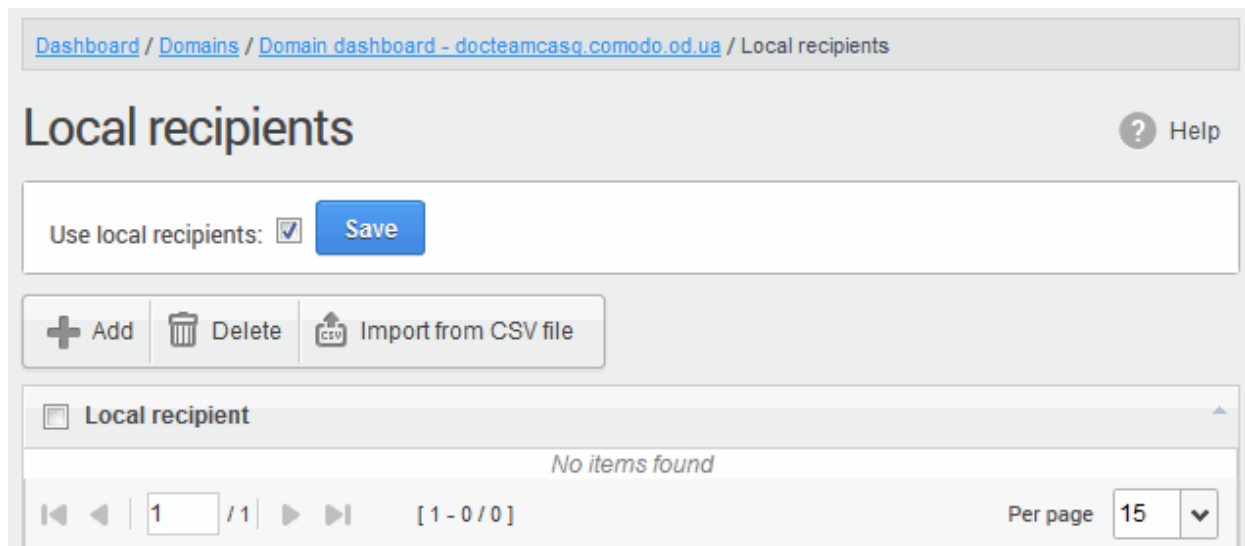
CASG continuously performs a cached recipient callouts to check that recipient email addresses do actually exist in the destination mail servers. When the 'Local Recipients' option is enabled, only existing and valid email accounts in the destination server will be accepted. When this option is selected, *all the recipients* have to be added manually, else even valid users for that account will not receive emails. Comodo recommends that this option should be used in specific cases only and not required in normal cases.

To add local recipients

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Local recipients' tab.

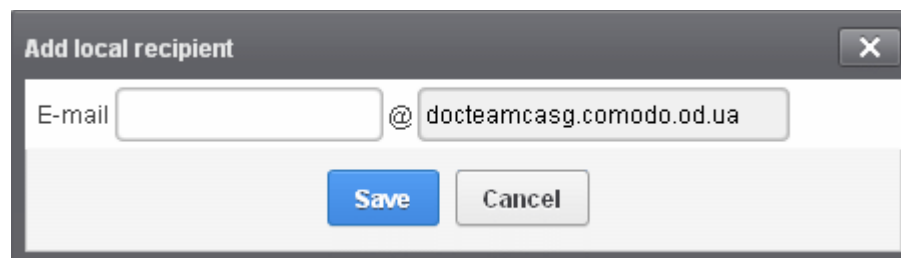


The Local Recipients configuration area of the selected domain will open:

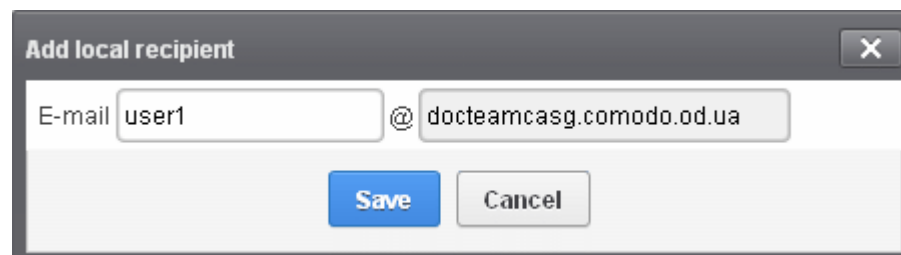


- Select the 'Use local recipients' check box and click the 'Save' button
- Click the 'Add' button

The 'Add local recipient' dialog box will open.

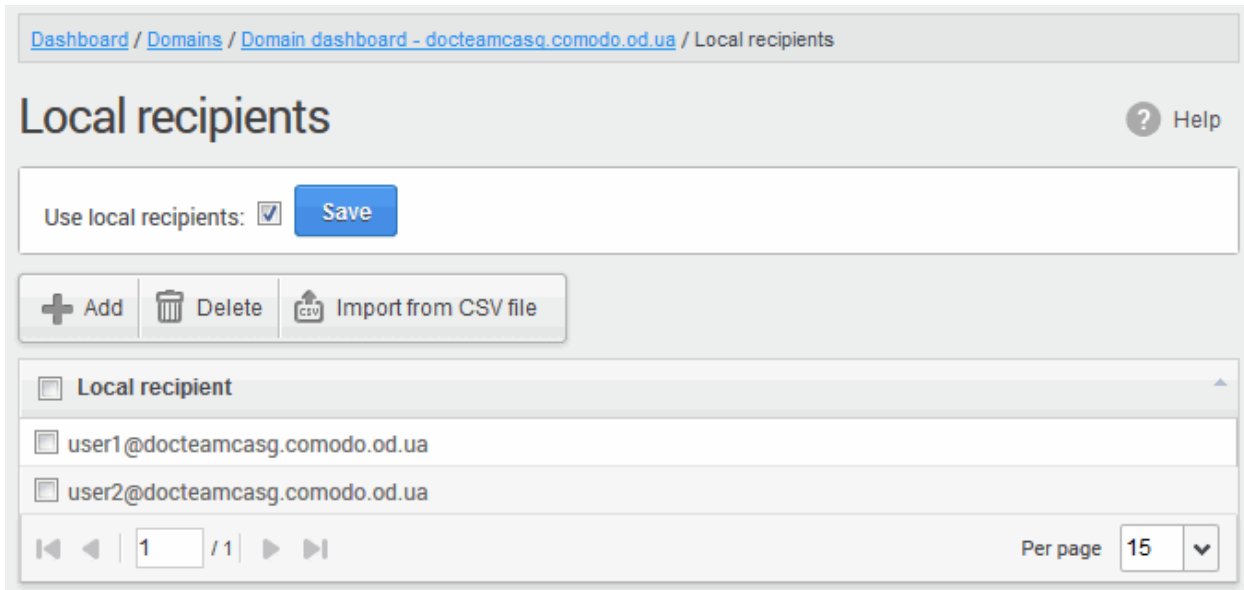


- Enter the recipient's in the E-mail field



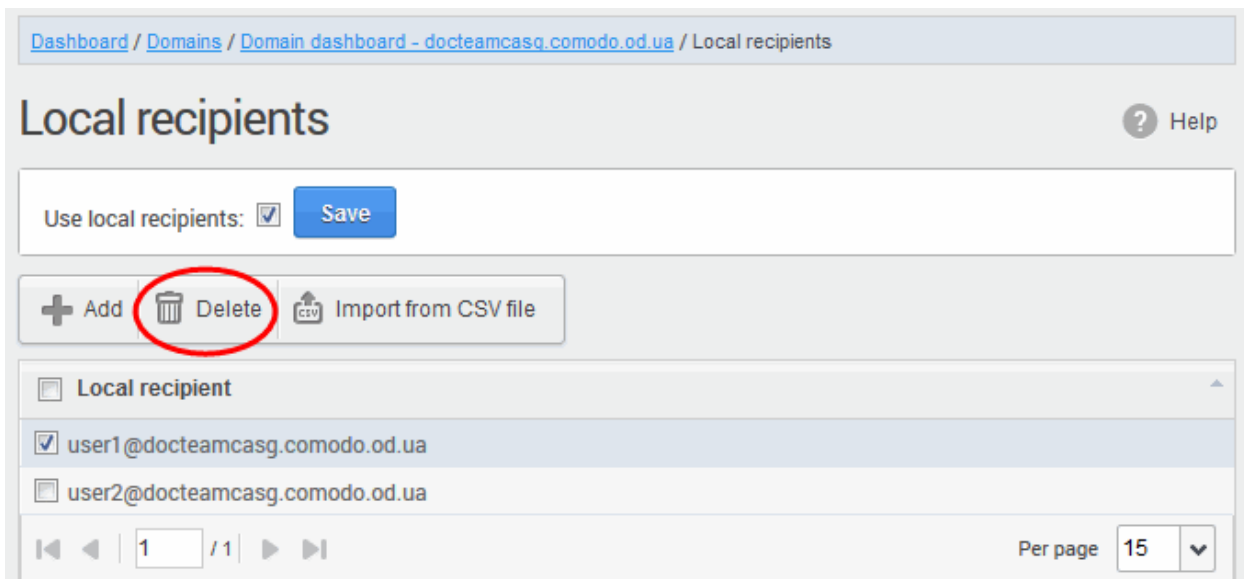
- Click the 'Save' button

Repeat the process till you have added all the users.

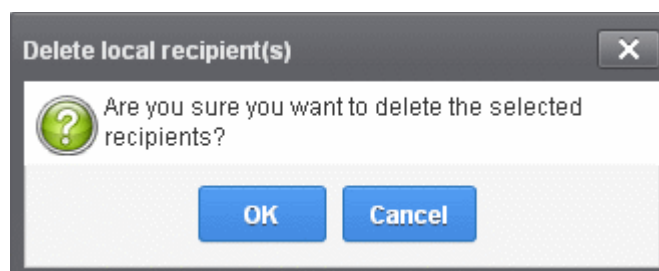


To delete a local recipient

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



- Click 'OK' to confirm.



The selected recipient will be deleted from the list

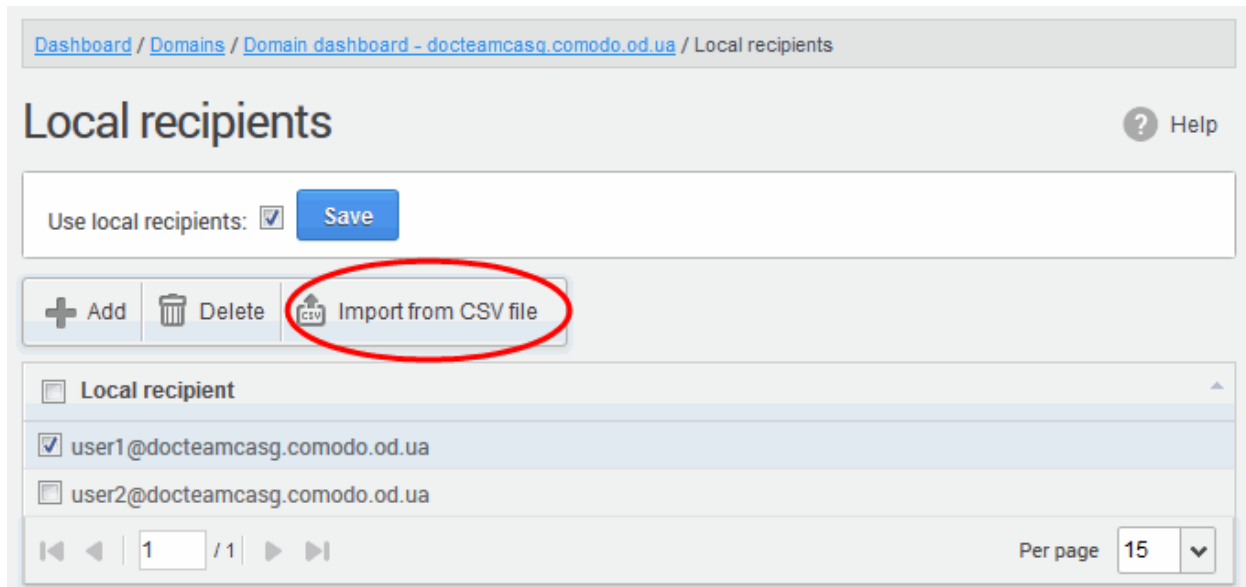
Tip: You can select multiple recipients to delete by pressing and holding the Shift or Ctrl keys.

To import local recipients from CSV file

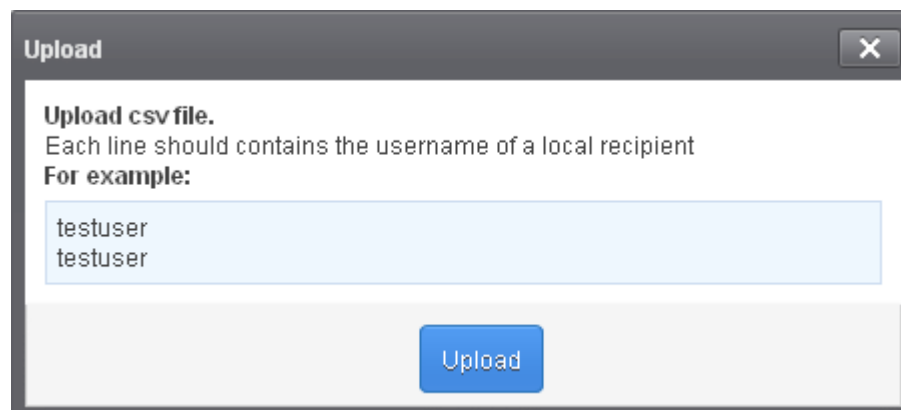
You can add many new users at a time by importing from a file. The users should be saved in separate lines as shown below:

```
user1  
user2  
user3
```

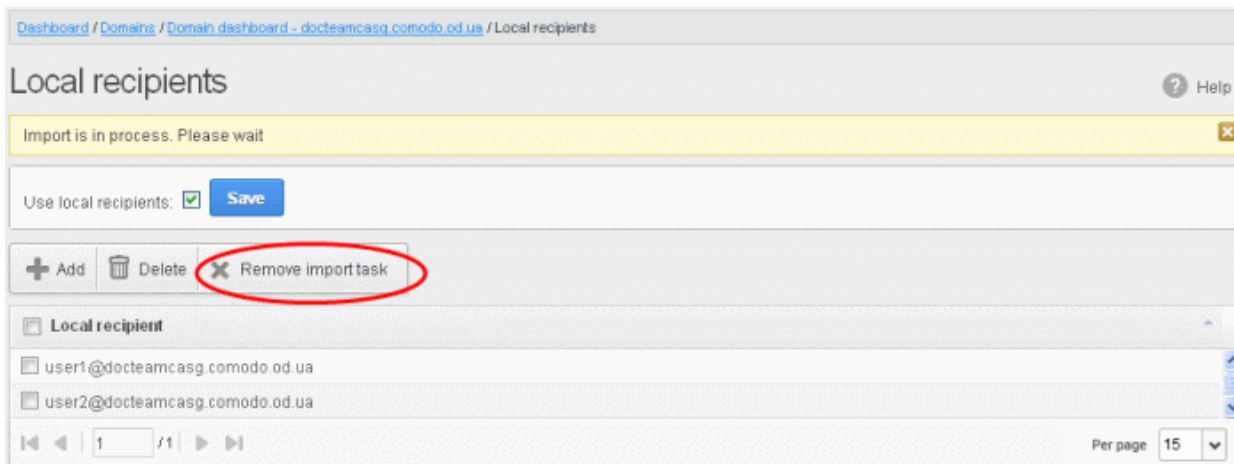
- Click the 'Import from CSV file' to import new users from a CSV file.



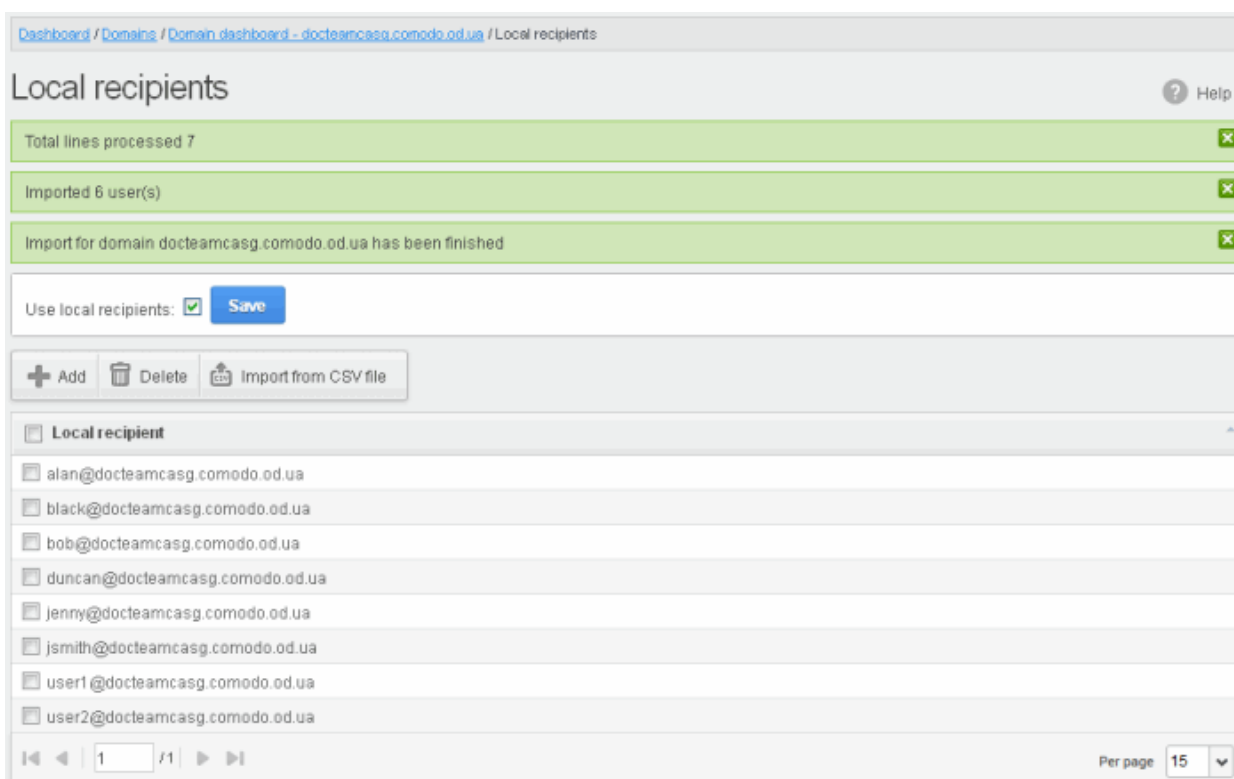
- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.



The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, the results will be displayed.



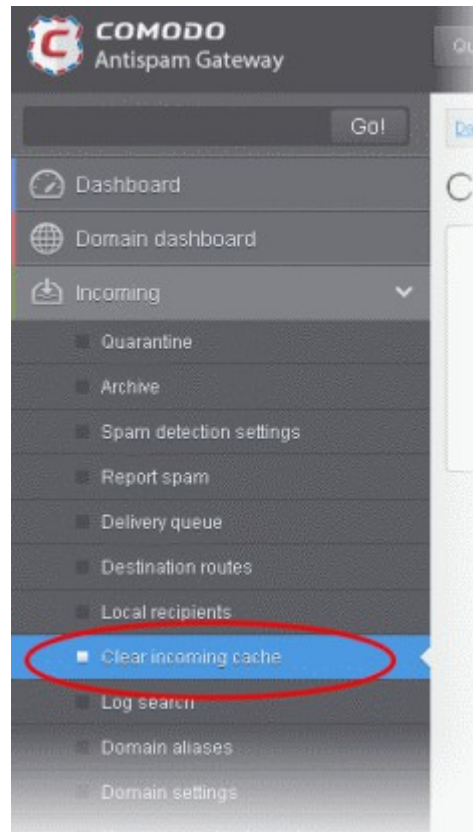
The local recipients from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

Clear Incoming Cache

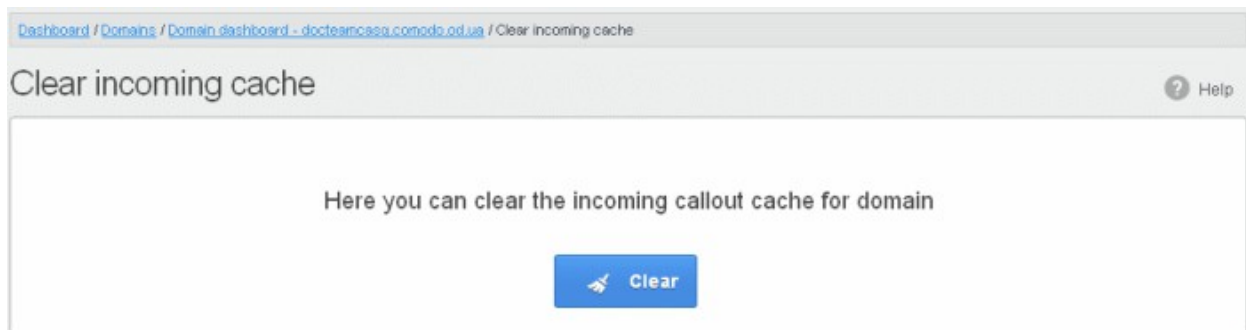
CASG continuously performs a cached recipient callouts to check that recipient email addresses do actually exist in the destination mail servers. When an email for a certain recipient is permanently rejected by the destination server with a 5xx error code, the destination address of the recipient is considered invalid and all emails sent to the recipient will be rejected. CASG filtering servers caches this information locally for up to two hours. CASG interface allows you to clear the callout cache without waiting for the servers to clear it.

To clear incoming cache

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Clear incoming cache' tab.

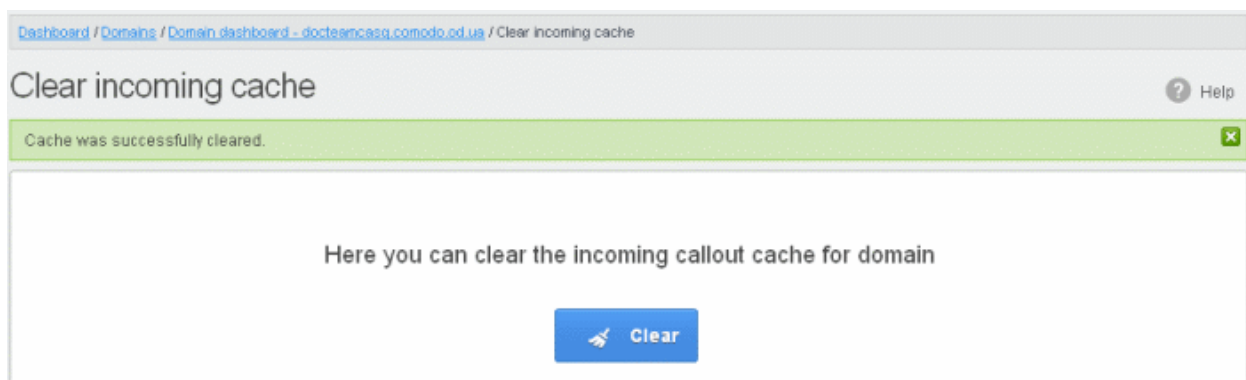


The 'Clear incoming cache' area of the selected domain will open:



- Click the 'Clear' button

The callout cache for the incoming domain is cleared.



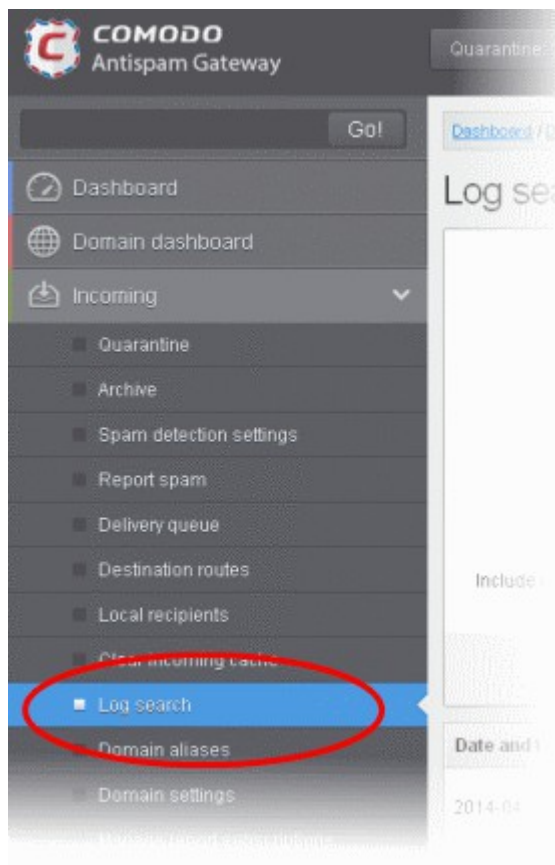
- Click the  button to close the notification.

Log Search

The Log Search option in CASG allows you to search for a specific email message.

To search logs for incoming mails

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Log search' tab.



The 'Log search (incoming)' interface of the selected domain will open:

[Dashboard](#) / [Domains](#) / [Domain dashboard - docteamcasg.comodo.od.ua](#) / [Log search \(incoming\)](#)

Log search (incoming) Help

Date range: -

Message ID:

Sender:

Recipient: @docteamcasg.comodo.od.ua

Sender IP:

Sender host:

Predicate:

Include results from the last minutes:

- **Date range:** Select the date range for which you want to search the log file. The date range for which the log search can be processed depends on the settings configured in **Domain Settings** > Log retention period.
- **Message ID** - Enter a unique message identifier (*optional*)
- **Sender:** Enter a sender email address in this field.
- **Recipient:** Enter the email address in this field (for example, 'testuser1').
- **Sender IP:** Enter the IP address of the sender.
- **Sender host:** Enter the sender host name.
- **Predicate:** You have the option to select either 'AND' or 'OR' in the drop-down. When you choose 'AND' option, all the entered search terms will be searched together and when you choose 'OR' option, the application will search any of the search items entered.
- **Include results from the last minutes:** If selected, CASG 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.

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

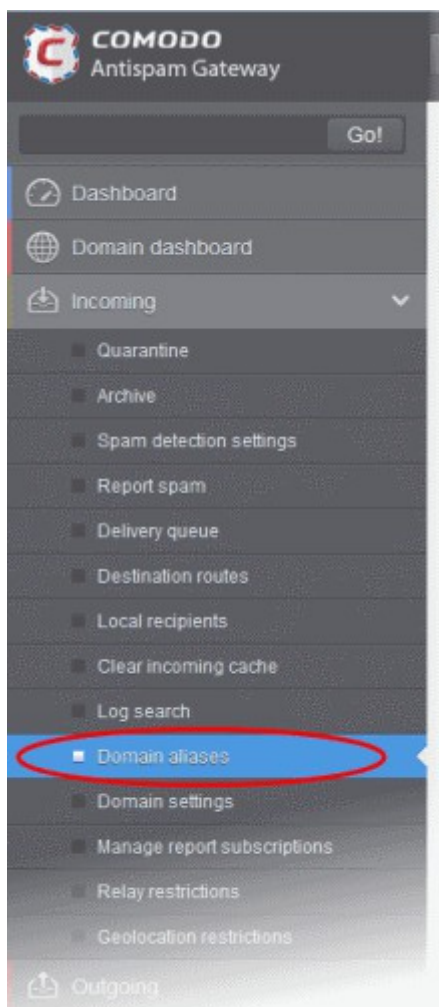
Date and time	Host (Exim id)	Sender hostname	Sender	Recipient	Subject	Classification
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xK-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xK-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo1	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo2	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:26:19	mxsrv1.spamgateway.cor 1Xj6ms-0008Pk-CK	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	Archive email 2	Accepted

Domain Aliases

The Domain aliasing feature in CASG allows the administrator to add multiple domains as aliases for the main domain. After adding a domain alias, the MX records should be configured to activate the filtering process for this domain alias. Once this is done, mails sent to users at alias domain will be filtered and delivered to users at main domain. For example, if you add *testdomain.org* as an alias domain for the main domain *testdomain.com* and mail sent to *user1@testdomain.org* will be filtered and delivered to *user1@testdomain.com*. The 'To:' headers in the email will still display the original recipient as *user1@testdomain.org*.

To add domain aliases

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Archive' tab.

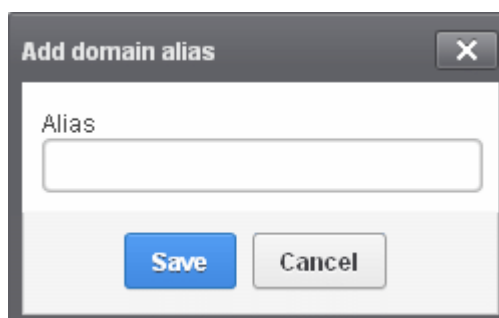


The 'Domain Aliases' interface of the selected domain will open:

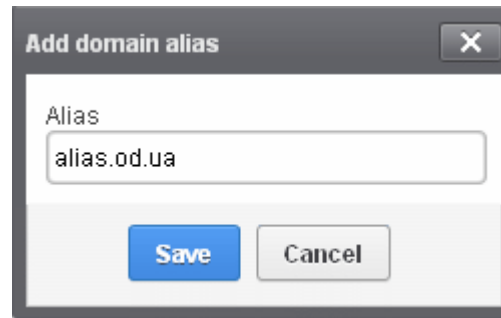


- Click the 'Add' button to add a domain alias for the selected domain

The 'Add domain alias' dialog box will open.



- Enter the domain alias name in the 'Alias' field

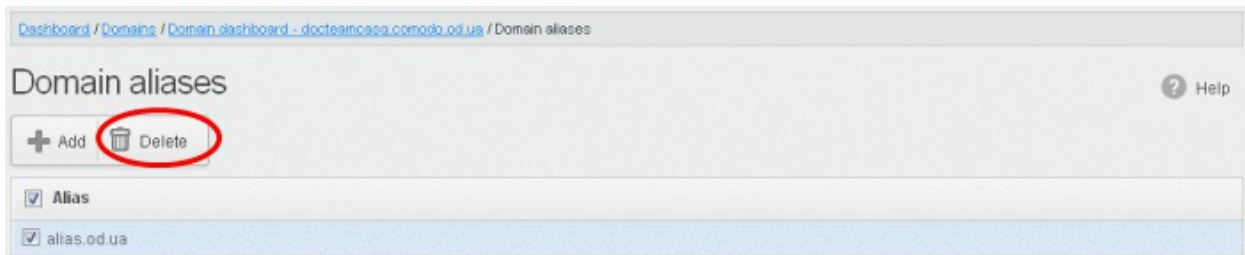


- Click the 'Save' button

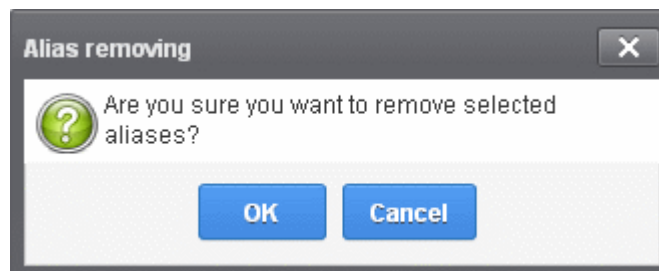
The domain will be added to the main domain as alias and will be listed in the interface.



- To delete a domain alias, select the domain alias from the list and click the 'Delete' button



- Click 'OK' to confirm the deletion.



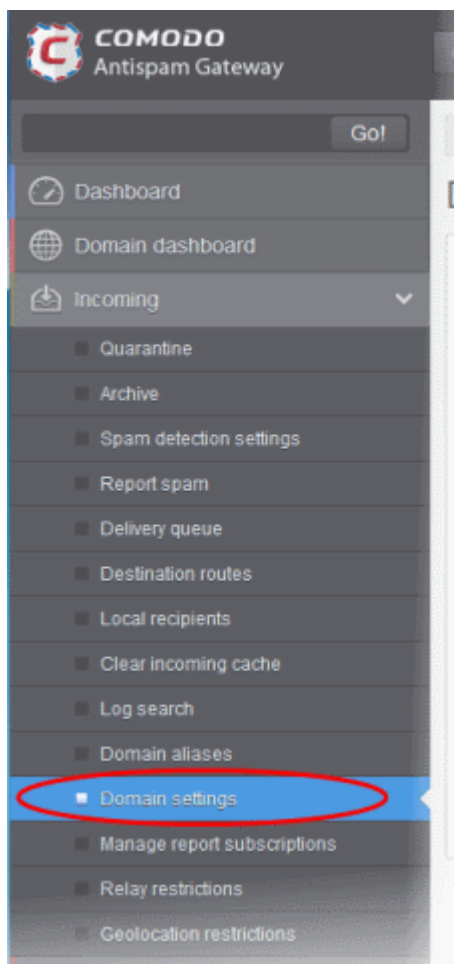
The selected domain alias will be deleted from the list.

Domain Settings

An administrator can configure various settings for the selected domain such as primary contact email address, the administrator's email address and maximum number of bounces allowed before a mail being rejected.

To configure domain settings

- Click the 'Incoming' tab on the left hand side navigation to expand and then click the 'Domain settings' tab.



The 'Domain Settings' interface of the selected domain will open:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Domain settings

Domain settings Help

Maximum bounces:

Log retention period:

Maximum days to retry:

Change locale for system messages:

Max. number of users:

Enable archive cleanup:

Retain Archived items for:

Enable user auto-login:

Days before cookie expiration:

Email for license notifications:

Timezone:

- **Maximum bounces:** Each recipient of the selected domain will be limited to receive only these many message bounces set in this field per hour (messages from postmaster addresses or with an empty envelope sender). Please note that if the number of bounces exceeds the limit set in this field, the messages are not quarantined but are permanently rejected and will not be received later. You can set this to a low value, if the users at the selected domain do not send mails to invalid addresses frequently. By default this field is set to 6000.
- **Log retention period:** All spam and non spam email connections to a domain are logged in the CASG server. By default the storage period of this log is 30 days. You can store the log for a longer period by entering the number of days that you want to store in the field. After the end of set period, the log data will be moved to a separate storage and cannot be retrieved.
- **Maximum days to retry:** If the destination route has temporary problems, the messages are queued and automatically retried at fixed intervals for the number of days entered in the field. Even after this period if the emails cannot be delivered, they are bounced to the sender. By default, this is set to 4 days, the main reason being that the senders should be aware that his\her messages are not being delivered for 4 days.
- **Change locale for system messages:** Allows you to choose the language in which the messages from CASG are to be displayed and sent to the administrators of the domain, according to the location of them. Choose the language from the drop-down.
- **Max. number of users:** Enter the maximum of users that can be added for this domain. Leaving this setting as 'Unlimited' will allow you to add up to, but not exceed, the maximum number of users permitted by your current license. This can also be done while **creating a domain** or in the **editing domain** interface.
- **Enable archive cleanup:** Allows you to enable or disable the auto-clean up of archived incoming mails in the archive storage. This option is available for customers that has purchased archive storage from Comodo.
- **Retain Archived items for:** Allows you to set the period in months or days, for which the archived mails should be retained in the archive storage, if you have enabled archive clean-up. The messages that are older than the period set in this field will be purged automatically.
- **Enable user auto-login:** If enabled, end-users can login into their CASG account without entering their

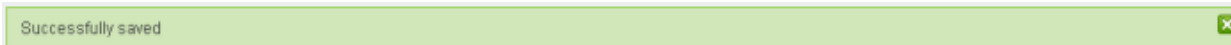
credentials. On first login, the users will be asked to confirm their auto login. The users can also change the settings on their 'My Profile' page. The users' credentials will be stored in the browser as auto-login cookie and will be valid for the number of days that is entered in the next field 'Days before cookie expiration'.

- **Days before cookie expiration:** Allows you to enter the validity period of the auto-login cookie (in days) for the end-users, if you have enabled user-auto-login. Upon expiry of the cookie, the users need to provide credentials while accessing their CASG account. The period starts after each login by the user.
- **Email for license notification:** Enter the email address for receiving license notifications for this domain. You can enter different email addresses for different domains for receiving notifications with respect to CASG license. If the field is left blank, then license notifications will be sent to admins' registered email address in Comodo Accounts Manager (CAM).
- **Timezone** - Allows you to choose the zone for the domain, depending on the location from which it is hosted. CASG will use the selected time-zone for events which concern that domain, especially for maintaining the quarantine list, archive list, log search, reports and report subscriptions.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field, but CASG checks if the total number of users for all domains is within your license limit.

- Click 'Reset to default' to reset default settings in CASG.
- Click the 'Save' button.

A confirmation dialog indicating the successful configuration of the domain settings will be displayed. Click 'X'.

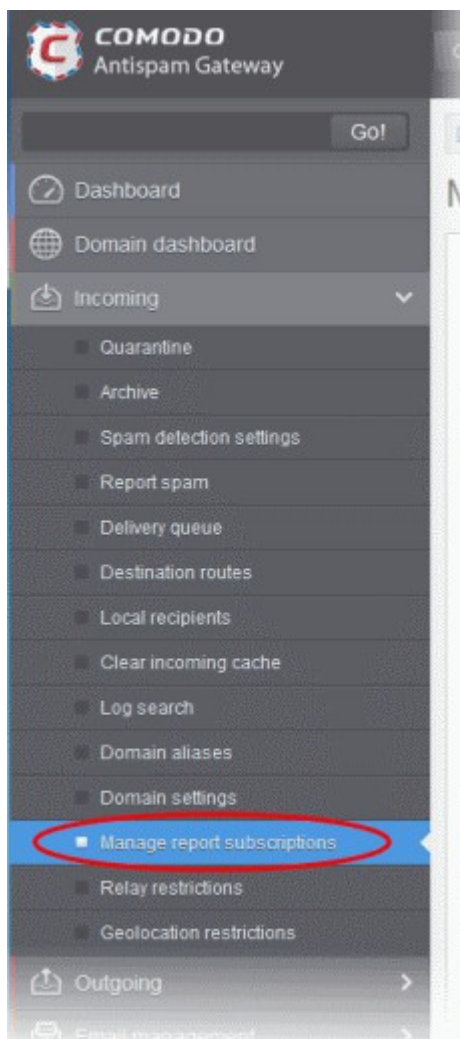


Manage Report Subscriptions for Selected Domain

The Manage report subscriptions interface accessible from the 'Incoming' configuration area of a selected domain allows the administrator to configure the subscription to the periodical Domain, User import and Quarantine summary reports generated for that domain. The administrator can also specify the self and peer administrators of that domain to whom the reports are to be delivered. Refer to **CASG Reports - an Overview** for more details on the reports.

To access Manage report subscriptions interface

- Click the 'Incoming' tab from the left hand side navigation to expand it and then click the 'Manage report subscriptions' tab.



The 'Manage report subscriptions' interface will be displayed:

The Report recipients field will not be auto-populated as it does in the interface of **Customer Management > Managing Report Subscriptions**. Enter the email address of the administrators belonging to that domain in the text field separated by a comma after each email address.

- You can expand/collapse a report configuration section by clicking on the respective strip.
- Clicking the 'Reset settings to default' button will disable all the reports. The 'Report Recipients' field will not be cleared.

The administrator can configure the subscription for three types of reports from this interface:

- **Quarantine Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the mails that are identified as spam or containing malicious content and moved to Quarantine of the domain automatically by CASG. Refer to **CASG Reports - An Overview** for more details.
- **Domain Statistics Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of number of users, mails that have been received at and sent from the domain, number of spams identified and blocked and so on. Refer to **CASG Reports - An Overview** for more details.

Overview for more details.

- **Users auto-import report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain details of new users that were auto-imported based on incoming mails received for them at the mail server. For more details on configuring CASG for auto-importing new users, refer to the section **Managing User Auto-import**. For more details on the reports, refer to the section **CASG Reports - An Overview**.
- **Quarantine Release Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the quarantined mails that are released by the administrator to the recipient. Refer to **CASG Reports - An Overview** for more details.
- **Reported Spam Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly will contain a detailed statistics of the mails that are reported as spam by administrators and users. Refer to **CASG Reports - An Overview** for more details.

To configure the subscription of the reports

- If you want the administrators of the account to receive the periodical reports, select the 'Enabled' checkbox in the row of the respective report type. If both the reports are required, you can select both the checkboxes.
- Leave the 'Send empty' checkbox unchecked if empty reports are not to be sent to recipients.
- Select the frequency of the report to be sent to the administrators from the options for:
 - **Quarantine Report;**
 - **Domain Statistics Report;**
 - **User Auto-Import Report;**
 - **Quarantine Release Report;** and
 - **Reported Spam Report.**

Quarantine Report

Quarantine report						
Hour	Day of month	Day of week	Send empty	Enabled	Start date (GMT)	Report length
<input type="radio"/> Every hour <input checked="" type="radio"/> Choose 0 1 2 3 4	<input checked="" type="radio"/> Every day <input type="radio"/> Choose 1 2 3 4 5	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <input checked="" type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29, 2015 03:00	Next report for 3 day(s) from last run (2015-06-25 17:00)

- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that will be generated depending on the options chosen.

Domain Statistics Report

Period	Hour	Day of month	Day of week	Send empty	Enabled	Start date (GMT)	Report length
Weekly	<input checked="" type="radio"/> Every hour <input type="radio"/> Choose 0 1 2 3 4	<input checked="" type="radio"/> Every day <input type="radio"/> Choose 1 2 3 4 5	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 29, 2015 00:00	Next report for last week(s) from last run (2015-06-22 17:00)

- **Period** - Enables you to set the period to be covered in the report. The report will contain the statistics of all the domains in the account for the past one hour, one week, one month or one year, as selected from drop-down from the scheduled report time.
- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that will be generated depending on the options chosen.

User Auto-Import Report

Hour	Day of month	Day of week	Send empty	Enabled	Start date (GMT)	Report length
<input type="radio"/> Every hour <input checked="" type="radio"/> Choose 3 4 5 6 7	<input type="radio"/> Every day <input checked="" type="radio"/> Choose 1 2 3 4 5	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Feb 05, 2016 05:00	Next report for 224 day(s) from last run (2015-06-25 17:00)

- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that will be generated depending on the options chosen.

Quarantine Release Report

Hour	Day of month	Day of week	Send empty	Enabled	Start date (GMT)	Report length
<input type="radio"/> Every hour <input checked="" type="radio"/> Choose 0 <input checked="" type="checkbox"/> 1 2 3 4	<input checked="" type="radio"/> Every day <input type="radio"/> Choose 1 2 3 4 5	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 28, 2015 01:00	Next report for 95 day(s) from last run (2015-03-25 00:00)

- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that will be generated depending on the options chosen.

Reported Spam Report

Hour	Day of month	Day of week	Send empty	Enabled	Start date (GMT)	Report length
<input type="radio"/> Every hour <input checked="" type="radio"/> Choose 0 <input type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 3 4	<input checked="" type="radio"/> Every day <input type="radio"/> Choose 1 2 3 4 5	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jun 28, 2015 02:00	Next report for 95 day(s) from last run (2015-03-25 00:00)

- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
 - **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
 - **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
 - **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
 - **Report length** - Displays the period of the report that will be generated depending on the options chosen.
- Click 'Save' for your settings to take effect.

Relay Restrictions

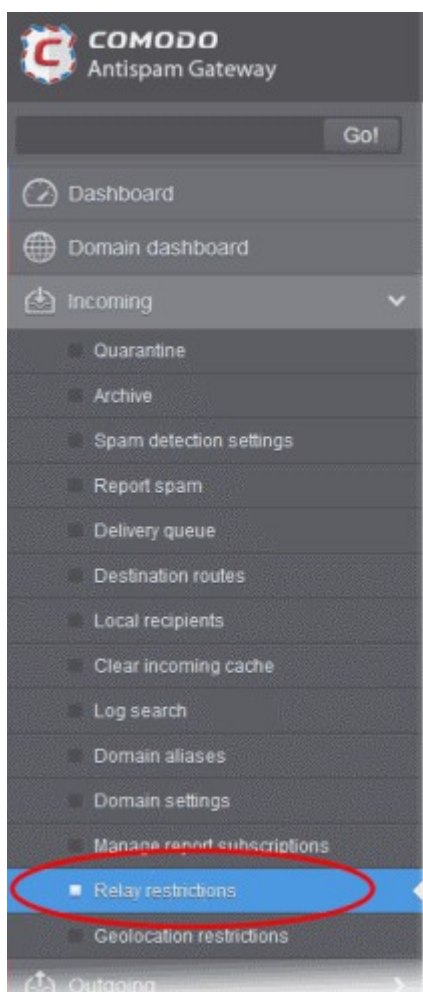
The 'Relay restrictions' interface allows administrators to specify Message Transfer Agents (MTA), mail servers or other mail relays from which incoming mail to a domain should be accepted or strictly rejected.

For example, a business that has regional offices can configure their regional systems to accept only incoming emails from the email servers at the home office.

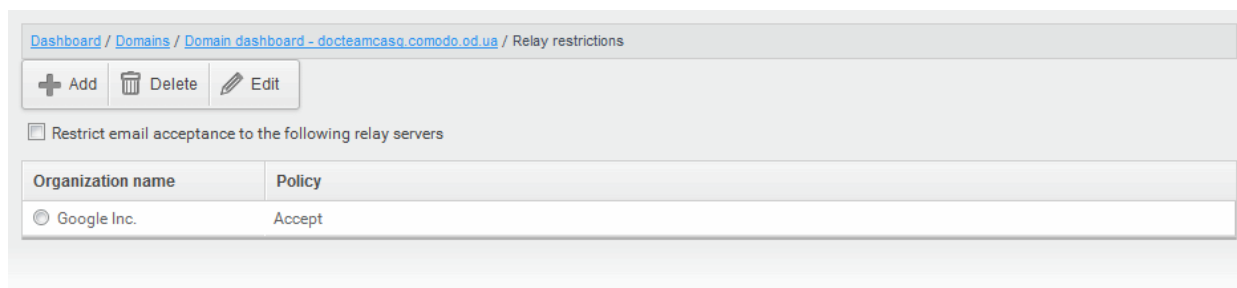
Email administrators can define the Organization names from which emails can be accepted or rejected. CASG parses the mail headers of each incoming mail to ensure the existence of an MTA's IP address or FQDN of the organization before accepting the mail. If the organization name is not known, administrators can use the 'Lookup' feature from the interface itself by entering the IP address of the email domain name of an incoming mail.

To add a relay restriction rule

- Click the 'Incoming' tab from the left hand side navigation then click the 'Relay Restrictions' tab:



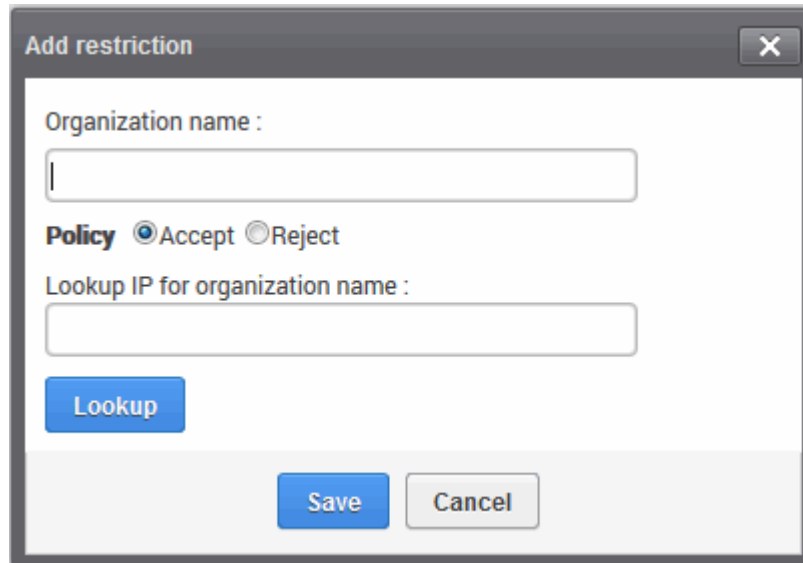
The relay restrictions interface for the selected domain will open:



- Select the 'Restrict email acceptance to the following relay servers' check box .

- Click the 'Add' button

The 'Add restriction' dialog will appear.



- Enter the organization name in the 'Organization name' text box
 - If you are not sure about the organization name, obtain the IP address of the mail server from any incoming mail from the organization and enter it in the 'Lookup IP for organization name' field. Click 'Lookup' to perform the search.
 - CASG will perform a lookup from WHOIS.com website and auto-populate the Organization name field.
- Choose the acceptance policy for emails from the organization's mail server:
 - Accept - All mails from the selected organizations will be accepted. Those from other organizations will be blocked.
 - Reject - All mails from the selected organizations will be blocked. Those from other organizations will be accepted.
- Click 'Save' for the rule to take effect.

Relay restrictions now enabled.



- Repeat the process till you have added all the organizations.

The administrator need to add a rule for each organization from which the mails are to be accepted or rejected.

Illustrations:

1. For example, if you want to accept mails only from two domains, namely gooddomain1.com and gooddomain2.com and reject mails from all the other mail servers, create two rules, one for gooddomain1.com and other for gooddomain2.com.

- Rule 1 - Accept gooddomain1.com and block all other domains
- Rule 2 - Accept gooddomain2.com and block all other domains

Only the incoming mails from gooddomain1.com and gooddomain2.com will be accepted. Those from all the other domains will be rejected.

2. For example, if you want to block mails only from two domains, namely baddomain1.com and baddomain2.com and allow mails from all the other mail servers, create two rules, one for baddomain1.com and other for baddomain2.com.

- Rule 1 - Reject baddomain1.com and allow all other domains

- Rule 2 - Reject baddomain2.com and allow all other domains

Only the incoming mails from baddomain1.com and baddomain2.com will be blocked. Those from all the other domains will be accepted.

You can create any number of 'Allow' and 'Reject' rules. The 'Accept' rules have more priority and reject rules will be skipped in case of any rule conflict.

The incoming mails from blacklisted domains in the global or domain blacklist will be rejected even if they are accepted by the relay restrictions rules. The priority order of rules checked on allowing an email is as follows:

1. Global blacklist
2. Domain whitelist/blacklist
3. Relay restriction rules
4. Per user whitelist/blacklist

Note: The 'Relay restrictions' is disabled for TRIAL customers.

Editing Relay Restriction Rules

You can change the organization name or acceptance policy of any rule at any time.

To edit a rule

- Choose the rule to be edited and click the 'Edit' button.

The screenshot shows the 'Relay restrictions' page in the Comodo Antispam Gateway administration interface. The page title is 'Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Relay restrictions'. There are three buttons: '+ Add', 'Delete', and 'Edit'. The 'Edit' button is circled in red. Below the buttons, there is a checkbox labeled 'Restrict email acceptance to the following relay servers' which is checked. A table lists the relay servers:

Organization name	Policy
<input type="radio"/> Google Inc.	Accept
<input type="radio"/> Yahoo	Accept
<input checked="" type="radio"/> Rediff.com India Limited,	Accept

The 'Rediff.com India Limited,' row is highlighted in blue. A red arrow points from the 'Edit' button to the 'Add/Edit restriction' dialog box. The dialog box has the following fields:

- Organization name: Rediff.com India Limited,|
- Policy: Accept Reject
- Lookup IP for organization name: (empty field)
- Buttons: Lookup, Save, Cancel

The Add/Edit restriction dialog will appear.

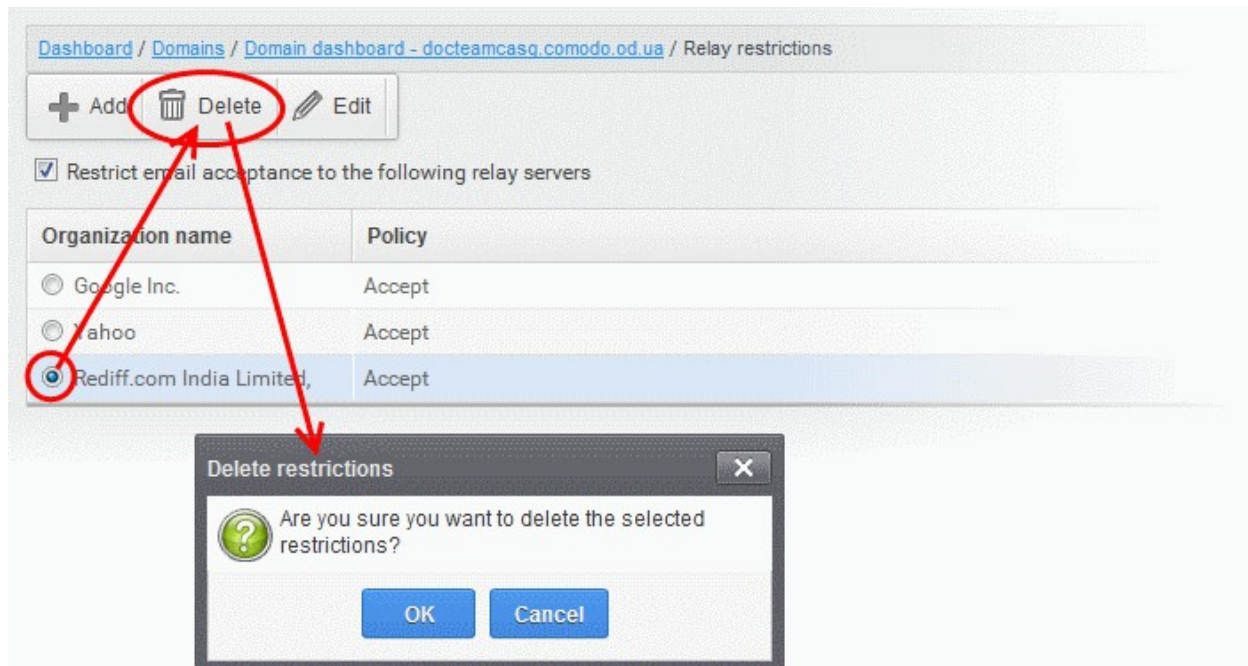
- Edit the fields and policy options as required. For more details refer to the explanation under **To add a Relay Restriction Rule**.
- Click 'Save' for your changes to take effect.

Removing Relay Restriction Rules

You can remove unwanted rules at anytime from CASG.

To remove a Relay Restriction rule

- Choose the rule you want to remove and click the 'Delete' button



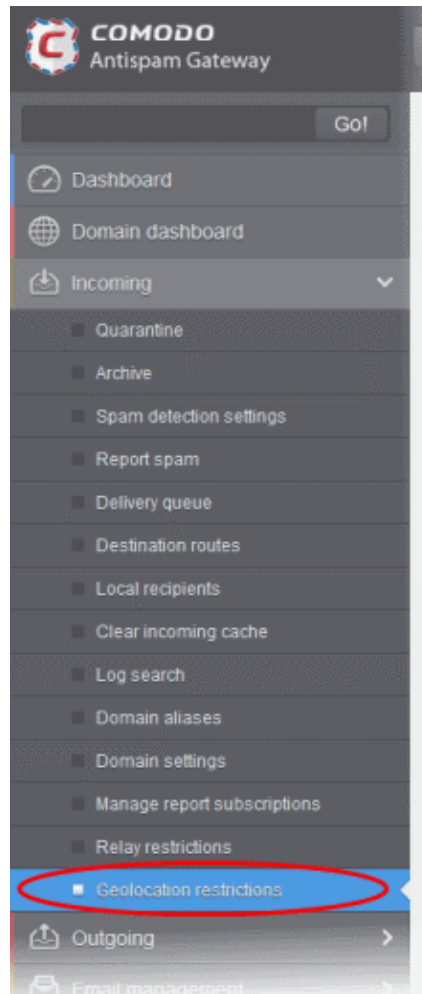
- Click 'OK' in the confirmation dialog.

Geolocation Restrictions

The 'Geolocation restrictions' interface allows administrators to specify the country from which CASG administrators and users can access the CASG web interface. By creating access control policies, you have better control in deciding from which locations admins and users can access the web interface thus minimizing the security threat.

To create a geolocation policy

- Click the 'Incoming' tab from the left hand side navigation then click the 'Geolocation restrictions' sub tab:



The geolocation restrictions interface for the selected domain will open:



- **Enable geolocation restrictions** - Allows administrators to apply the geolocation restriction policies. Select the check box to apply the policies in the list.

From the interface, you can:

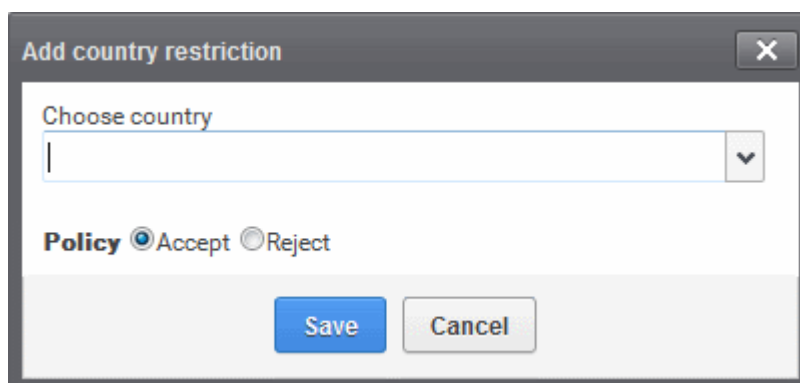
- **Add a geolocation restriction policy**
- **Edit a geolocation restriction policy**
- **Delete a geolocation restriction policy**

To add a new geolocation restriction policy

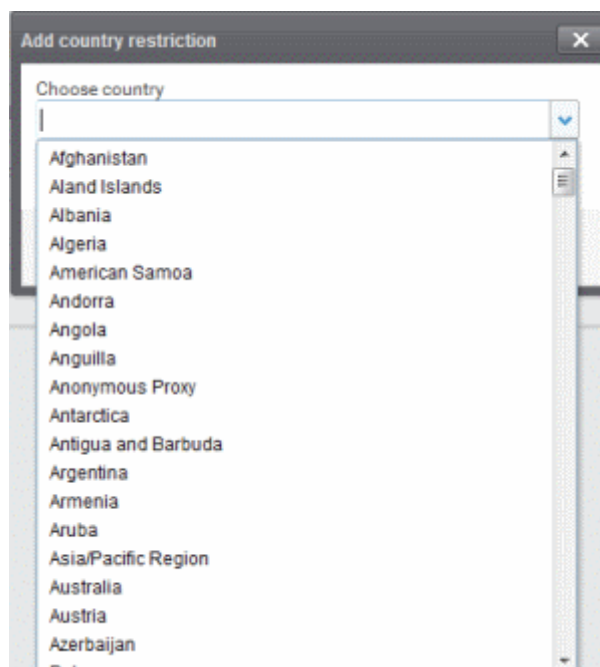
- Click the 'Add' button



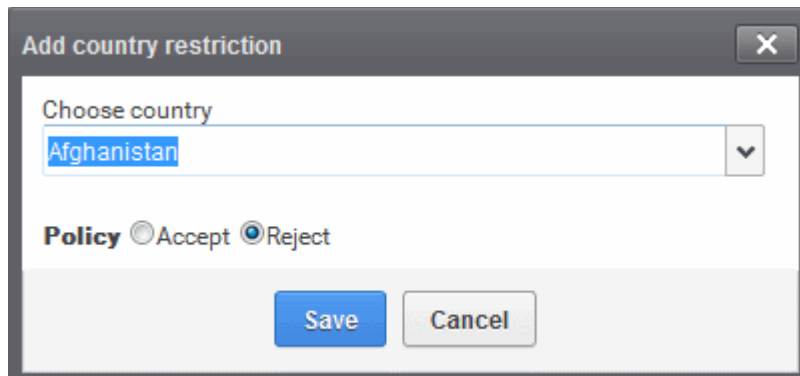
The 'Add country restriction' dialog will appear.



- Select the country from the 'Choose country' drop-down



- Choose the geolocation restriction policy for accessing the CASG web interface
- Accept - Admins and users from these countries are allowed to access the web interface
- Reject - Admins and users from these countries are not allowed to access the web interface



Add country restriction

Choose country
Afghanistan

Policy Accept Reject

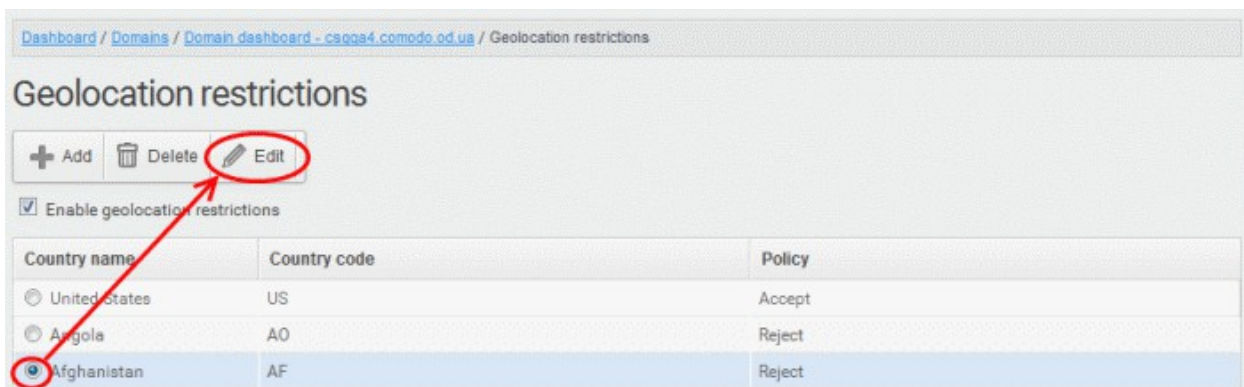
Save Cancel

- Click 'Save' to create the policy

To edit a geolocation restriction policy

A geolocation restriction policy cannot be edited for a country. But you can change the country for the policy.

- Select the policy for which you want to change the country and click the 'Edit' button



Dashboard / Domains / Domain dashboard - cs00a4.comodo.od.ua / Geolocation restrictions

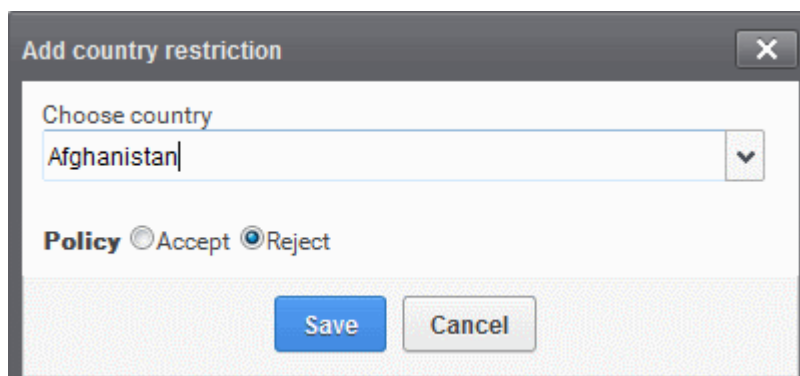
Geolocation restrictions

+ Add Delete Edit

Enable geolocation restrictions

Country name	Country code	Policy
<input type="radio"/> United States	US	Accept
<input type="radio"/> Angola	AO	Reject
<input checked="" type="radio"/> Afghanistan	AF	Reject

- Select a different country from the drop-down



Add country restriction

Choose country
Afghanistan

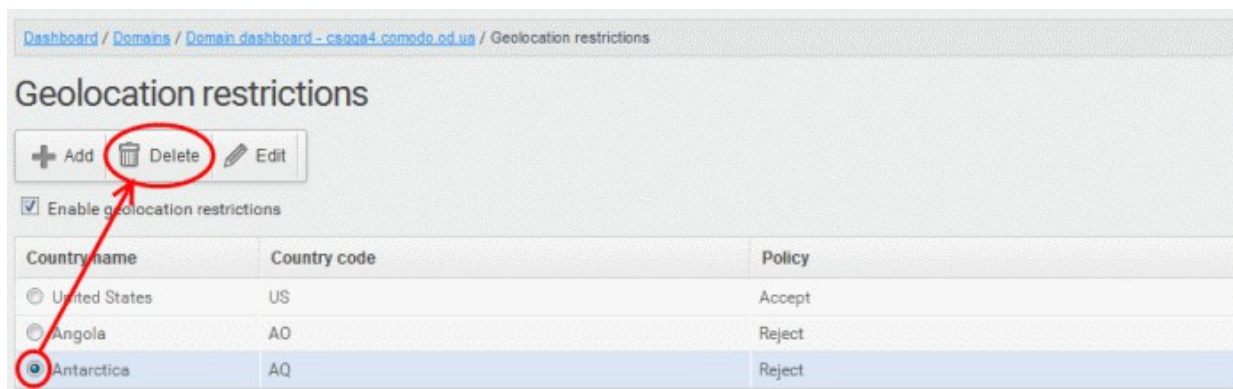
Policy Accept Reject

Save Cancel

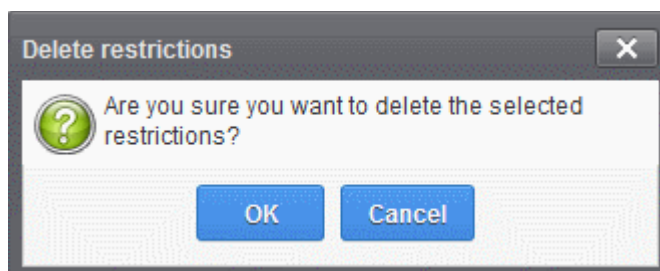
- Click the 'Save' button for the changes to take effect

To delete a geolocation restriction policy

- Select the policy that you want to remove from the list and click the 'Delete' button



- Click 'OK' to confirm the removal of the selected geolocation restriction policy from the list



The policy will be removed from the list.

3.2.1.1.4.3 Outgoing

To be able to send outgoing email, first a valid user needs to be added to the filter cluster. This can be done from the **web interface**. The following ports are available for the outgoing service:

- SMTP AUTH: Port 25 or 587
- SMTP StartTLS Port 587
- SMTP SSL Port 465

Comodo recommends port 587. The outgoing service listens by default on all IPv4 addresses activated on the server.

Create a separate outgoing user on the filtering cluster for each end-user to relay outgoing email and use an **"automatic user locking"** to automatically close the account in case abuse is detected. There are two methods you can make per-user authentication to work - The first method is to instruct all end-users to authenticate directly to the filter cluster for their outgoing emails or in the second method, configure your current outgoing SMTP server so that it authenticates each end-user separately to the filter cluster for all outgoing emails. If you choose the second method, how easily you can configure your SMTP server depends on the SMTP software.

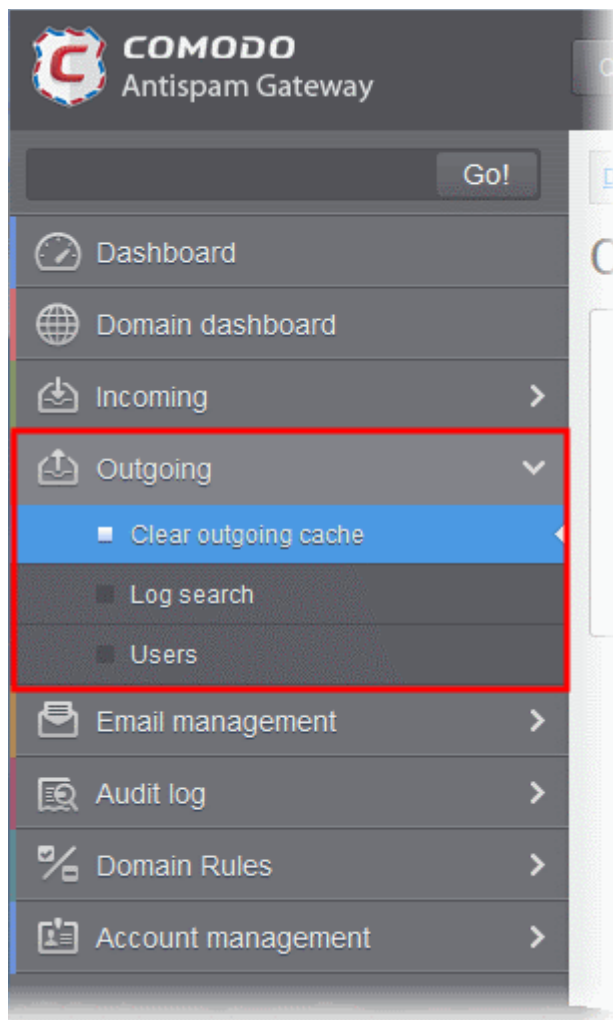
While using per-user authentication for outgoing mails, ensure to set the limits correctly based on the usage of the end-user and enable automatic locking.

If you find using the per-user authentication method for outgoing mails too cumbersome to set up, the other alternative is to use smarthost setup. In this method, you add a single outgoing account either based on IP or username/password in the filtering server and point all outgoing emails to this server, thus using the filtering cluster as smarthost. Most email servers have **'smarthost setting'** feature with which you can easily accomplish the task of configuring outgoing email filtering. Make sure to disable the **'automatic user locking'** setting to prevent the full server account getting locked even if one end-user sends out spam email. Also ensure to enable **'block spam'** so that individual spam messages will be blocked and the administrator notified.

While using smarthosting setup for outgoing mail filtering, ensure to set the limits correctly per user based on the server.

In the 'Outgoing' area of the Manage Domain section you can set a user account for spam checking, clear outgoing

cache, search for outgoing email messages and outgoing spam checking.



Click the following links for more details:

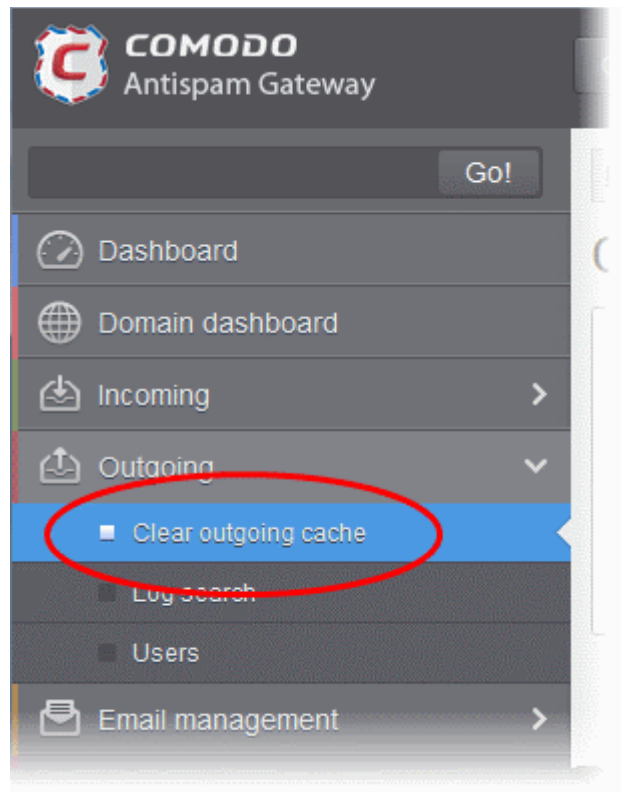
- [Clear outgoing cache](#)
- [Log search](#)
- [Users](#)

Clear outgoing cache

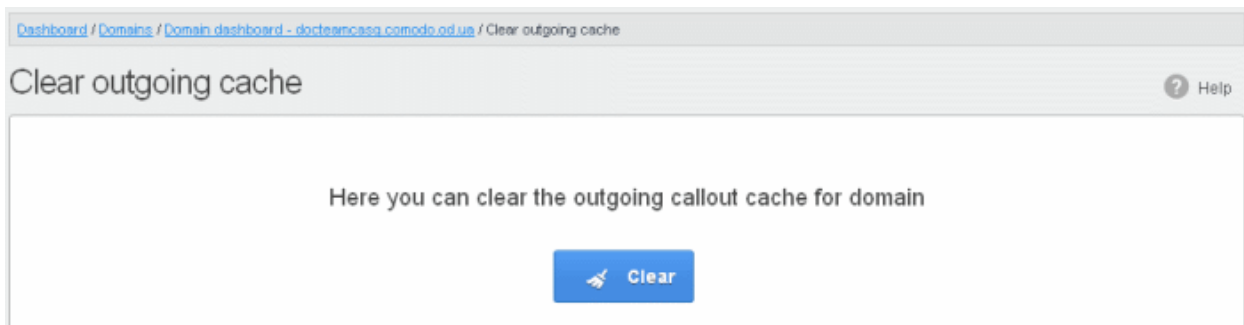
CASG continuously performs a cached recipient callouts to check that recipient email addresses existing/non-existing email accounts at the destination mail servers to minimize the number of recipient callouts. When an email for a certain recipient is permanently rejected by the destination server with a 5xx error code, the destination address of the recipient is considered invalid and all emails sent to the recipient will be rejected. CASG filtering servers caches this information locally for up to two hours. CASG interface allows you to clear the callout cache without waiting for the servers to clear it.

To clear outgoing cache

- Click the 'Outgoing' tab on the left hand side navigation to expand and then click the 'Clear outgoing cache' sub tab.

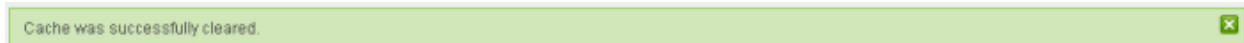


The 'Clear outgoing cache' area of the selected domain will be displayed:



- Click the 'Clear' button.

The callout cache for the outgoing domain is cleared.

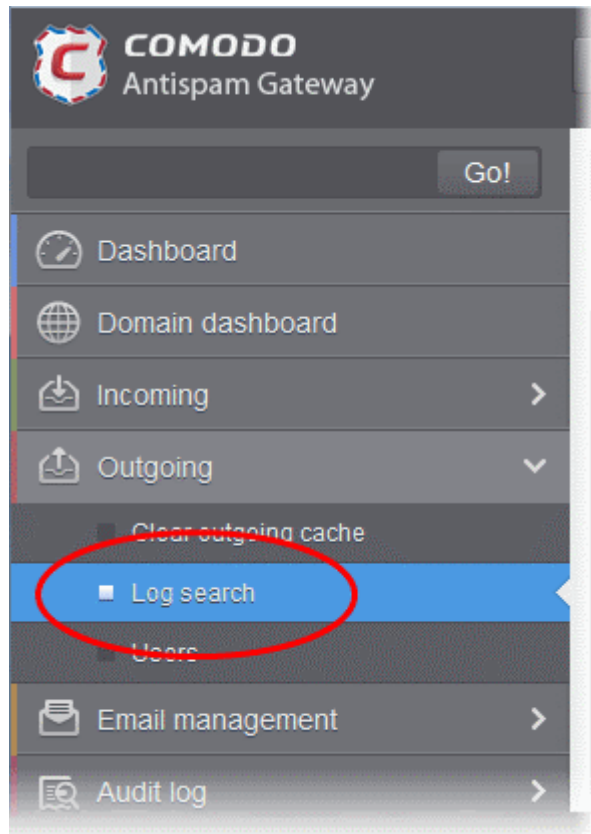


- Click 'X' to close the 'Cache successfully cleared' dialog box.

Log search

The Log Search option in CASG allows you to search for a specific outgoing email message.

- Click the 'Outgoing' tab on the left hand side navigation to expand and then click the 'Log search' sub tab.



The 'Log Search (Outgoing)' interface of the selected domain will be displayed:

[Dashboard](#) / [Domains](#) / [Domain dashboard - docteamcasg.comodo.od.ua](#) / Log search (outgoing)

Log search (outgoing) Help

Date range: -

Message ID:

Sender:

User:

Recipient:

Sender IP:

Sender host:

Predicate:

Classification:

Include results from the last minutes:

- **Date range:** Select the date range for which you want to search the log file. The date range for which the

log search can be processed depends on the settings configured in **Domain Settings** > Log retention period.

- **Message ID** - Enter a unique message identifier (*optional*)
- **Sender**: Enter the sender email address in this field.
- **User**: Enter the username of the outgoing email address for in this field (for example, 'testuser1').
- **Recipient**: Enter the email address in this field. (for example, 'testuser1@example.com').
- **Sender IP**: Enter the IP address of the sender.
- **Sender host**: Enter the sender host name.
- **Predicate**: You have the option to select either 'AND' or 'OR' in the drop-down. When you choose 'AND' option, all the entered search terms will be searched together and when you choose 'OR' option, the application will search any of the search items entered.
- **Classification**: Select the type of email that you want to search from the drop-down options.
- **Include results from the last minutes**: If selected, CASG 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. CASG will search for the entered terms and display the results.

Date and time	Host (Exim id)	Sender hostname	Sender	Recipient	Subject	Classification
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xK-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:37:05	mxsrv1.spamgateway.cor 1Xj6xK-0008ET-B2	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,DQ demo 2	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo1	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:36:33	mxsrv1.spamgateway.cor 1Xj6wo-0007pb-Ag	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	,Re: DQ demo	Accepted Message content looked like non-spam
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo1	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:34:32	mxsrv2.spamgateway.cor 1Xj6up-00070G-Jb	mxsrv1.spamgateway.cor 178.33.199.65	demo@csg.comodo.od.u	demo2	,DQ demo	Rejected Rejected by relay restriction for this recipient
2014-10-28 13:26:19	mxsrv1.spamgateway.cor 1Xj6ms-0008Pk-CK	mxsrv2.spamgateway.cor 178.33.199.66	demo@csg.comodo.od.u	demo2	Archive email 2	Accepted

Sorting the Entries

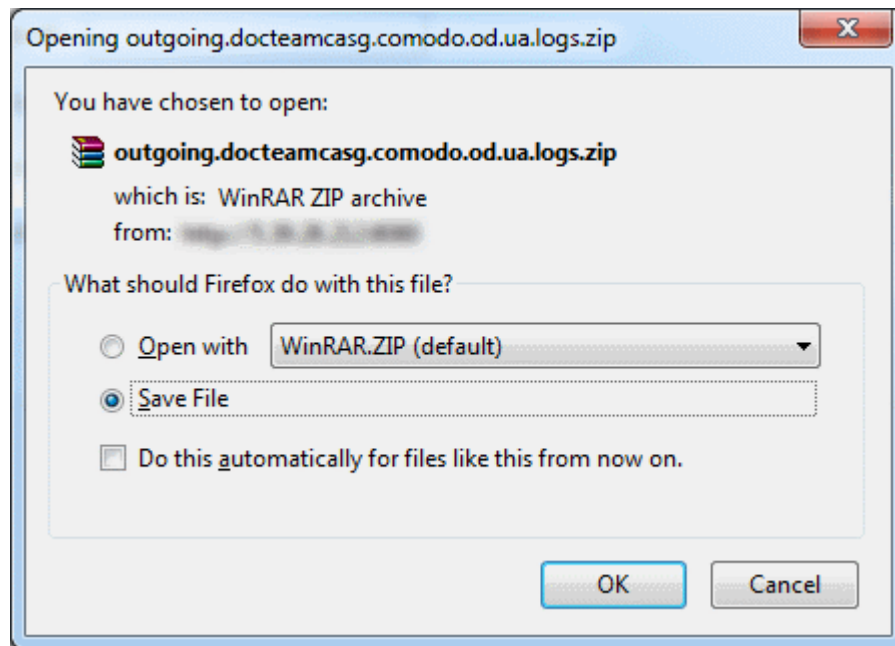
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Downloading the Report

The '**Download**' button allows users to download the log report of sent mails for the filters entered and/or selected.

- Click the Download button.

The download dialog will be displayed.



You can choose to 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 appropriate application such as Excel or Openoffice Calc for easy analysis.

Users

Outgoing email messages should be checked for spam or malicious content because of the risk such content poses to the organization's reputation. Often the outbound email path bypasses the system that scans incoming emails from the internet, and instead sends the emails directly out to the destination. Filtering the outgoing user's mail also prevent spam from reaching end user mailboxes.

Configuring User's Email Client for Outgoing Mail Filtering

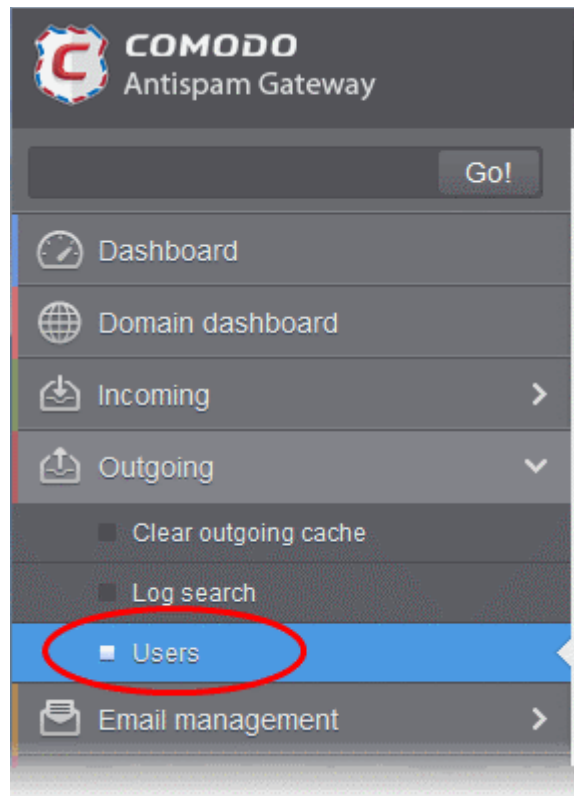
The email clients of the users added for outgoing email filtering must be configured to point to CASG service.

In the Account Settings interface of the user's email client, enter the following details:

- Smtip server: mxpool1.spamgateway.comodo.com
- Connection Security: STARTTLS or SSL
- Port : 587
- Username: <username@domainname.com>

To access the 'Outgoing users' interface:

- Click the 'Outgoing' tab on the left hand side navigation to expand and then click the 'Users' sub tab.



The 'Users' interface of the selected domain will be displayed:

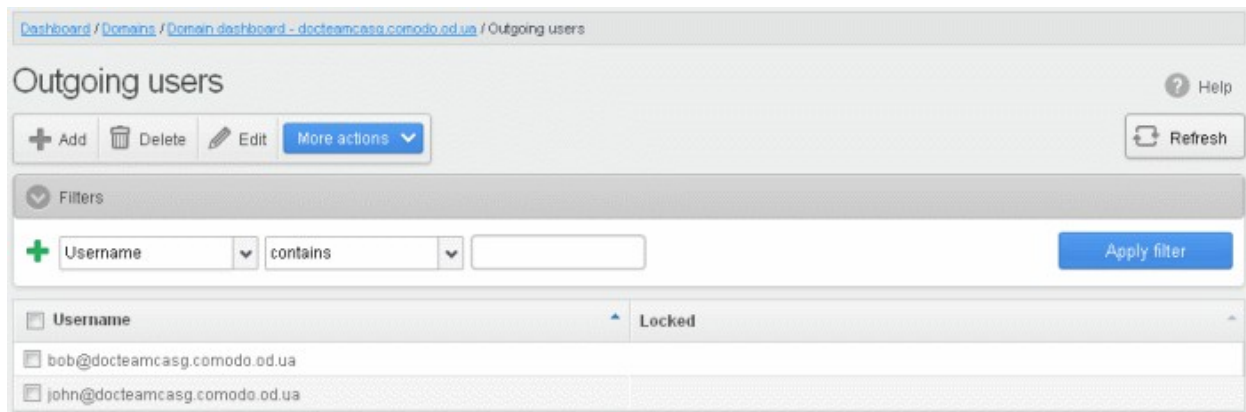


Sorting the Entries

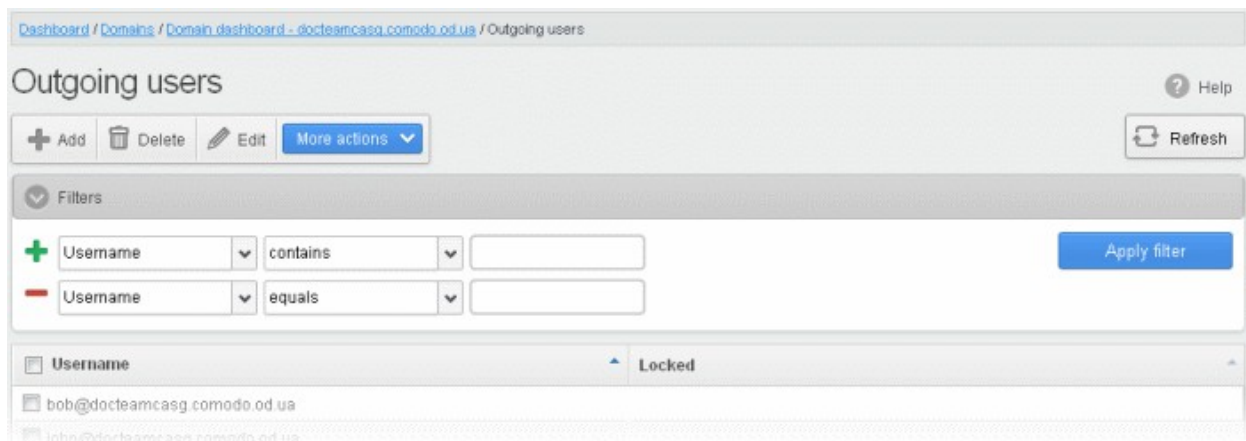
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search users

- Click anywhere on the Filters tab to open the filters area.



You can add more filters by clicking  for narrowing down your search.



You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

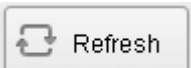
If 'Username' is selected, the following conditions are available:

- **Equals:** Displays all usernames that match the text entered in the text box.
- **Not Equals:** Displays all users except the one entered in the text box.
- **Contains:** Displays all username(s) that contain the words entered in the text box.
- **Not Contains:** Displays all username(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all usernames(s) that starts with the words entered in the text box.
- **Ends With:** Displays all usernames(s) that ends with the words entered in the text box.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.

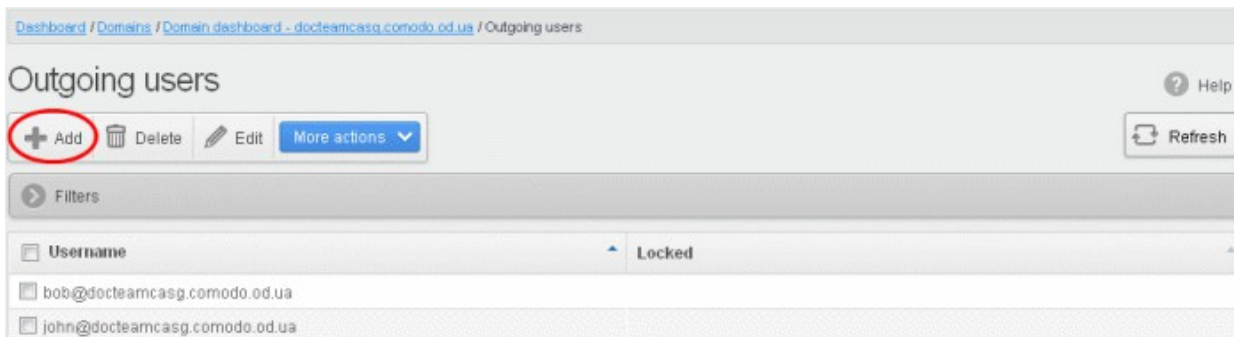
Click the  button to display all the outgoing users.

Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to

close the filters area and then click the 'Refresh' button.

To add a new user

- Click the 'Add' button.



The 'Add outgoing user' dialog will be displayed.

- Enter the username for the new outgoing user that will be first part of the email address. For example, testuser. The email address of the added user will be testuser@testdomain.com.
- Enter the password in the Password field. If the 'Password' field is left blank, then the 'Username' must be an IP address, and any connection from that IP will be considered authenticated without needing to use SMTP AUTH (Note: authorizing IP addresses may be disabled on the system).
- Click the 'Edit outgoing settings' button to configure outgoing settings for the user. The 'Add outgoing settings' dialog will expand:

Add outgoing user

Username:

Domain:

Password:

[Edit outgoing settings](#)

Block outgoing spam:

Automatic lock:

User lock timeout:

Maximum unlocks by timeout:

Enable outgoing limits:

Limit per hour:

Limit per minute:

Valid sender address required:

Maximum number of recipients per day:

Invalid recipient limit:

Maximum days to retry:

Quarantine response:

[Save](#) [Cancel](#)

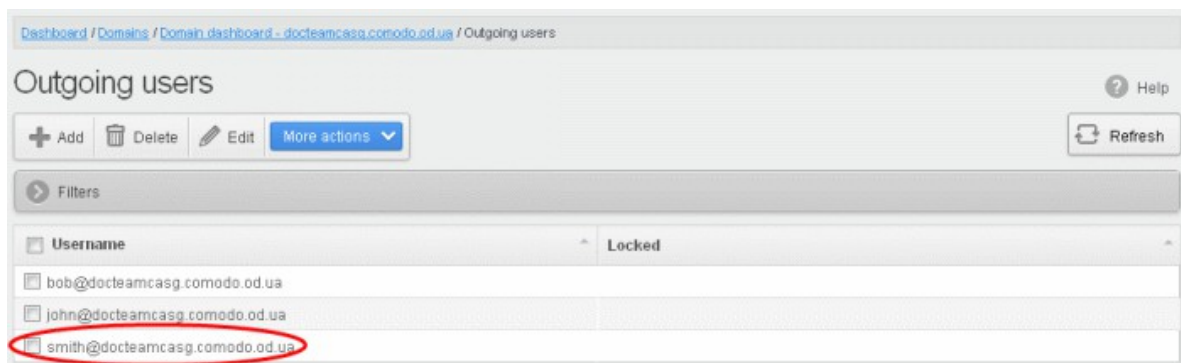
- **Block outgoing spam/Automatic lock**
 - **Block outgoing spam** - Blocks all outgoing spam mails from the user.
 - **Automatic lock** - If CASG detects spam or malicious mail from the user, it will automatically lock the user from sending mails for the period set in the 'User lock timeout' field.
- **User lock timeout** - The time in minutes the user will be locked out from sending mails after CASG detects outgoing spam or malicious mails from the user.
- **Maximum unlocks by timeout** - The number of times the locked out user will be unlocked for sending out mails. After reaching the maximum limit, the user will be locked out from sending any mails till it is unlocked by the administrator.
- **Enable outgoing limits** - Allows you to activate / deactivate limits on outgoing mails.
 - **Limit per hour** - The number of mails that can be sent per hour.
 - **Limit per minute** - The number of mails that can be sent per minute.
- **Valid sender address required** - If enabled, outgoing mails must have valid sender address.
- **Maximum number of recipients per day** - Maximum number of recipients that a user can send mails per day.
- **Invalid recipient limit** - The number of invalid recipients that a user can send mails to.
- **Maximum days to retry** - Maximum number of days CASG will retry to send queued outgoing mails after which they are bounced to the user.
- **Quarantine response** - Determines the response that CASG will send to the SMTP server that

delivered a message in the event that the mail is identified as spam.

Note - If you have enabled quarantine functionality, then spam/malicious mail will be quarantined (and not delivered to the recipient) regardless of your choice here. These options merely determine what message CASG will send back to the SMTP mail server.

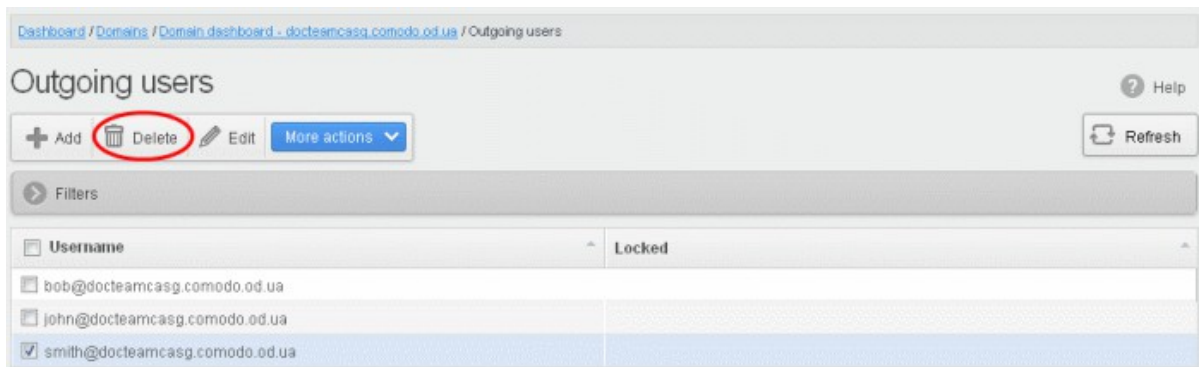
Options:

- **Rejected** - Will inform the SMTP server that the email wasn't delivered to recipient. (By default is 'Rejected'.)
- **Accepted** - The senders will not be notified if the outgoing mails are detected as spam. They will be blocked and not delivered to recipients.
- Click the 'Save' button.

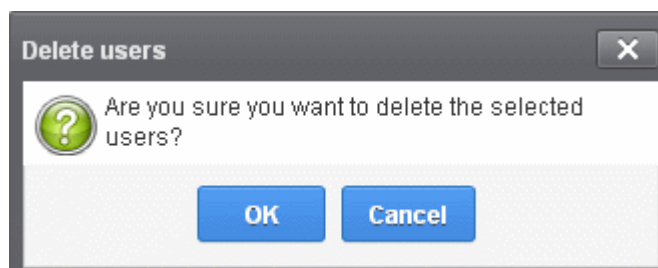


To delete an existing user

- Select the user you want to delete from the list and click the 'Delete' button.



Tip: You can select multiple users to delete by pressing and holding the Shift or Ctrl keys.

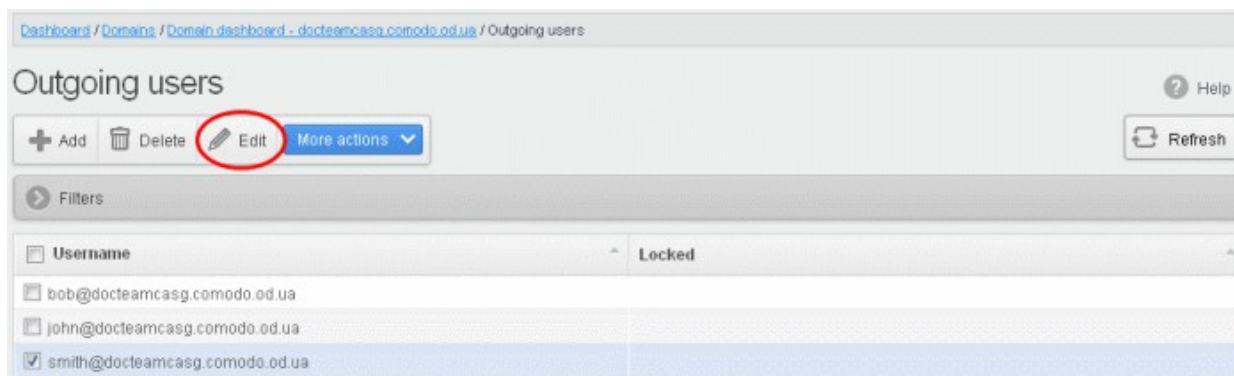


- Click 'OK' to confirm.

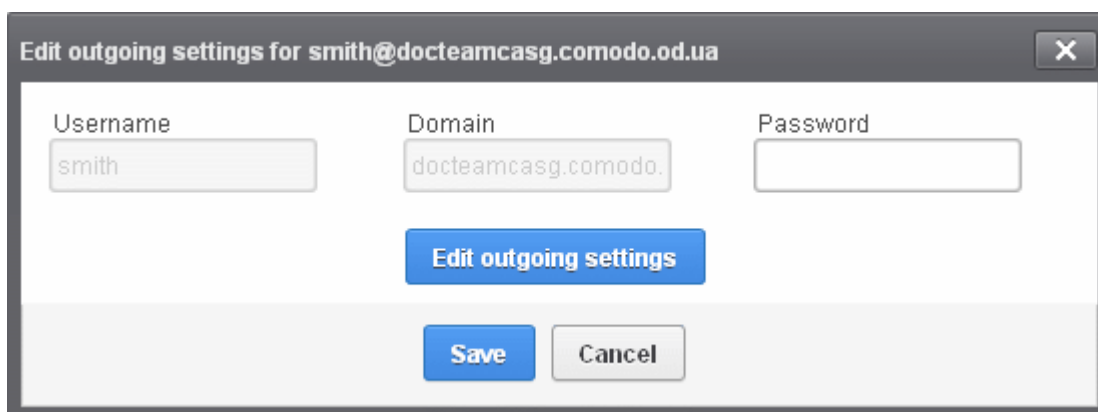
To edit an existing user

You can reset password, modify the outgoing settings configured from the **'Add outgoing user'** interface.

- Select the user that you want to edit from the list and click the 'Edit' button.



- Click the 'Edit outgoing settings' button.



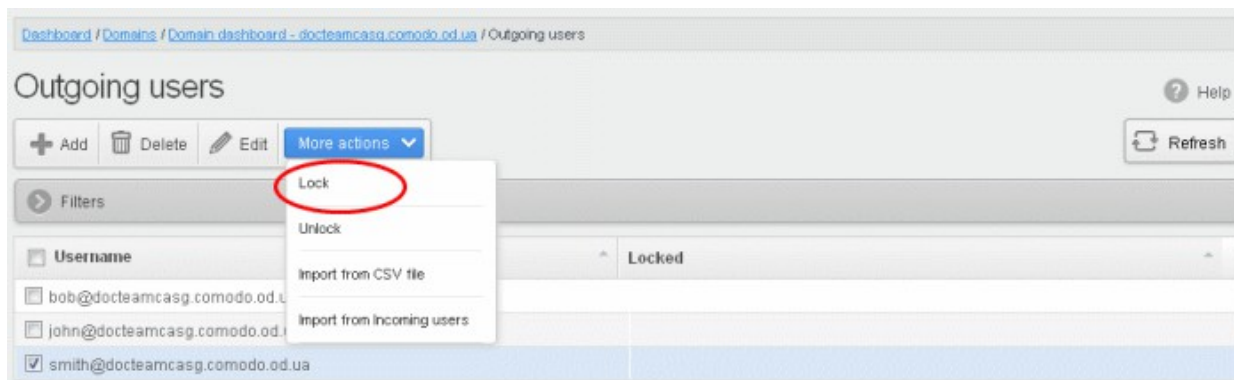
The 'Edit outgoing settings' will be displayed.

- Reset the password and / or make other changes as explained in the **'Add outgoing user'** section.
- Click the 'Save' button to confirm your changes.

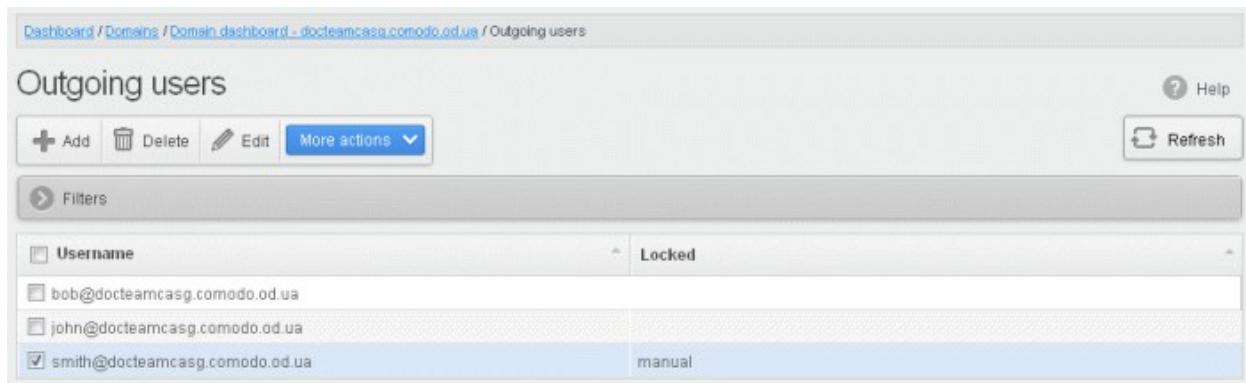
To manually lock outgoing user

Due to administrative or any other reason if you want to prevent a user from sending out mails, the Lock feature allows you to do so.

- Select the user that you want to lock, click 'More actions' and then click 'Lock'.



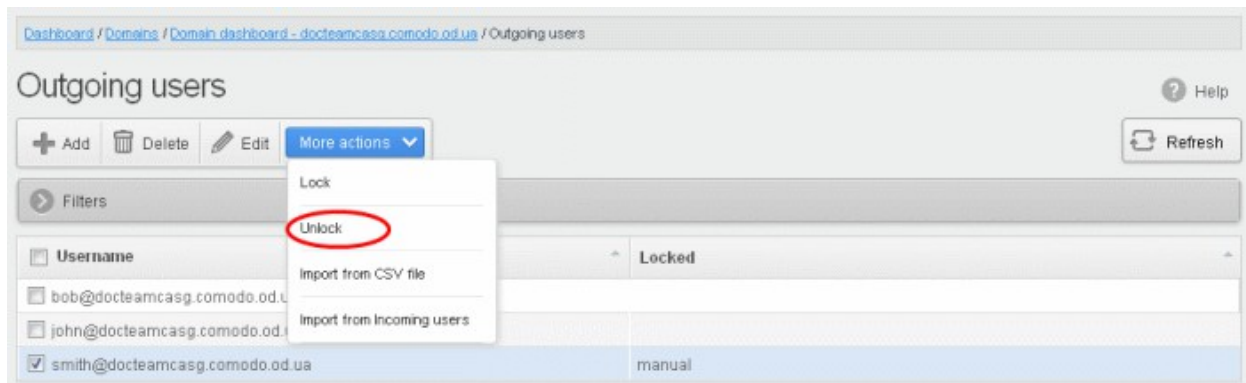
The selected user will be locked from sending mails.



To manually unlock outgoing user

A user who has been locked either manually or automatically (see [Edit outgoing settings](#)) can be unlocked from this interface.

- Select the user that you want to unlock, click 'More actions' and then click 'Unlock'.



The user will be unlocked and he/she can send mails.

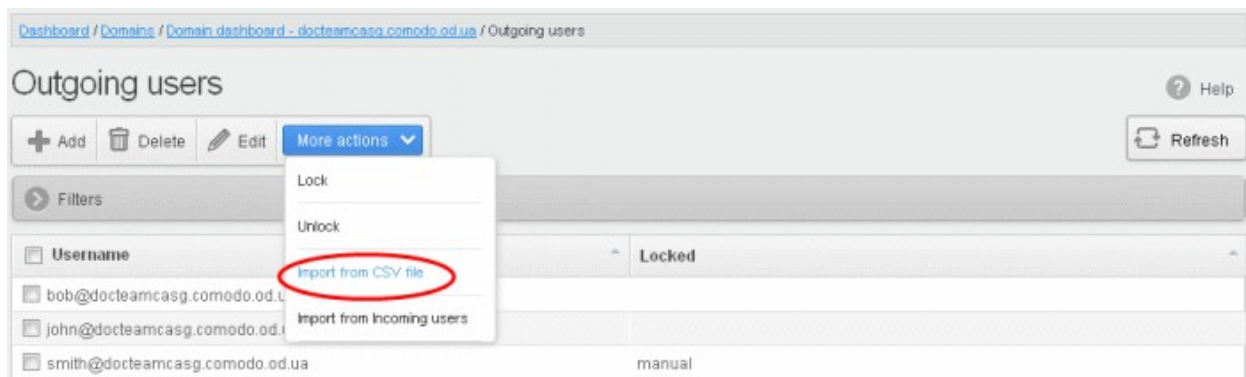
To import outgoing users from CSV file

Administrators can import many users from a file to the outgoing users list at a time. The users should be saved in the format shown below as an example:

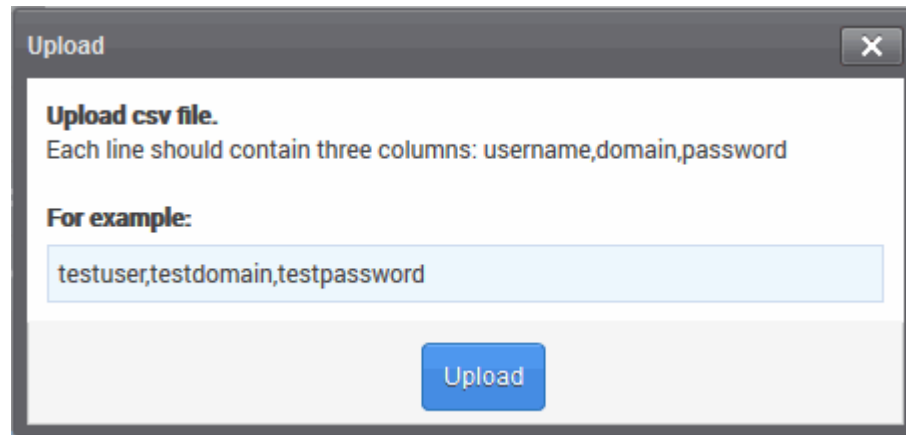
user1, domainname, password

user2, domainname, password

- To import outgoing users from a CSV file, click 'More actions' > 'Import from CSV file'

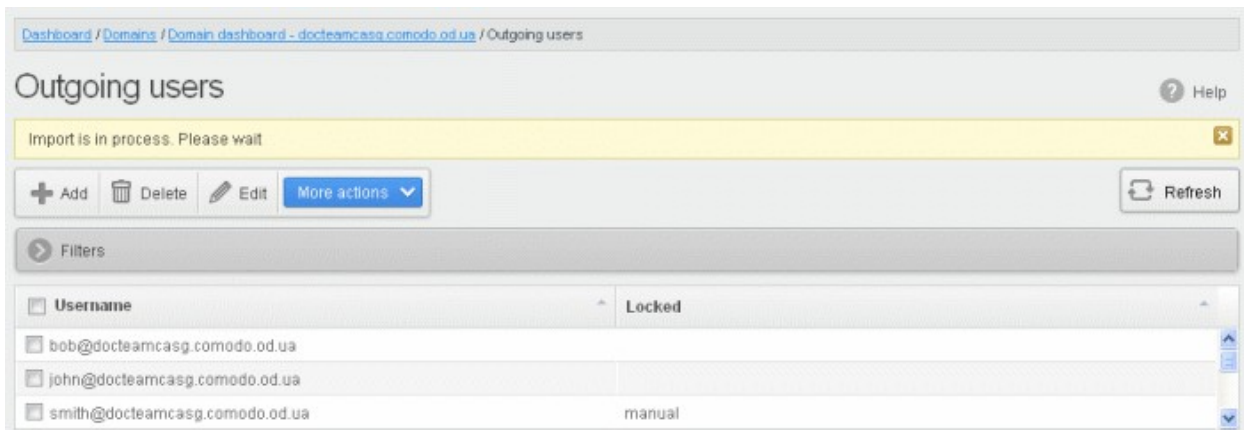


The Upload dialog will be displayed.

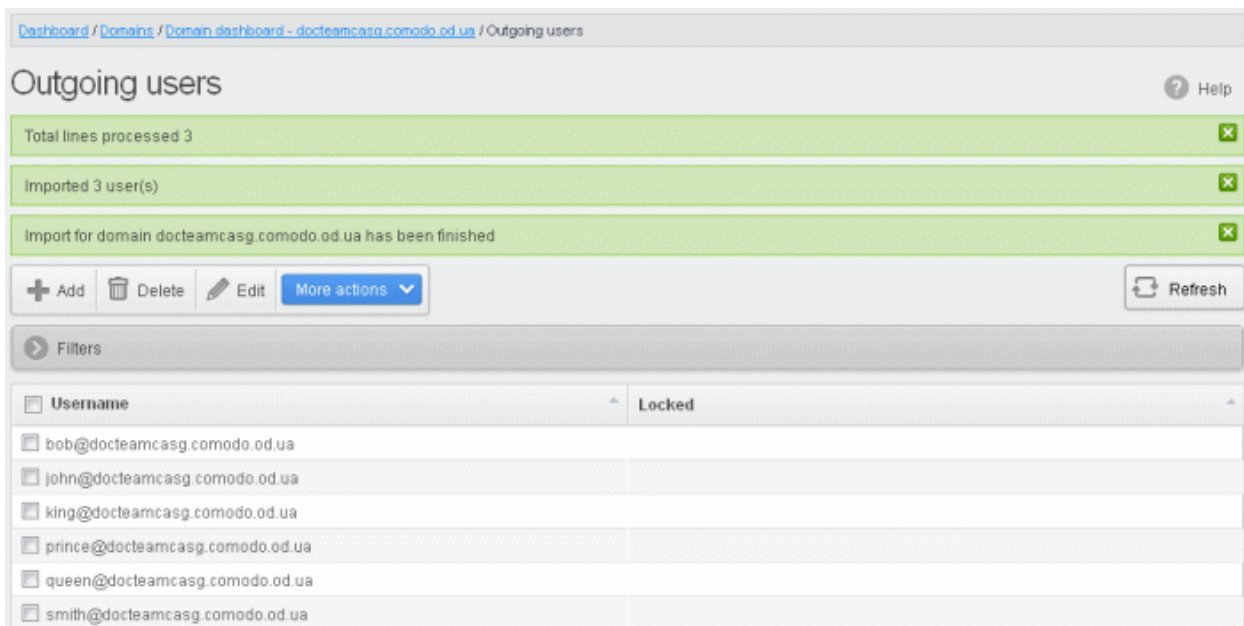


- Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button.

The upload progress will be displayed...



...and when completed, the results will be displayed.

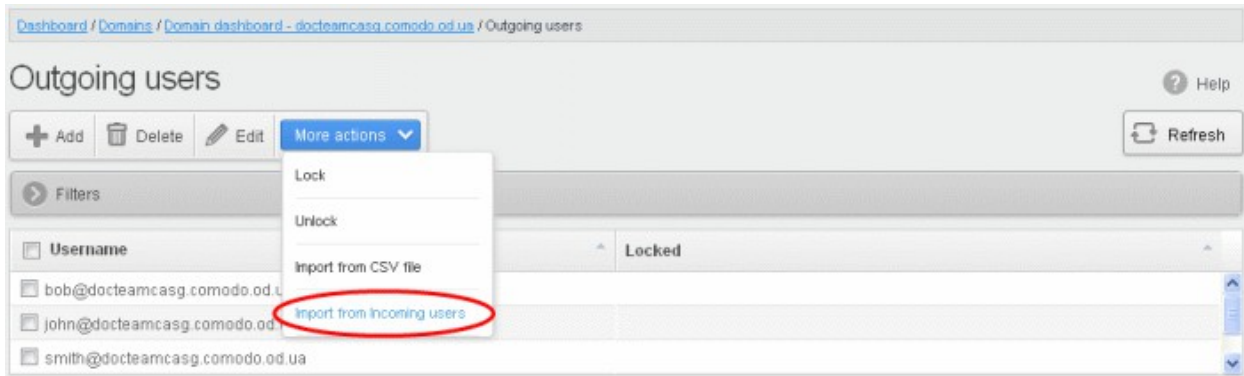


The administrator who carried out the task will receive a notification about the import task completion.

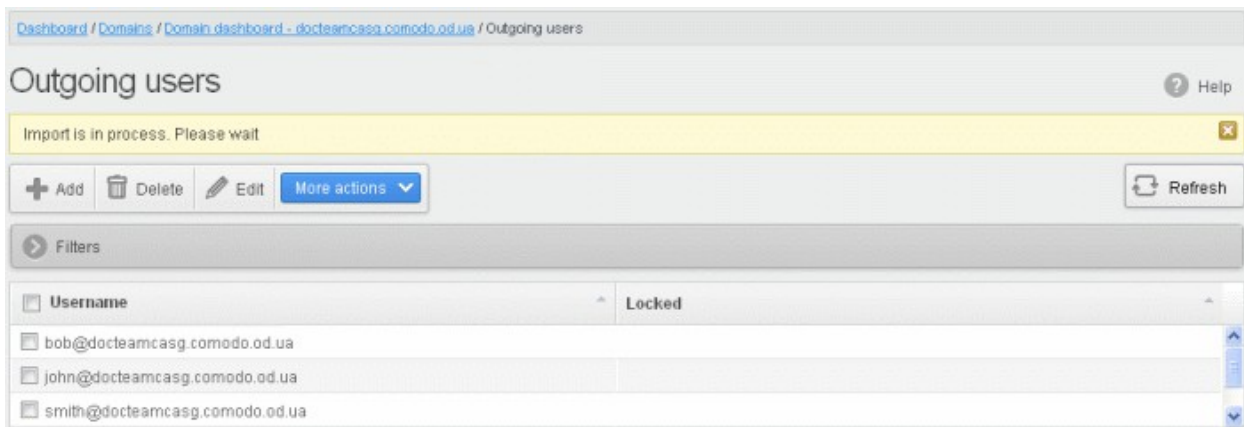
Import from incoming users

Administrators can add all incoming users to the outgoing users list by importing. If there is an outgoing user with the same name, the import of incoming user will be skipped.

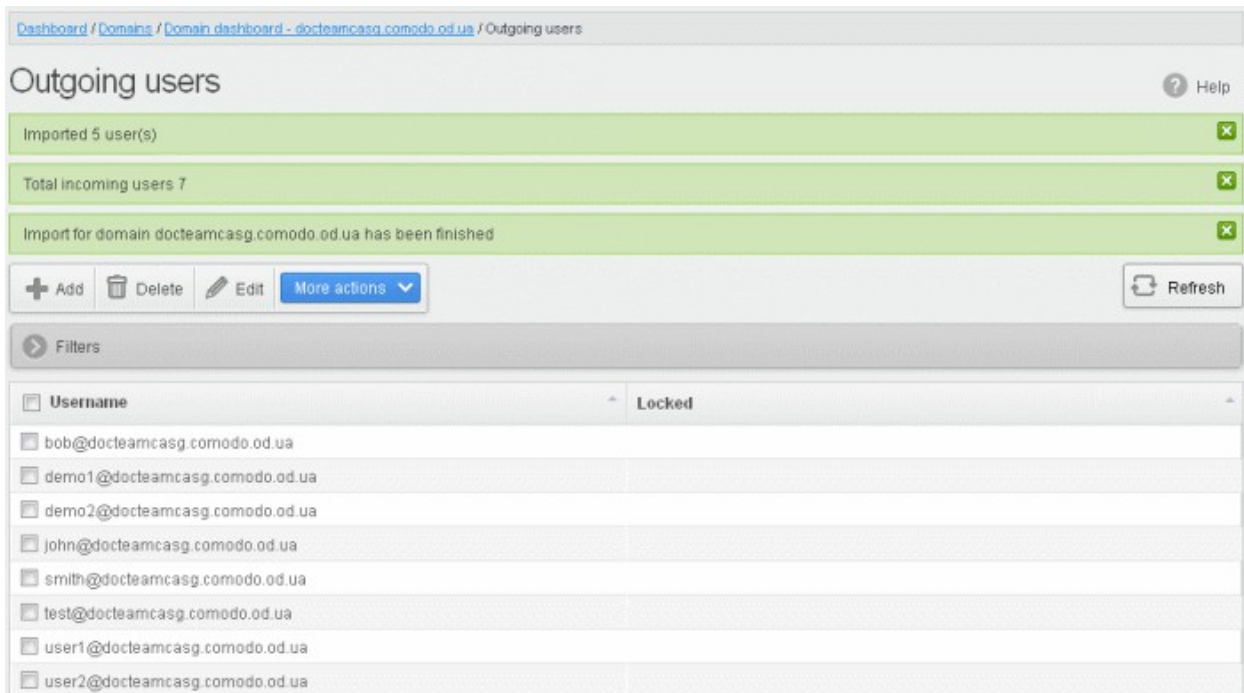
- To import outgoing users from incoming users, click 'More actions' > 'Import from Incoming users'



The upload progress will be displayed...



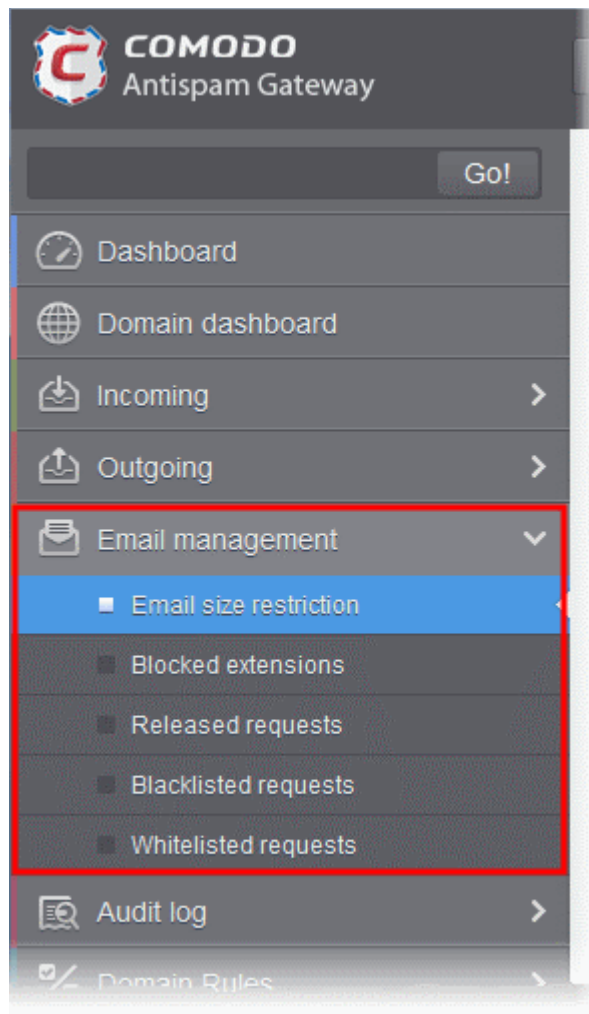
...and when completed, the results will be displayed.



The administrator who carried out the task will receive a notification about the import task completion.

3.2.1.1.4.4 Email Management

From this interface an administrator can configure the maximum size of each email and select the file types of attachments to be allowed. An administrator can also choose to release or reject requests from users for releasing quarantined emails, adding senders to blacklist and whitelist.



Click the following links for more details:

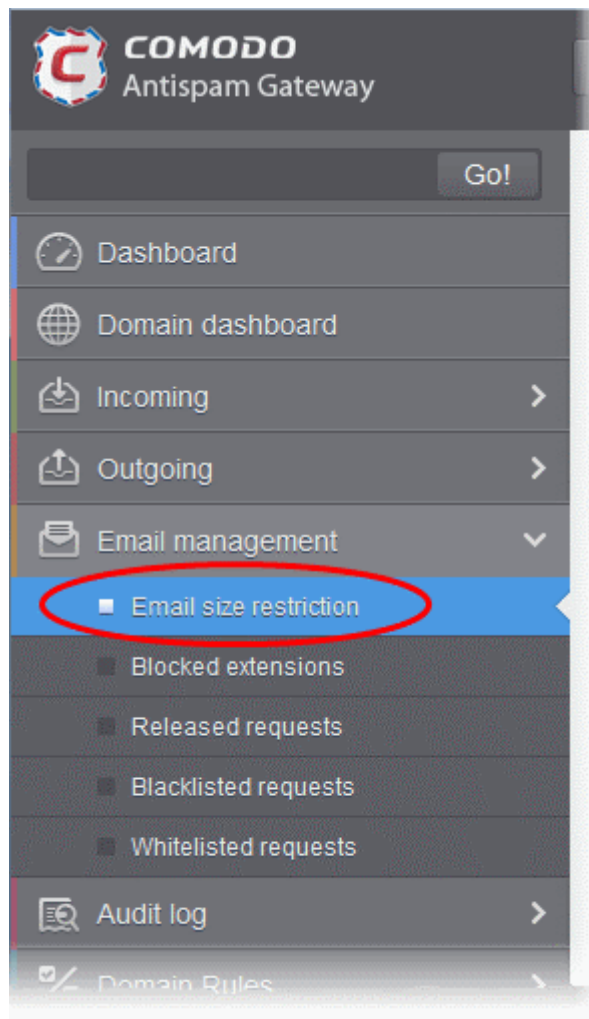
- [Email size restriction](#)
- [Blocked extensions](#)
- [Released requests](#)
- [Blacklisted requests](#)
- [Whitelisted requests](#)

Email Size Restriction

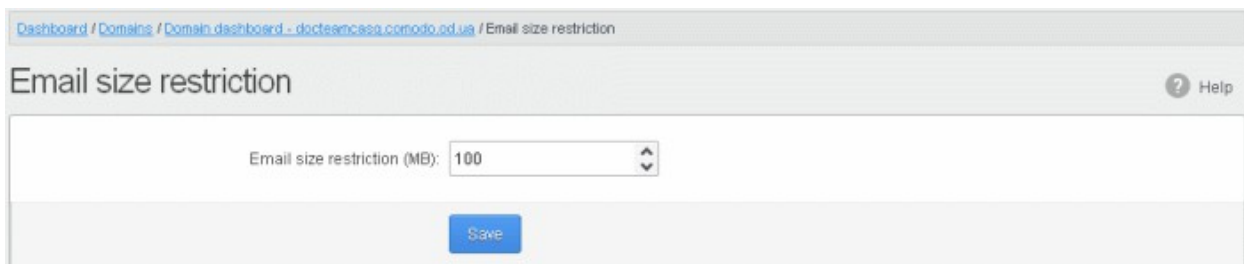
In order to avoid your domain storage space getting used up quickly due to large size of emails, CASG allows you to set the maximum size of each email that are allowed. Administrators have a choice of restricting email size of up to 250 MB. If you require to set the size of email more than 250 MB, please contact your account manager at Comodo or please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready.

To set email size restriction

- Click the 'Email management' tab on the left hand side navigation to expand and then click the 'Email size restriction' sub tab.



The 'Email restrictions' interface of the selected domain will be displayed:



- Enter the maximum allowed size (up to 250 MB) of each email that you want to set in the 'Email size restriction' field.

If you enter a value more than 250 MB, an alert will be displayed to contact your account manager at Comodo and the email size will be automatically set as 250 MB.

Dashboard / Domains / Domain dashboard - docteamcasa.comodo.od.ua / Email size restriction

Email size restriction Help

Incorrect capacity value. Value must be between 1 and 250. If you require more than 250Mb please call us. ✕

Email size restriction (MB):

- If you want to set the size above 250 MB, please open a ticket at support.comodo.com or call 1.888.COMODO (2666.6361) and have your account number ready.
- Click 'Save' to confirm your changes.

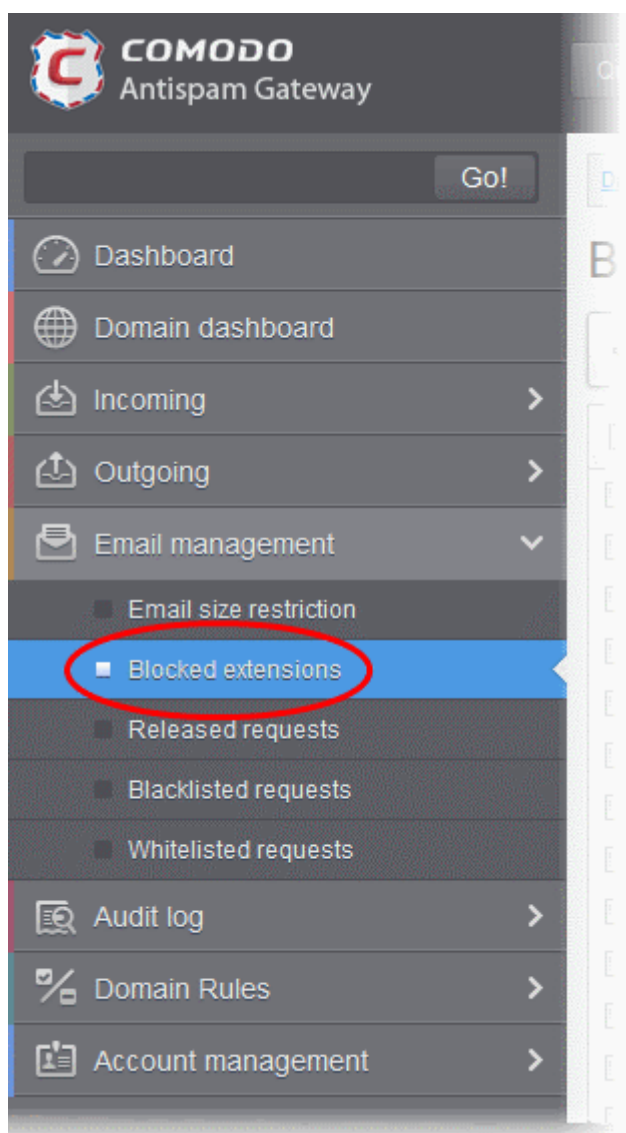
Note: Incoming and outgoing emails with size more than the value set here will be rejected.

Blocked Extensions

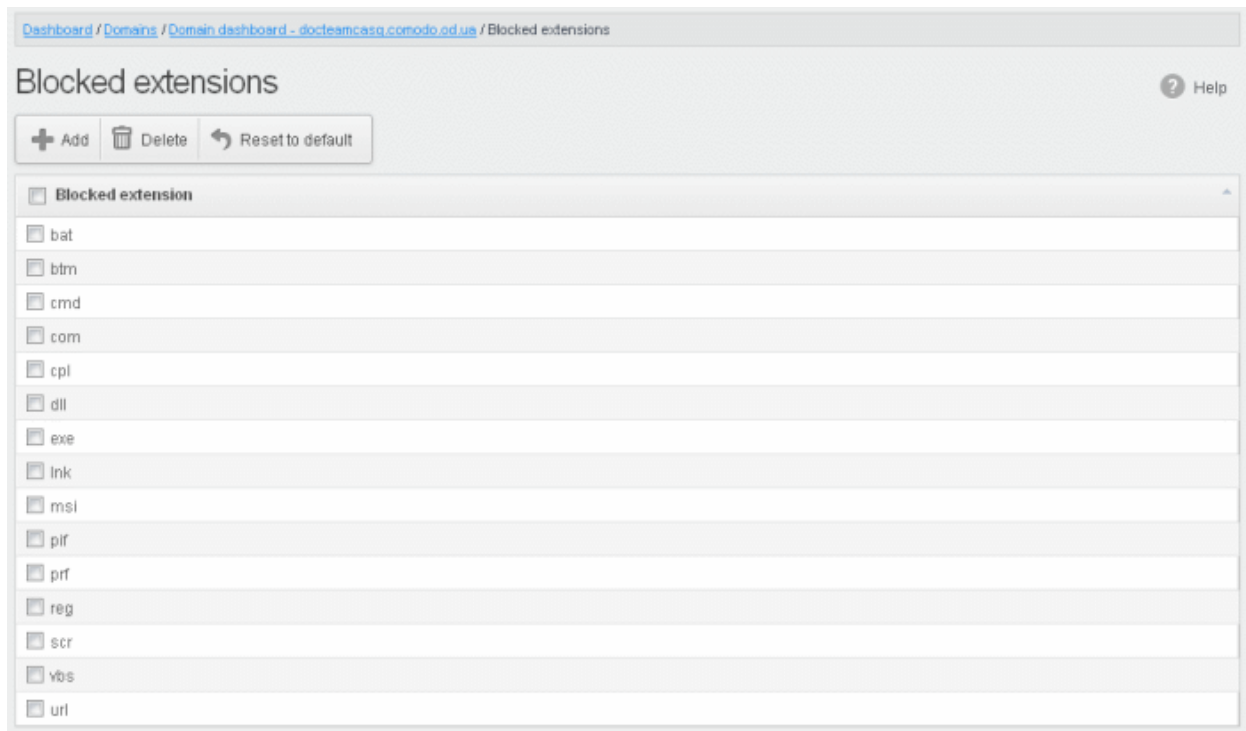
CASG allows you automatically block email attachments with certain file extensions. For example, an attachment with .exe extension may contain malicious code which could infect a recipient's computer. [Click here](#) to see a complete list of extensions you can block.

To add file extensions to be blocked

- Click the 'Email management' tab on the left hand side navigation to expand and then click the 'Blocked extensions' sub tab.



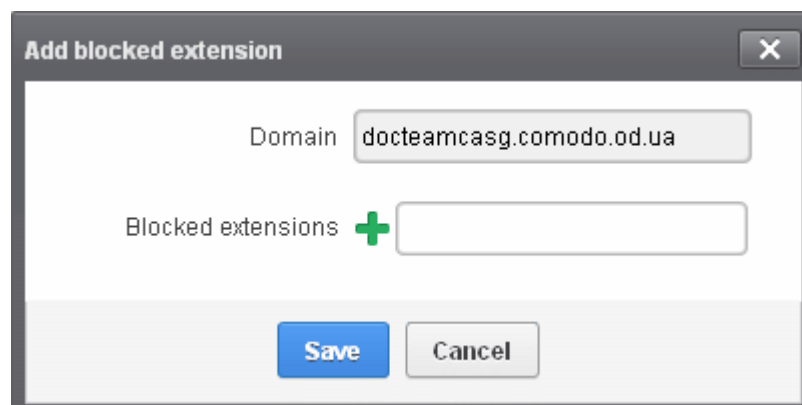
The 'Blocked extensions' interface of the selected domain will be displayed:




The list of default blocked extensions is displayed. You can sort the blocked extensions list alphabetically in ascending or descending order by clicking the 'Blocked extensions' title bar.

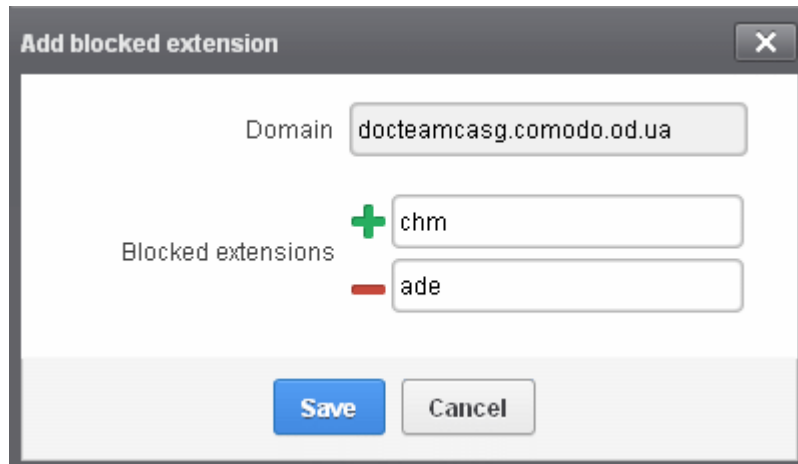
- Click the 'Add' button to include another blocked extension

The 'Add blocked extension' will be displayed.



- Enter the extension name to be blocked in the text box

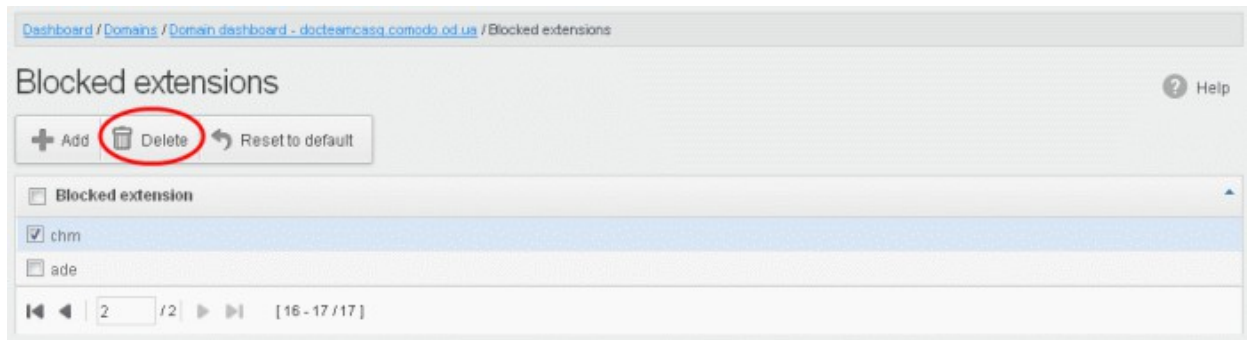
You can add many extensions at a time by clicking the  icon.



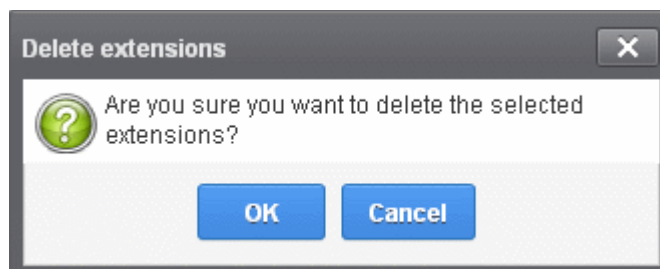
- Click the 'Save' button

The entered extensions will be added to the list.

- To delete an extension, select it from the list and click the 'Delete' button



An alert will be displayed to confirm to delete the selected extensions.



The selected blocked extension will be deleted from the list and email attachment with this file extension will be allowed provided it passes the size restriction filter.

Click the 'Reset to default' button to restore default blocked extensions in CASG.

List of blocked Extensions

ade	csb	lib	msh	psc1	vbe
adp	dll	lnk	msh1	psc2	vbs
air	exe	mad	msh1xml	pst	vbscript
app	gadget	maf	msh2xml	reg	vsm
as	hlp	mag	mshxml	rgs	vsmacros
asf	hta	mam	msi	scf	vss
asp	html	maq	mst	scr	vst
asx	htr	mar	mst	script	vsw
bas	iim	mas	nexe	sct	vxd
bat	inf	mat	nws	sh	widget
bin	ins	mau	ocx	shb	wmd
btm	inx	mav	ops	shs	wmf
cab	isp	maw	otm	swf	wms
cer	isu	mda	paf	sys	wmz
chm	its	mdb	pcd	tmp	ws
cil	jar	mde	pif	u3p	wsc
cmd	job	mdt	prf	udf	wsf
com	js	mdw	prg	upx	wsh
cpl	jse	mdz	ps1	url	xap
crt	ksh	msc	ps1xml	vb	xml

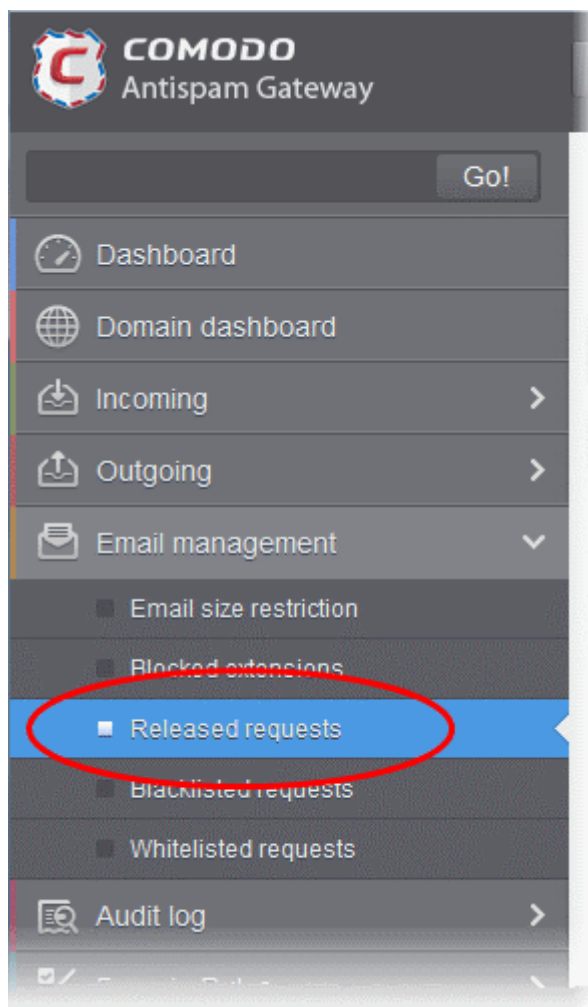
Released Requests

An administrator can choose to release or reject requests from users for releasing quarantined emails from their accounts. The release requests from users will be notified to all admins for that account via emails and will also be displayed in the interface. The users who requested for release of quarantined emails will also receive email notifications.

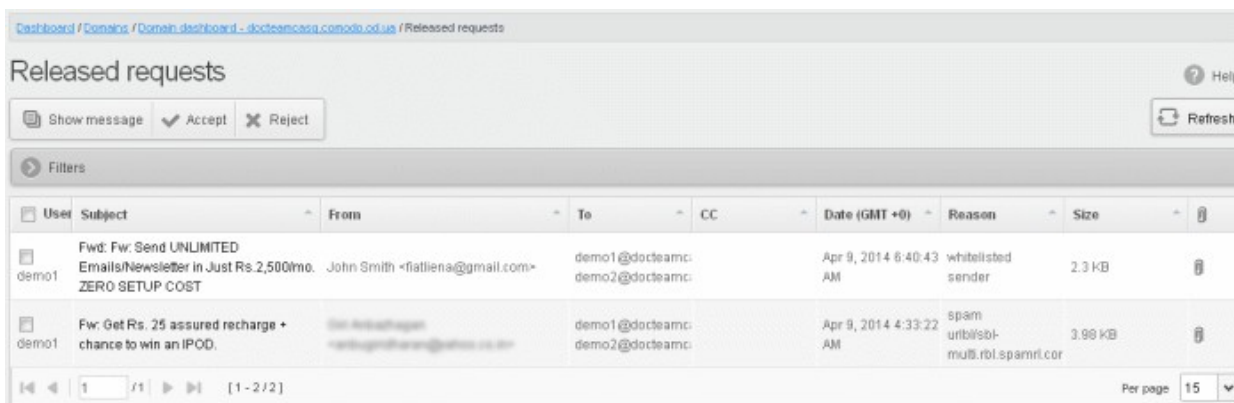
Note: User who have been assigned as 'Power User' can release quarantined mails without approval from the administrators. See the section '**Groups & Permissions**' and '**Managing Permissions**' for more details.

To open the released requests interface

- Click the 'Email management' tab on the left hand side navigation to expand and then click the 'Released requests' sub tab.



The 'Release requests' interface will be displayed:



The list of emails that users requested to release will be displayed. The list contains nine columns providing information about the requested user, subject, the sender, details of the recipients, details of recipients in CC list, the date they were sent, the reason they were quarantined and the size of the email. The last column indicates whether there is any attachment in the mails.

Sorting the Entries

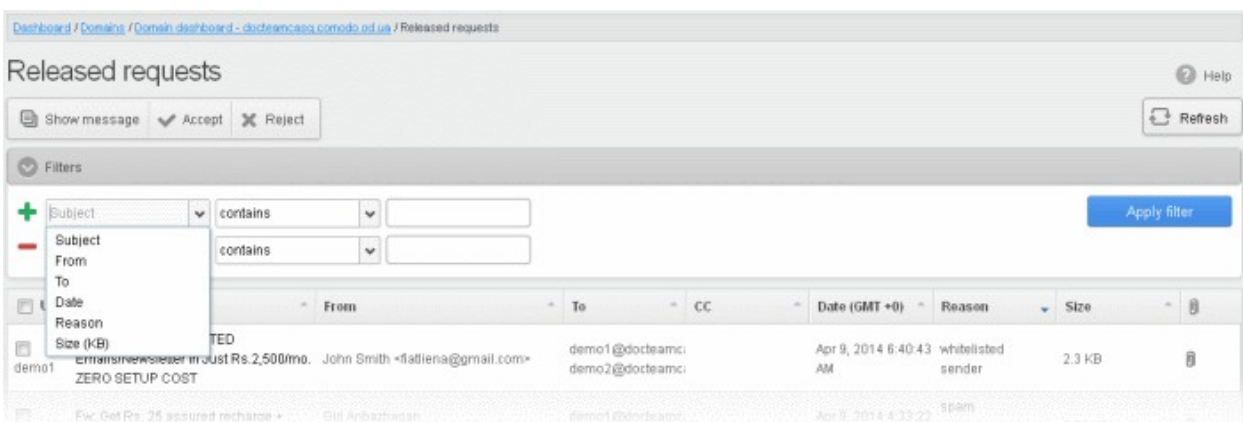
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search released requests

Click anywhere on the Filters tab to open the filters area.



You can add more filters by clicking  for narrowing down your search.



You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Subject::** Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From:** Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To:** Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason:** Will execute a search of words in the reason column according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Equals:** Displays all quarantined mails that contain only the words entered in the text box
- **Not Equals:** Displays all quarantined mails that do not contain only the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box
- **Starts with:** Displays all quarantined emails that starts with the words entered in the text box
- **Ends with:** Displays all quarantined emails that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.

- **Size:** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions are available:


- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

If 'Size' is selected, the following conditions are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box
- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all the release requested emails.

Note: To display all the release requested emails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing Details of Release Requested Mails

The details such as user, subject, sender, recipient, date, reason and size of the mails requested for release can be viewed in two ways:

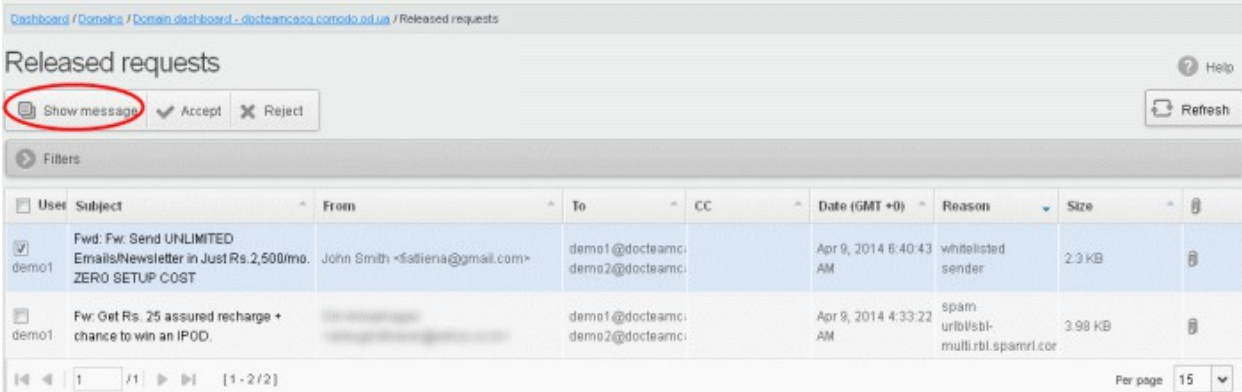
- **In the same CASG window**
- **In a new CASG window**

To view details of release requested mails in the same CASG window:

- In the released requests area, 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.

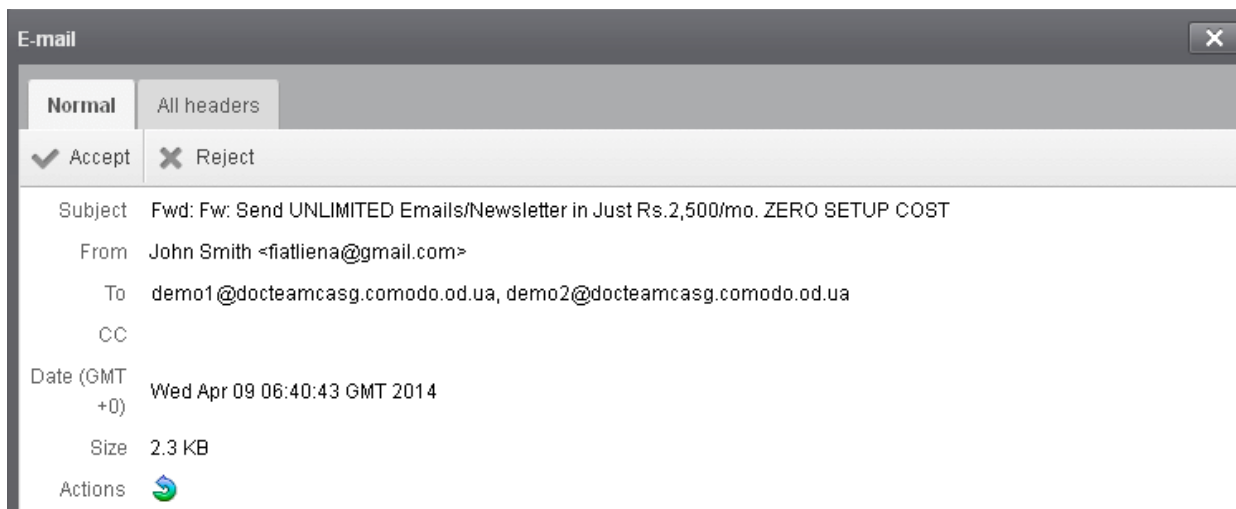


The screenshot shows the 'Released requests' section of the Comodo Antispam Gateway. At the top, there are buttons for 'Show message' (circled in red), 'Accept', and 'Reject'. A 'Refresh' button is also visible. Below these buttons is a 'Filters' section. The main part of the screenshot is a table with the following columns: User, Subject, From, To, CC, Date (GMT +0), Reason, Size, and an icon column. Two rows of email data are visible:

User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	Icon
demo1	Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs.2,500/mo. ZERO SETUP COST	John Smith <fatiana@gmail.com>	demo1@docteamc; demo2@docteamc;		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	
demo1	Fw: Get Rs. 25 assured recharge + chance to win an IPOD.		demo1@docteamc; demo2@docteamc;		Apr 9, 2014 4:33:22 AM	spam urlib/sbi-multi.rtl.spamrl.cor	3.98 KB	

At the bottom of the table, there are navigation controls including a page number '1' and a 'Per page' dropdown set to '15'.

The details of the selected email will be displayed.

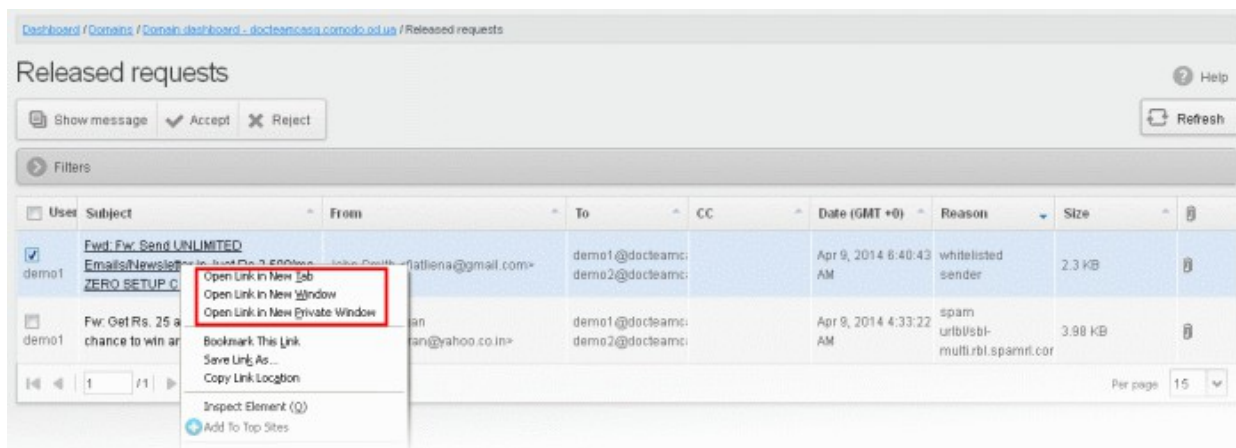


To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient, click 'All headers' tab. The headers give full details of the sender, route, recipient, sent date, mail type and so on and enable you to check the authenticity of the mail.

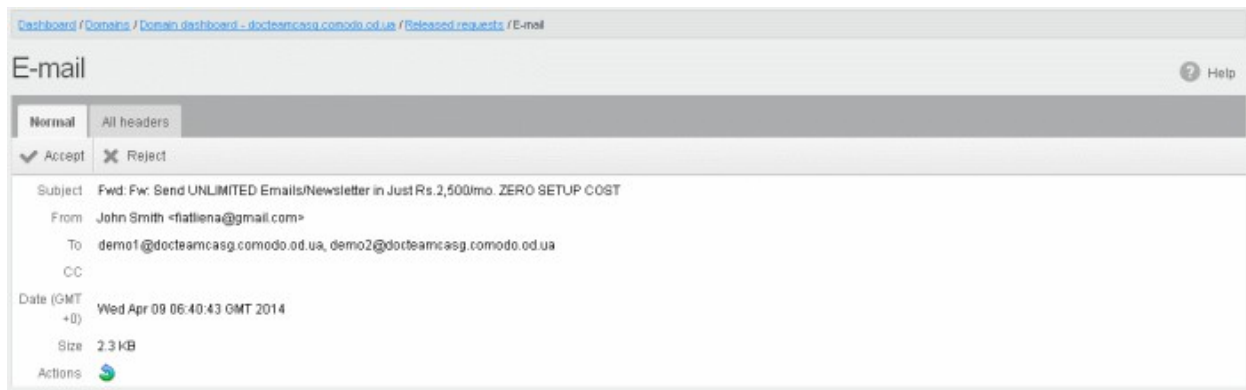
Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it. If the mail is accepted, it will be released to the user's inbox. If it is rejected, the email will be no longer in the released emails list. Please note that emails will continue to remain in the **Quarantined** list irrespective of the action taken.

To view details of release requested mails in a new CASG window:

- In the released requests area, select the mail that you want to view, right-click on the email link in the subject column and select to open in a new tab or new window.



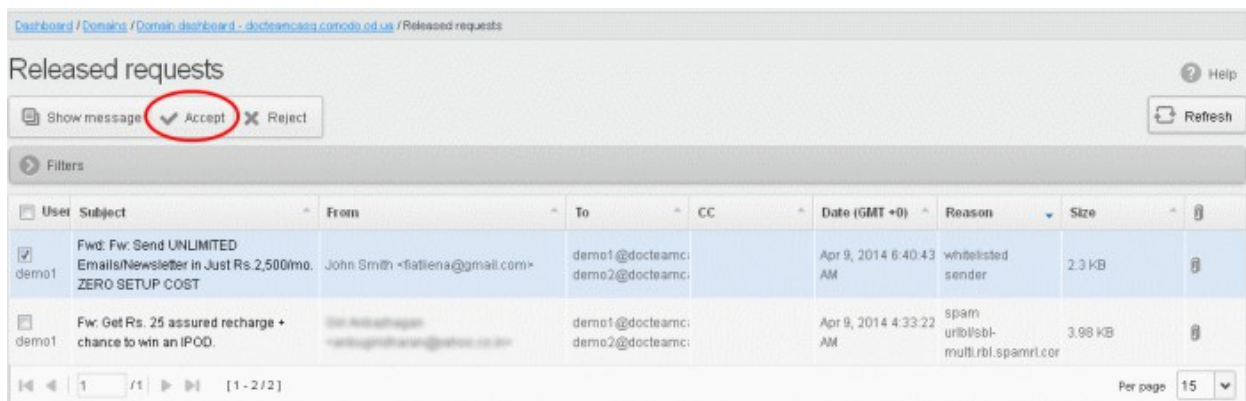
The details of the selected mail will be displayed in a new CASG window.



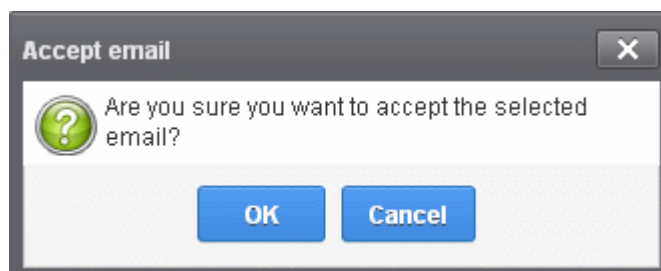
To accept the release request from users

After viewing the details and ensuring that the selected email is not a spam you can choose to release the mail to the recipient.

- Select the mail that you want to release and click the 'Accept' button.



An alert will be displayed to confirm the release of selected email to the requested user.



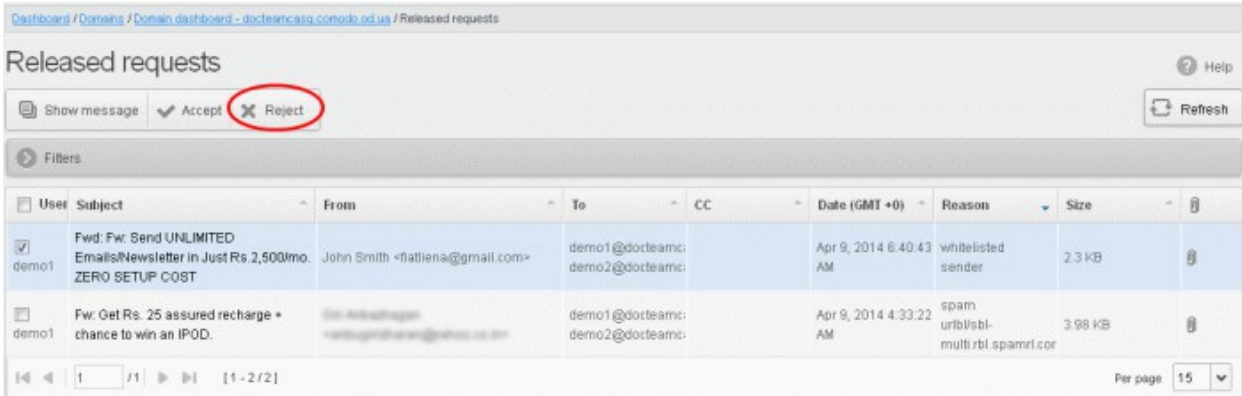
- Click 'OK' to confirm the release.

The email will be released to the user and the mail will no longer be in the released mail list. However, it will continue to remain in the **Quarantined** list.

To reject the release request from users

After viewing the details of the email and if not satisfied with its authenticity you can choose to reject the request from the user.

- Select the mail that you want to reject and click the 'Reject' button.



Released requests

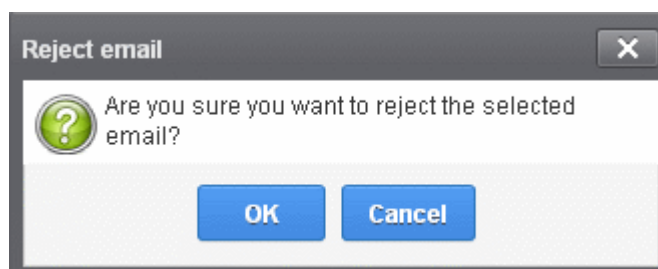
Show message Accept **Reject** Refresh

Filters

User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	
<input checked="" type="checkbox"/> demo1	Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs.2,500/mo. ZERO SETUP COST	John Smith <flatienna@gmail.com>	demo1@docteamc: demo2@docteamc:		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	
<input type="checkbox"/> demo1	Fw: Get Rs. 25 assured recharge + chance to win an IPOD.	...	demo1@docteamc: demo2@docteamc:		Apr 9, 2014 4:33:22 AM	spam urltblsbl- multitbl.spamr1.cor	3.98 KB	

Per page 15

An alert will be displayed to confirm the rejection of selected email.



- Click 'OK' to confirm the rejection.

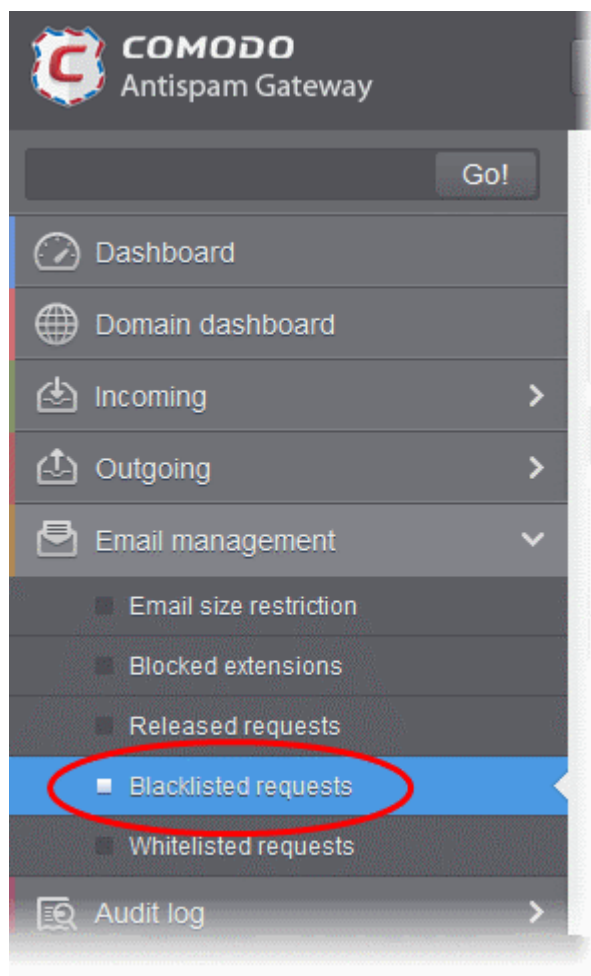
The email will not be released to the user and the mail will no longer be in the released mail list. However, it will continue to remain in the **Quarantined** list.

Blacklisted Requests

CASG allow users to send requests to their email account administrators to add senders to blacklist. Administrators in addition to receiving emails for these requests also can view the list of such requests in 'Blacklisted requests' section of the administrator interface under 'Email management' section. The senders added to balcklist on users' request will be applicable for the requested users only. Mails from these blacklisted senders to the requested users will be rejected by CASG even though these blacklisted senders may be in general sender whitelist. Refer to the sections **Sender Whitelist** and **Blacklist Senders Per User** for more details.

To open the blacklisted requests interface

- Click the 'Email management' tab on the left hand side navigation to expand and then click the 'Blacklisted requests' sub tab.



The 'Blacklisted requests' interface will be displayed:

Dashboard / Domains / Domain dashboard - docteamcaso.comodo.od.ua / Blacklisted requests

Blacklisted requests Help

Show message Accept Reject Refresh

Filters

<input type="checkbox"/>	User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs.2,500/mo. ZERO SETUP COST	John Smith <fatiens@gmail.com>	demo1@docteamc;	demo2@docteamc;	Apr 9, 2014 8:40:43 AM	whitelisted sender	2.3 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: Get Rs. 25 assured recharge + chance to win an IPOD.	www.spamrbl.com	demo1@docteamc;	demo2@docteamc;	Apr 9, 2014 4:33:22 AM	spam urlbl/bsi-multi.rbl.spamrbl.com	3.98 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: Register and Get Rs. 5000 to Shop Now! Introducing Pepperfry.com - India's L...	www.spamrbl.com	demo1@docteamc;	demo2@docteamc;	Apr 9, 2014 4:32:36 AM	spam urlbl/uri.rbl.spamrbl.com	3.05 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	Fw: We have free samples for you, now try before you buy @ your doorsteps!	www.spamrbl.com	demo1@docteamc;	demo2@docteamc;	Apr 7, 2014 8:52:31 AM	spam urlbl/uri.rbl.spamrbl.com	3.02 KB	<input type="checkbox"/>
<input type="checkbox"/>	demo1	test spam email 1	www.spamrbl.com	demo1@docteamc;		Apr 2, 2014 2:26:40 PM	spam External pattern match (Sanesecurity.Junk.	8.16 KB	<input type="checkbox"/>

1 / 1 [1 - 5 / 5] Per page 15

The list of emails that users requested for adding the senders to blacklist will be displayed. The list contains nine columns providing information about the requested user, subject, the sender, details of the recipients, details of recipients in CC list, the date they were sent, the reason they were quarantined and the size of the email. The last column indicates whether there is any attachment in the mails.

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the

entries as per the information displayed in the respective column.

Using Filter option to search blacklisted requests

Click anywhere on the Filters tab to open the filters area.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.cd.us / Blacklisted requests

Blacklisted requests

Show message Accept Reject Refresh

Filters

+ Subject contains [] Apply filter

User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	
demo1	Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs 2,500/mo.	John Smith <fatiana@gmail.com>	demo1@docteamc- demo2@docteamc-		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	

You can add more filters by clicking  for narrowing down your search.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.cd.us / Blacklisted requests

Blacklisted requests

Show message Accept Reject Refresh

Filters

+ Subject contains [] Apply filter

- Subject
- From
- To
- Date
- Reason
- Size (KB)

User	Subject	From	To	CC	Date (GMT +0)	Reason	Size	
demo1	Fwd: Fw: Send UNLIMITED Emails/Newsletter in Just Rs 2,500/mo.	John Smith <fatiana@gmail.com>	demo1@docteamc- demo2@docteamc-		Apr 9, 2014 6:40:43 AM	whitelisted sender	2.3 KB	
						spam		

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Subject::** Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From:** Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To:** Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason:** Will execute a search of words in the reason column according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Equals:** Displays all quarantined mails that contain only the words entered in the text box
- **Not Equals:** Displays all quarantined mails that do not contain only the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box
- **Starts with:** Displays all quarantined emails that starts with the words entered in the text box
- **Ends with:** Displays all quarantined emails that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size:** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions are available:


- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar

If 'Size' is selected, the following conditions are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box
- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all the blacklisted requests emails.

Note: To display all the blacklisted requests mails after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

Viewing Details of Blacklisted Requests

The details such as user, subject, sender, recipient, date, reason and size of the mails requested for blacklisting can be viewed in two ways:

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

To view details of blacklisted requests in the same CASG window:

- In the blacklisted requests area, 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.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests

Blacklisted requests

[Show message](#) [Accept](#) [Reject](#) [Refresh](#)

Filters

<input checked="" type="checkbox"/>	Subject	From	To	CC	Date (GMT)	Reason	Size	
<input checked="" type="checkbox"/>	Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry	Junk <junkemail@yahoo.co.in>	bob@doctea bob@democ john@docte		2016-04-20 11:02:07	spam Combined (0.15)	13.31 KB	

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

The details of the selected email will be displayed.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests / E-mail

E-mail

[Normal](#) [All headers](#)

[Accept](#) [Reject](#)

Subject: Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry

From: Junk <junkemail@yahoo.co.in>

To: bob@docteamcasg.comodo.od.ua, bob@democasg.comodo.od.ua, john@docteamcasg.comodo.od.ua, john@democasg.comodo.od.ua, dyanorat481@gmail.com, robin@democasg.comodo.od.ua, avantistude@gmail.com

CC:

Date (GMT +00:00): 2016-04-20 11:02:07

Size: 13.31 KB

Actions

[Plain text](#) [Html source](#) [Original View](#)

On Sunday, 10 April 2016 11:25 AM, Netmeds Healthcare <support@youmnt.com> wrote:

If you're having trouble viewing this email, please click here. @media screen and (min-width:320p

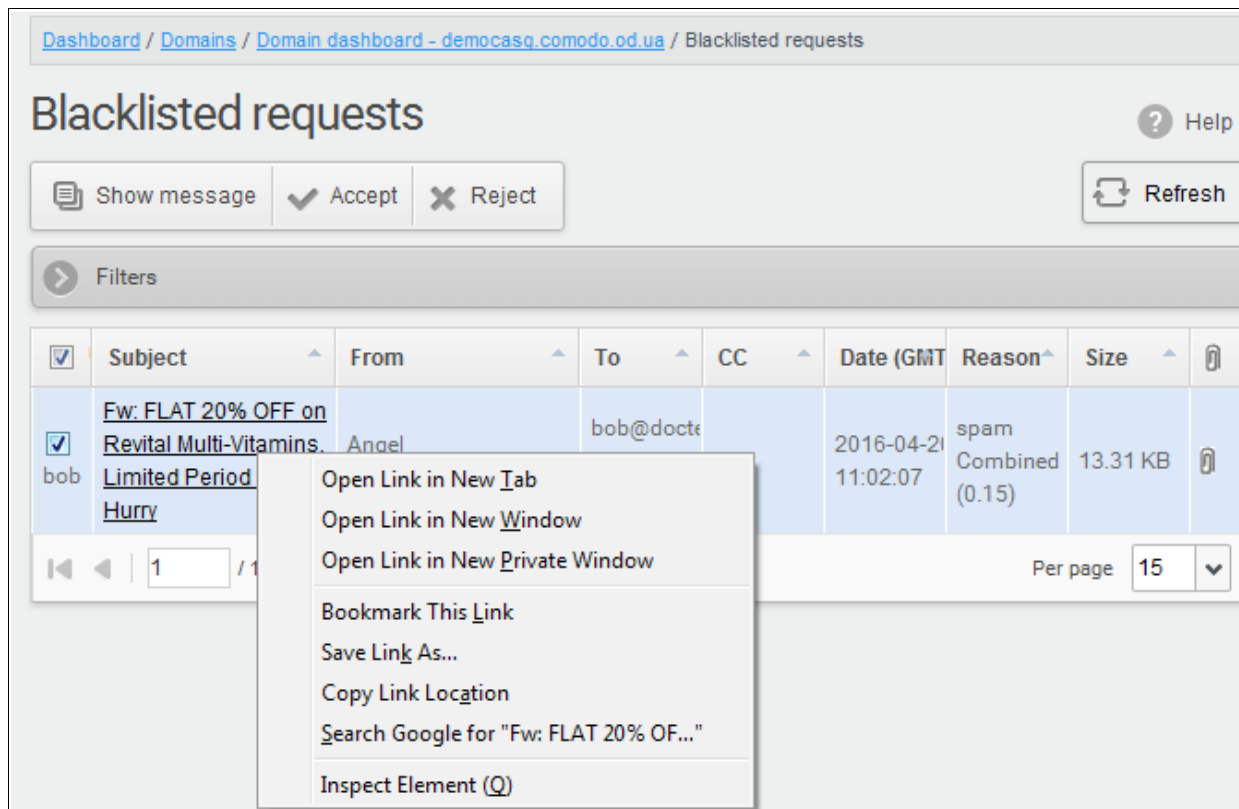
1800 103 0304

To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient, click 'All headers' tab. 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.

Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it for blacklisting the sender. If the request is accepted, the sender will be added to '**Blacklist Senders Per User**'. If it is rejected, the email will be no longer in the blacklisted requests emails list. Please note that emails will continue to remain in the **Quarantined** list irrespective of the action taken.

To view details of blacklisted requests in a new CASG window:

- In the blacklisted requests area, select the mail that you want to view and click the 'Show message in new window' button or right-click and select to open in a new tab or new window.



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

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests / E-mail

E-mail

? Help

Normal All headers

✓ Accept ✗ Reject

Subject Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry

From Junk <junkemail@yahoo.co.in>

To bob@docteamcasg.comodo.od.ua, bob@democasg.comodo.od.ua, john@docteamcasg.comodo.od.ua, john@democasg.comodo.od.ua, dyanorat481@gmail.com, robin@democasg.comodo.od.ua, avantistude@gmail.com

CC

Date (GMT +00:00) 2016-04-20 11:02:07

Size 13.31 KB

Actions

Plain text Html source Original View

On Sunday, 10 April 2016 11:25 AM, Netmeds Healthcare <support@youmnt.com> wrote:

If you're having trouble viewing this email, please click here.@media screen and (min-width:320p

- 1800 103 0304

To accept the blacklist request from users

After viewing the details, you can choose to accept the request from user to add the sender to **blacklist senders per user** list.

- Select the mail that you want to add the sender to blacklist and click the 'Accept' button.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Blacklisted requests

Blacklisted requests

? Help

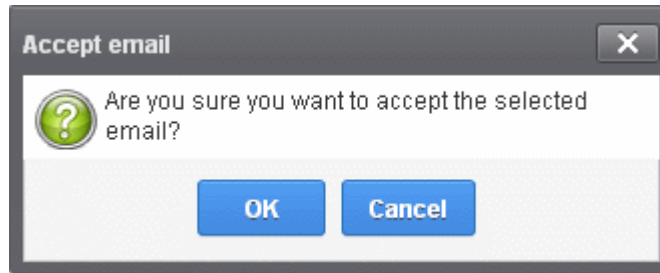
Show message **✓ Accept** ✗ Reject Refresh

Filters

<input checked="" type="checkbox"/>	Subject	From	To	CC	Date (GMT)	Reason	Size	
<input checked="" type="checkbox"/>	Fw: FLAT 20% OFF on Revital Multi-Vitamins. Limited Period Offer. Hurry	Angel <angel@heaven.co.in>	bob@docteamcasg.comodo.od.ua, bob@democasg.comodo.od.ua, john@docteamcasg.comodo.od.ua		2016-04-20 11:02:07	spam Combined (0.15)	13.31 KB	

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

An alert will be displayed to confirm adding the sender to '**Blacklist Senders Per User**'.



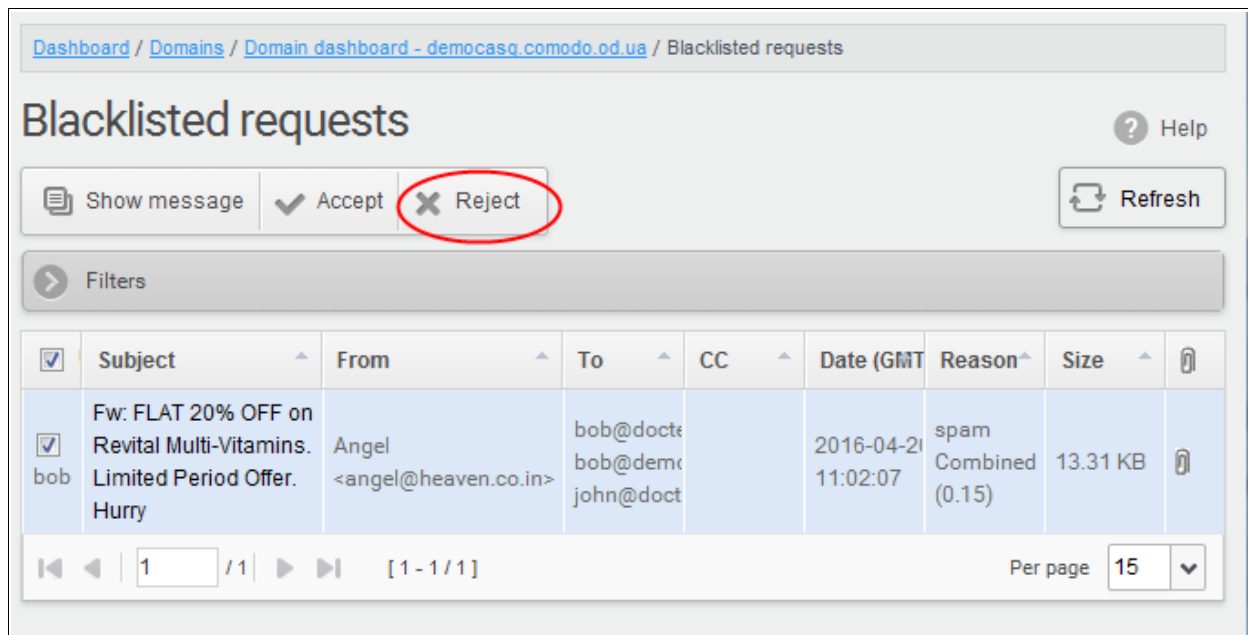
- Click 'OK' to confirm the acceptance.

The sender of the email will be added to '**Blacklist senders per user**'. See the section '**Blacklist Senders Per User**' for more details.

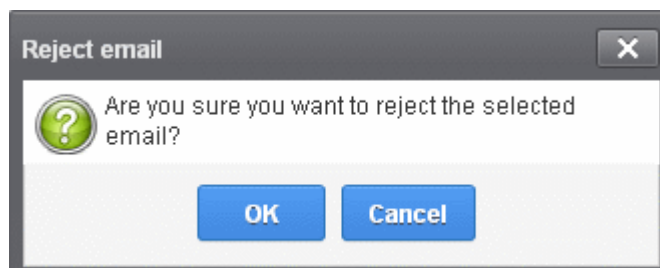
To reject the blacklist request from users

After viewing the details of the email, you can choose to reject the request from the user.

- Select the mail that you want to reject and click the 'Reject' button.



An alert will be displayed to confirm the rejection of selected email.



- Click 'OK' to confirm the rejection.

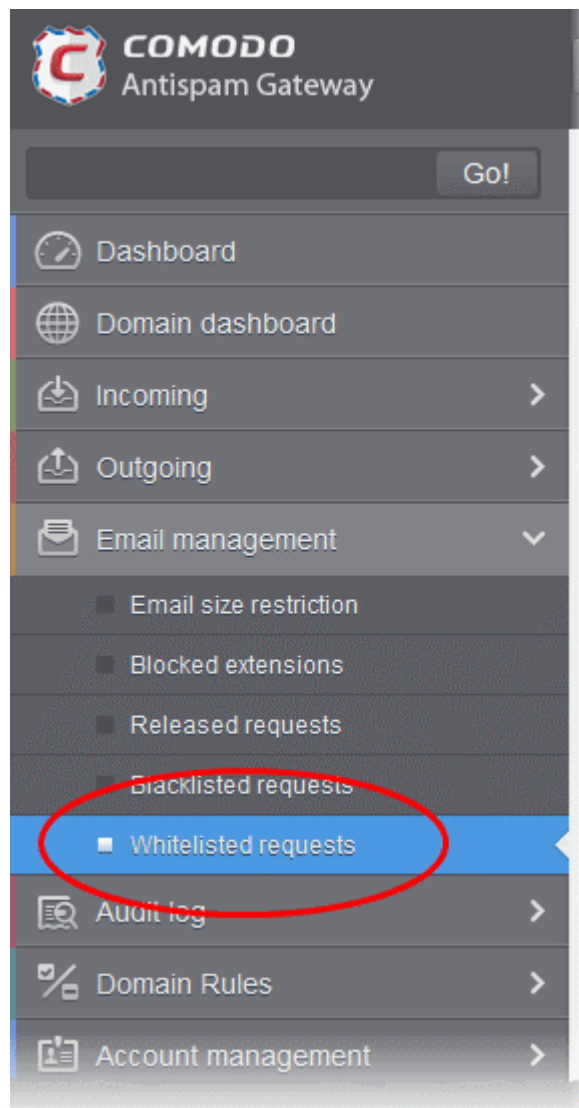
The sender will not be added to blacklist and the selected email will no longer be in the blacklisted emails list.

Whitelisted Requests

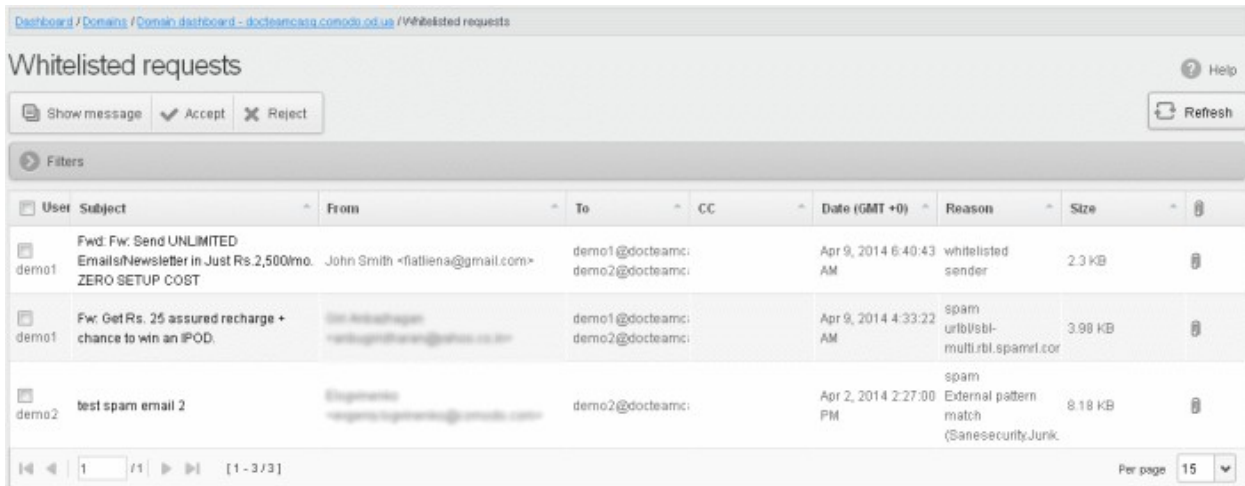
CASG allows users to send requests to their email account administrators to add senders to whitelist from their Quarantine interface. Administrators in addition to receiving emails for these requests also can view the list of such requests in 'Whitelisted requests' section of the administrator interface under 'Email management' section. The senders added to whitelist on users' request will be applicable for the requested users only. Mails from these whitelisted senders to the requested users will be allowed by CASG without passing through the antispam engine, that is, emails from a whitelisted sender to the user will delivered without any spam check. Refer to the sections **Sender Whitelist** and **Whitelist Senders Per User** for more details.

To open the whitelisted requests interface

- Click the 'Email management' tab on the left hand side navigation to expand and then click the 'Whitelisted requests' sub tab.



The 'Whitelisted requests' interface will be displayed:



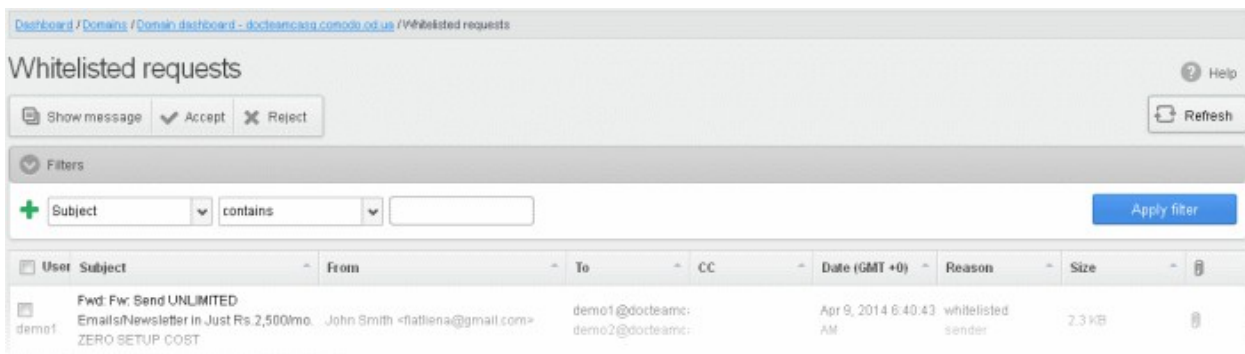
The list of emails that users requested for adding the senders to whitelist will be displayed. The list contains nine columns providing information about the requested user, subject, the sender, details of the recipients, details of recipients in the CC list, the date they were sent, the reason they were quarantined and the size of the email. The last column indicates whether there is any attachment in the mails.

Sorting the Entries

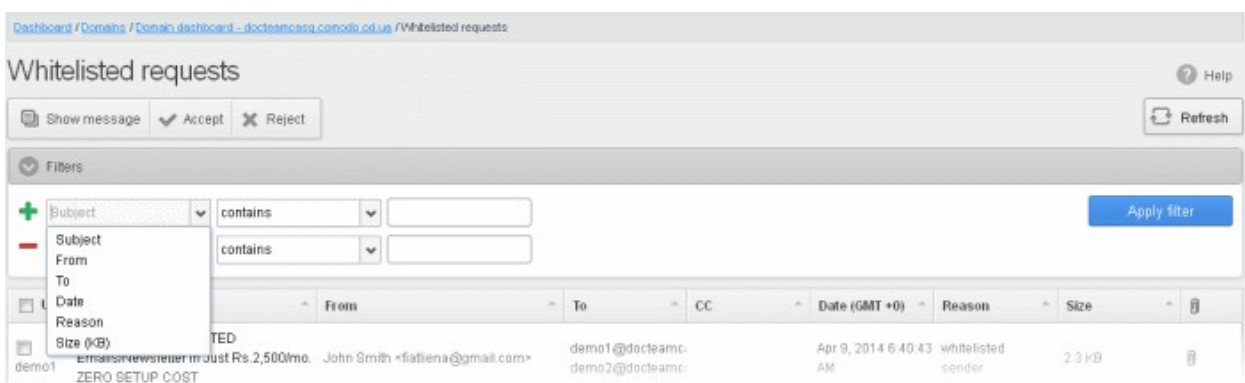
Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using Filter option to search whitelisted requests

Click anywhere on the Filters tab to open the filters area.



You can add more filters by clicking for narrowing down your search.



You can remove a filter by clicking the icon beside it.

Available filters are:

- **Subject:** Will execute a search of subject according to the text entered in the text box (column 3) and the condition selected in column 2.
- **From:** Will execute a search of senders according to the text entered in the text box (column 3) and the condition selected in column 2.
- **To:** Will execute a search of users according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Reason:** Will execute a search of words in the reason column according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all quarantined mails that contain the words entered in the text box
- **Equals:** Displays all quarantined mails that contain only the words entered in the text box
- **Not Equals:** Displays all quarantined mails that do not contain only the words entered in the text box
- **Not Contains:** Displays all quarantined emails that don't contain the words entered in the text box
- **Starts with:** Displays all quarantined emails that starts with the words entered in the text box
- **Ends with:** Displays all quarantined emails that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of mail received dates according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Size:** Will execute a search of mails according to the size selected or entered in third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions are available:

- **Equals:** Displays the quarantined emails that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the quarantined emails with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the quarantined emails with dates greater than the selected date in the third box from the calendar


If 'Size' is selected, the following conditions are available:

- **Less than:** Displays the quarantined emails with size less than the selected or entered size in the third box
- **Greater than:** Displays the quarantined emails with size greater than the selected or entered size in the third box

- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all the whitelisted requests emails.

Note: To display all the whitelisted requests after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

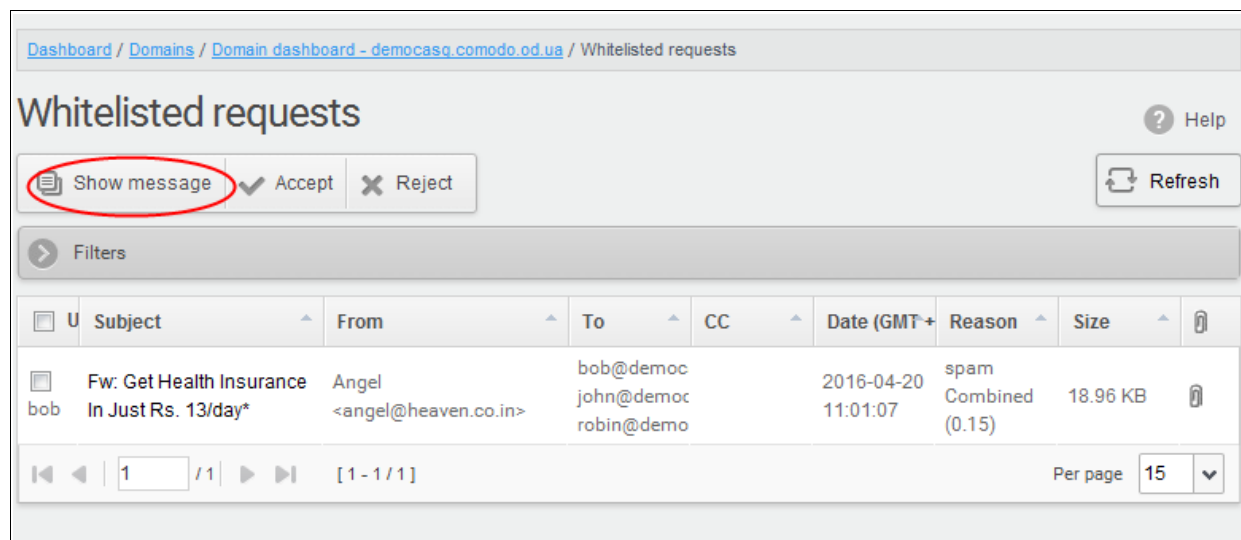
Viewing Details of Whitelisted Requests

The details such as user, subject, sender, recipient, date, reason and size of the mails requested for whitelisting can be viewed in two ways:

- In the same CASG window
- In a new CASG window

To view details of whitelisted requests in the same CASG window:

- In the whitelisted requests area, 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 details of the selected email will be displayed.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests / E-mail

E-mail ? Help

Normal All headers

✓ Accept ✗ Reject

Subject Fw: Get Health Insurance In Just Rs. 13/day*

From Angel <angel@heaven.co.in>

To bob@democasg.comodo.od.ua, john@democasg.comodo.od.ua, robin@democasg.comodo.od.ua, avantistude@gmail.com, sumeetdomestic@gmail.com, john@docteamcasg.comodo.od.ua

CC

Date (GMT +00:00) 2016-04-20 11:01:07

Size 18.96 KB

Actions

Plain text Html source Original View

On Wednesday, 20 April 2016 10:53 AM, Online Health Plan <support@indiadz.com> wrote:

If you're having trouble viewing this email, please click here.#yiv3139774641 .yiv3139774641text_box

```

|   |
|   |
|   | The Best Hospitals are Now Affordable |
|   | Get
|   | Health Insurance
|   | In Just
|   | Rs. 13/day* Get Health Insurance In Just Rs. 13/day*   |
|   |
|   |
|   |
|   | Get
|   | Cashless Claim
|   | Hospital Bills are directly

```

To view the email headers, which contain the tracking information of the mail detailing the path it has crossed before reaching the recipient, click 'All headers' tab. 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.

Check the details of the mail and ascertain whether it is a spam mail or not. You can choose to either **accept** the mail or **reject** it for whitelisting the sender. If the request is accepted, the sender will be added to '**Whitelist sender per user**'. If it is rejected, the email will be no longer in the whitelisted requests list. Please note that emails will continue to remain in the **Quarantined** list irrespective of the action taken.

To view details of whitelisted requests in new CASG window:

- In the whitelisted requests area, select the mail that you want to view and click the 'Show message in new window' button or right-click and select to open in a new tab or new window.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests

Whitelisted requests

Help

Show message Accept Reject Refresh

Filters

U	Subject	From	To	CC	Date (GMT+)	Reason	Size	
bob	Fw: Get Health Insurance In Just Rs. 13/day*	Angel	bob@democ john@democ robin@demo		2016-04-20 11:01:07	spam Combined (0.15)	18.96 KB	

Per page 15

Open Link in New Tab
Open Link in New Window
Open Link in New Private Window
Bookmark This Link
Save Link As...
Copy Link Location
Search Google for "Fw: Get Health ..."
Inspect Element (Q)

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

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests / E-mail

E-mail

Help

Normal All headers

Accept Reject

Subject Fw: Get Health Insurance In Just Rs. 13/day*

From Angel <angel@heaven.co.in>

To bob@democasg.comodo.od.ua, john@democasg.comodo.od.ua, robin@democasg.comodo.od.ua, avantistude@gmail.com, sumeetdomestic@gmail.com, john@docteamcasg.comodo.od.ua

CC

Date (GMT +00:00) 2016-04-20 11:01:07

Size 18.96 KB

Actions

Plain text Html source Original View

On Wednesday, 20 April 2016 10:53 AM, Online Health Plan <support@indiadz.com> wrote:

If you're having trouble viewing this email, please click here.#yiv3139774641 .yiv3139774641text_box

| |

| The Best Hospitals are Now Affordable |

| Get

Health Insurance

In Just

Rs. 13/day* Get Health Insurance In Just Rs. 13/day* |

| |

| |

| |

| Get

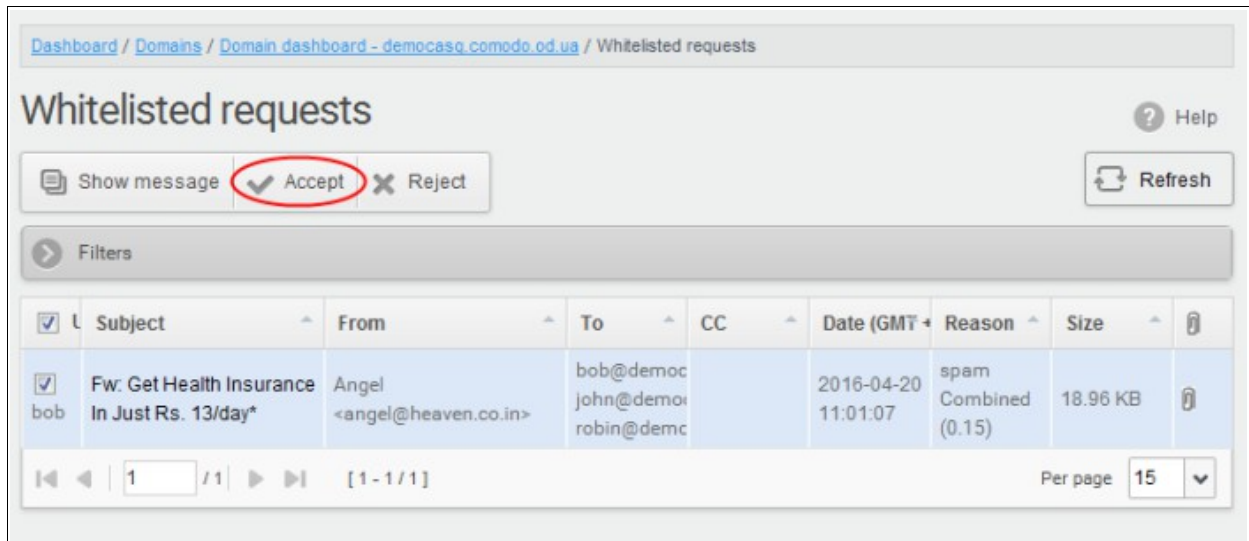
Cashless Claim

Hospital Bills are directly

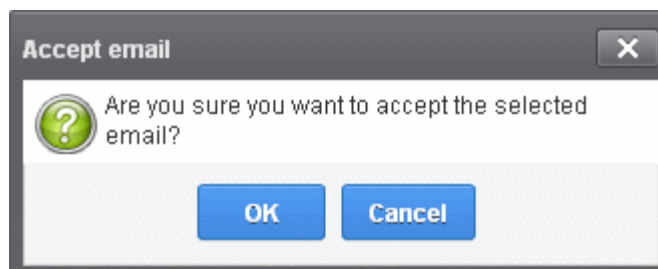
To accept the whitelist request from users

After viewing the details, you can choose to accept the request from user to add the sender to **whitelist senders per user** list.

- Select the mail that you want to add the sender to whitelist and click the 'Accept' button.



An alert will be displayed to confirm adding the sender to **'Whitelist sender per user'**.



- Click 'OK' to confirm the acceptance.

The sender of the email will be added to **'Whitelist sender per user'**. See the section **'Whitelist Sender Per User'** for more details.

To reject the whitelist request from users

After viewing the details of the email, you can choose to reject the request from the user.

- Select the mail that you want to reject and click the 'Reject' button.

Dashboard / Domains / Domain dashboard - democasg.comodo.od.ua / Whitelisted requests

Whitelisted requests

Help

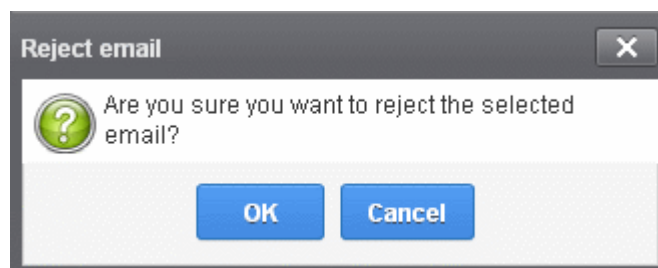
Show message Accept **Reject** Refresh

Filters

<input type="checkbox"/>	Subject	From	To	CC	Date (GMT)	Reason	Size	
<input type="checkbox"/>	Fw: Get Health Insurance In Just Rs. 13/day*	giri anbazhagan <anbugiridharan@yahoo>	bob@demc john@dem robin@dem		2016-04-20 11:01:07	spam Combined (0.15)	18.96 KB	

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

An alert will be displayed to confirm the rejection of user's request.



- Click 'OK' to confirm the rejection.

The sender will not be added to whitelist and the selected email will no longer be in the whitelisted requests list.

3.2.1.1.4.5 Domain Audit Log

CASG keeps a record of actions initiated by users and administrators for a selected domain. The Audit Log area allows administrators with appropriate privileges to configure and view these log reports. CASG also keeps a consolidated log for all domains belonging to an account. To know more about consolidated log for all domains, refer to the section **Audit Log** for more details. This section explains about audit log for a selected domain.

The screenshot displays the Comodo Antispam Gateway Administrator interface. At the top, there are status indicators for Quarantine (0), Release requests (0), Whitelist requests (0), and Blacklist requests (0), along with a 'My Account' link. The left sidebar contains a navigation menu with options: Dashboard, Domain dashboard, Incoming, Outgoing, Email management, Audit log (expanded to show Configuration and Log), Domain Rules, and Account management. The main content area is titled 'Audit configuration' and includes a breadcrumb trail: Dashboard / Domains / Domain dashboard - democasq.comodo.od.ua / Audit configuration. The configuration section is divided into four main areas: 1. 'Quarantined item released' with checkboxes for 'Create audit log entry' (checked) and 'Send notification email' (unchecked). 2. 'Whitelist rules updated' with checkboxes for 'Create audit log entry' (checked) and 'Send notification email' (unchecked). 3. 'Blacklist rules updated' with checkboxes for 'Create audit log entry' (checked) and 'Send notification email' (unchecked). 4. 'Notification recipients' with a text input field and a 'Save' button. At the bottom of the page, there is a support link: 'Having Trouble? Support is here to help, asqsupport@comodo.com or review the [Admin guide](#)'.

Click the following links for more details.

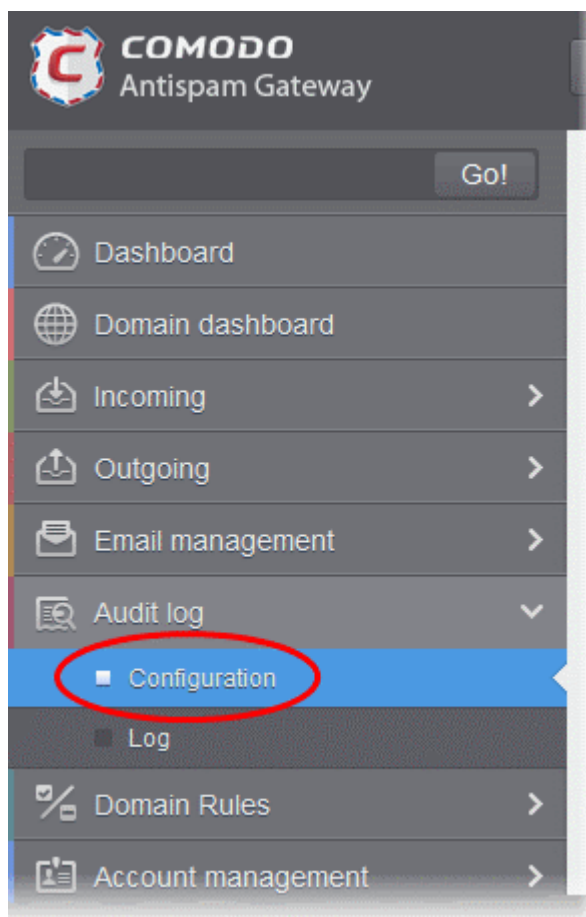
- [Audit Log Configuration](#)
- [View Domain Log](#)

Audit Log Configuration

CASG keeps a record of all actions initiated by administrators and users. However, some of the actions can be configured not be recorded such as releasing quarantined items, updating sender whitelist and blacklist senders per user. The screen also allows administrators to add recipients to whom the notifications will be sent.

To configure audit log

- Click the 'Audit log' tab on the left hand side navigation to expand and then click the 'Configuration' sub tab.



The Audit Configuration screen will be displayed:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Audit configuration

Audit configuration ? Help

Quarantined item released

Create audit log entry
 Send notification email

Sender whitelist updated

Create audit log entry
 Send notification email

Sender blacklist updated

Create audit log entry
 Send notification email

Notification recipients

[Save](#)

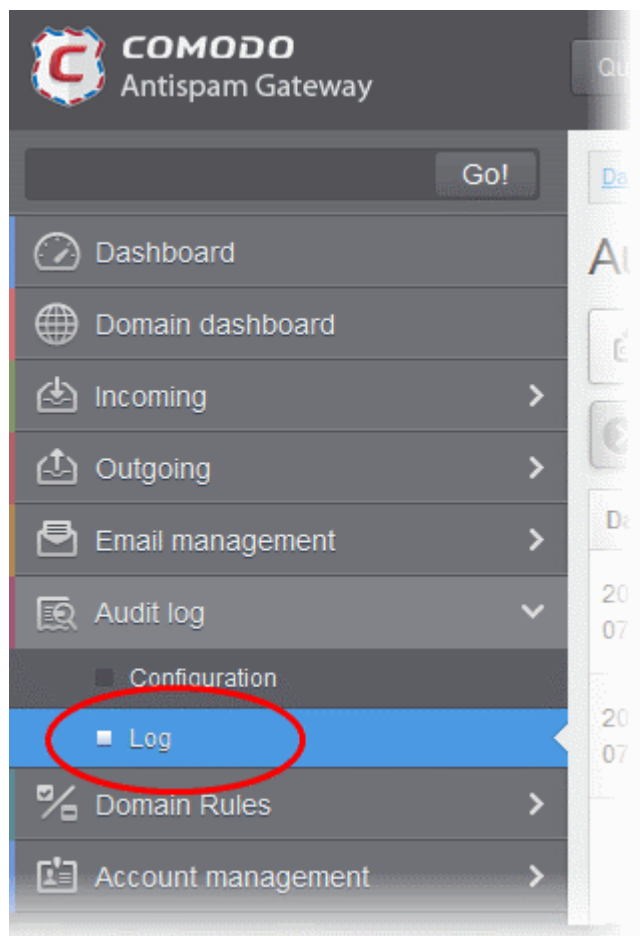
- **Quarantined item released**
 - Create audit log entry - If enabled, CASG records the release of **quarantined mails**.
 - Send notification email - If enabled, notification mails for quarantined mails release will be sent to recipients added in the 'Notification recipient's' box.
- **Sender whitelist updated**
 - Create audit log entry - If enabled, CASG records any updates to **Whitelist senders per user** interface
 - Send notification email - If enabled, notification mails for updates to **Whitelist senders per user** interface will be sent to recipients added in the 'Notification recipient's' box.
- **Sender blacklist updated**
 - Create audit log entry - If enabled, CASG records any updates to **Blacklist senders per user** interface.
 - Send notification email - If enabled, notification mails for updates to **Blacklist senders per user** interface will be sent to recipients added in the 'Notification recipient's' box.
- **Notification recipients** - Enter the email addresses of the persons to whom the email notifications for the above mentioned actions will be sent. Please note that any email addresses of the recipient's can be entered here.

View Domain Log

The log screen in CASG allows administrators with appropriate privileges to view the logs of the selected domain.

To view the audit log of the selected domain

- Click the 'Audit log' tab on the left hand side navigation to expand and then click the 'Log' sub tab.



The Audit log screen will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Audit log

Audit log

Export to CSV by filter Help Refresh

Filters

Date (GMT +0)	Role	Login	Operation key	Operation description	Details
2014-04-13 09:16:42	admin	john@docteamcas	UNWHITELIST_SE	Remove sender from the whitelist	goodguy@heaven.com
2014-04-13 08:57:07	admin	john@docteamcas	RELEASE_EMAIL_	Release quarantined message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: ; Date: Mon Apr 07 08:52:31 GMT 2014; Subject: Fw: We have free samples for you, now try before you buy @ your doorsteps!
2014-04-13 08:53:57	admin	john@docteamcas	WHITELIST_SEND	Whitelist sender	goodguy@heaven.com
2014-04-13 08:52:28	admin	john@docteamcas	UNWHITELIST_SE	Remove sender from the whitelist	someone@example.com
2014-04-13 08:50:23	admin	john@docteamcas	RELEASE_EMAIL_	Release quarantined message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: ; Date: Mon Apr 07 08:52:31 GMT 2014; Subject: Fw: We have free samples for you, now try before you buy @ your doorsteps!
2014-04-13 08:45:07	admin	john@docteamcas	BLACKLIST_SEND	Blacklist sender	devil@hell.com
2014-04-13 08:35:36	admin	john@docteamcas	WHITELIST_SEND	Whitelist sender	someone@example.com
2014-04-13 08:27:36	user	demo1	USER_BLACKLIST	Request blacklist sender for user	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: John Smith <fatlena@gmail.com>; Subject: Fwd: Fw: Send UNLIMITED Emails!Newsletter in Just Rs 2,500/mo. ZERO SETUP COST, Wed Apr 09 06:40:43 GMT 2014
2014-04-13 08:25:37	admin	john@docteamcas	REJECT_WHITELIS	Reject request whitelist sender for user	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: John Smith <fatlena@gmail.com>; Subject: Fwd: Fw: Send UNLIMITED Emails!Newsletter in Just Rs 2,500/mo. ZERO SETUP COST, 2014-04-09 06:40:43.0

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. The sorting option is not available for 'Operation description' column.

Using Filter options to search particular event(s)

- Click anywhere on the 'Filters' tab to open the filters area.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Audit log

Audit log

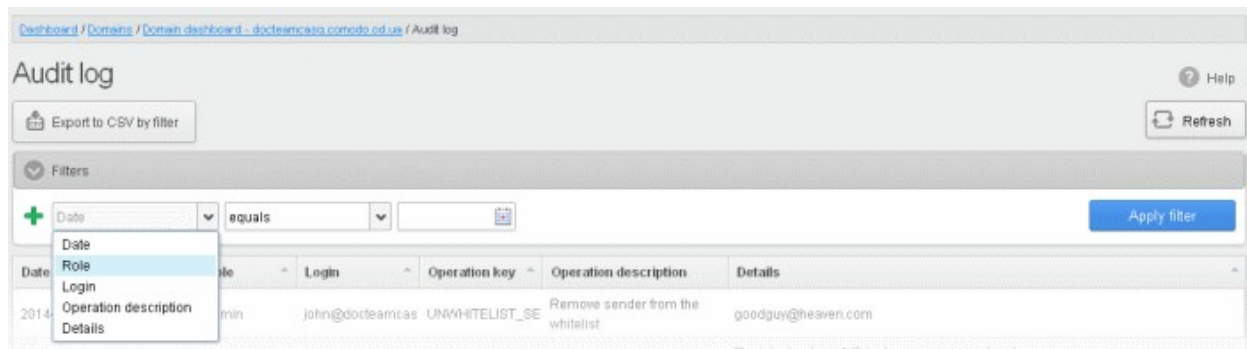
Export to CSV by filter Help Refresh

Filters

+ Date equals Apply filter

Date (GMT +0)	Role	Login	Operation key	Operation description	Details
2014-04-13 09:16:42	admin	john@docteamcas	UNWHITELIST_SE	Remove sender from the whitelist	goodguy@heaven.com

You can add more filters by clicking  for narrowing down your search.



You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Login:** Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Details:** Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all log entries that contain the words entered in the text box
- **Equals:** Displays all log entries that contain only the words entered in the text box
- **Not Equals:** Displays all log entries that do not contain only the words entered in the text box
- **Not Contains:** Displays all log entries that don't contain the words entered in the text box
- **Starts with:** Displays all log entries that starts with the words entered in the text box
- **Ends with:** Displays all log entries that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of log entries according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Role:** Will execute a search of log entries according to the role selected in the third field (column 3) and the condition selected in column 2.
- **Operative description:** Will execute a search of log entries according to the action selected in the third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions are available:

- **Equals:** Displays the log entries that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the log entries with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the log entries with dates greater than the selected date in the third box from the calendar

If 'Role' is selected, the following conditions are available:

- **Equals:** Displays all log entries that is equal to the role selected in column 3.
- **Not Equals:** Displays all log entries that except the role selected in column 3.

If 'Operative description' is selected, the following conditions are available:

- **Equals:** Displays all log entries that is equal to the event selected in column 3.
- **Not Equals:** Displays all log entries that except the event selected in column 3.
- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.



- Click the  button to display all the entries.

Note: To display all the log entries after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

The following table provides the details of actions initiated by user/administrator and shown under Operation Key and Operation Description columns in the log report:

S.No.	Operation Key	Operation Description
1	DELETE_EMAIL_FROM_QUARANTINE_BY_FILTER	Delete quarantined messages by filter
2	DELETE_EMAIL_FROM_QUARANTINE	Delete quarantined message
3	RELEASE_EMAIL_FROM_QUARANTINE	Release quarantined message
4	WHITELIST_RECIPIENT	Whitelist recipient
5	BLACKLIST_RECIPIENT	Blacklist recipient
6	UNWHITELIST_RECIPIENT	Remove recipient from the whitelist
7	UNBLACKLIST_RECIPIENT	Remove recipient from the blacklist
8	WHITELIST_SENDER	Whitelist sender
9	BLACKLIST_SENDER	Blacklist sender
10	UNWHITELIST_SENDER	Remove sender from the whitelist
11	UNBLACKLIST_SENDER	Remove sender from the blacklist
12	RESET_TO_DEFAULT_WHITELISTED_SENDERS	Reset senders whitelist
13	RESET_TO_DEFAULT_WHITELISTED_RECIPIENTS	Reset recipients whitelist
14	RESET_TO_DEFAULT_BLACKLISTED_SENDERS	Reset senders blacklist
15	RESET_TO_DEFAULT_BLACKLISTED_RECIPIENTS	Reset recipients blacklist
16	WHITELIST_SENDER_DOMAIN	Whitelist all senders of the domain
17	WHITELIST_RECIPIENT_DOMAIN	Whitelist all recipients of the domain
18	BLACKLIST_SENDER_DOMAIN	Blacklist all senders of the domain
19	BLACKLIST_RECIPIENT_DOMAIN	Blacklist all recipients of the domain
20	USER_WHITELIST_REQUEST_PER_USER	Request whitelist sender for user
21	USER_BLACKLIST_REQUEST_PER_USER	Request blacklist sender for user

22	USER_RELEASE_REQUEST	Release request
23	USER_CANCEL_WHITELIST_REQUEST_PER_USER	Cancel request whitelist sender for user
24	USER_CANCEL_BLACKLIST_REQUEST_PER_USER	Cancel request blacklist sender for user
25	USER_CANCEL_RELEASE_REQUEST	Cancel release request
26	ACCEPT_WHITELIST_REQUEST_PER_USER	Accept request whitelist sender for user
27	ACCEPT_BLACKLIST_REQUEST_PER_USER	Accept request blacklist sender for user
28	ACCEPT_RELEASE_REQUEST	Accept release request
29	REJECT_WHITELIST_REQUEST_PER_USER	Reject request whitelist sender for user
30	REJECT_BLACKLIST_REQUEST_PER_USER	Reject request blacklist sender for user
31	REJECT_RELEASE_REQUEST	Reject release request
32	SPAM_DETECTION_SETTINGS	Update spam detection settings
33	SPAM_DETECTION_SETTINGS_RESET_TO_DEFAULT	Reset spam detection settings
34	DELETE_EMAIL_FROM_ARCHIVE_BY_FILTER	Delete archived messages by filter
35	DELETE_EMAIL_FROM_ARCHIVE	Delete archived message
36	RESEND_EMAIL_FROM_ARCHIVE	Resend archived message
37	REPORTS_AS_SPAM	Reports archived message as a SPAM
38	QUARANTINE_EMAIL	Quarantine message
39	ACCEPT_AND_ARCHIVE_EMAIL	Accept and archive message
40	MARK_EMAIL_AS_SPAM	Mark message as spam
41	ACCEPT_EMAIL	Accept message
42	WHITELIST_USER_SENDER	Whitelist sender for user
43	BLACKLIST_USER_SENDER	Blacklist sender for user
44	UNWHITELIST_USER_SENDER	Remove sender from the user whitelist
45	UNBLACKLIST_USER_SENDER	Remove sender from the user blacklist
46	QUARANTINE_REPORT_SUBSCRIPTION_UPDATE	Quarantine report subscription update
47	QUARANTINE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Quarantine report subscription reset to default
48	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_UPDATE	Domain report subscription update

49	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Domain report subscription reset to default
50	DOMAIN_ADD	Add domain
51	DOMAIN_DELETE	Remove domain
52	ADMIN_ADD	Add admin
53	ADMIN_EDIT	Edit admin settings
54	ADMIN_DELETE	Remove admin
55	ADMIN_UNLOCK	Unlock admin
56	ADMIN_REGENERATE_PASSWORD	Regenerate password for admin
57	ADMIN_PASSWORD_UPDATE	Update password for admin
58	SYSTEM_NOTIFICATIONS_TEMPLATE_CHANGE	System notifications template change
59	ADMIN_PERMISSIONS_GROUP_ADD	Add admin permission group
60	ADMIN_PERMISSIONS_GROUP_DELETE	Remove admin permission group
61	ADMIN_PERMISSIONS_GROUP_UPDATE	Update admin permission group
62	ADMIN_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default admin permission group
63	ADMIN_PERMISSIONS_ASSIGN_GROUP	Assign admin permission group by selection
64	REPORT_SPAM_BY_FILE	Report delivered message as spam
65	DOMAIN_DESTINATION_ROUTES_UPDATE	Update destination routes
66	DOMAIN_LOCAL_RECIPIENTS_ADD	Add local recipient
67	DOMAIN_LOCAL_RECIPIENTS_DELETE	Remove local recipient
68	DOMAIN_LOCAL_RECIPIENTS_STATE_CHANGE	Local recipients state change
69	DOMAIN_ALIASES_ADD	Add domain alias
70	DOMAIN_ALIASES_DELETE	Remove domain alias
71	DOMAIN_SETTINGS_UPDATE	Update domain settings
72	DOMAIN_SETTINGS_RESET_TO_DEFAULT	Reset domain settings to default
73	DOMAIN_RELAY_RESTRICTIONS_ADD	Add relay restriction
74	DOMAIN_RELAY_RESTRICTIONS_UPDATE	Update relay restriction
75	DOMAIN_RELAY_RESTRICTIONS_DELETE	Remove relay restriction
76	DOMAIN_RELAY_RESTRICTIONS_STATE_CHANGE	Relay restriction state change
77	DOMAIN_OUTGOING_USER_ADD	Add outgoing user
78	DOMAIN_OUTGOING_USER_SETTINGS_UPDATE	Edit outgoing user

79	DOMAIN_OUTGOING_USER_DELETE	Remove outgoing user
80	DOMAIN_OUTGOING_USER_LOCK	Lock outgoing user
81	DOMAIN_OUTGOING_USER_UNLOCK	Unlock outgoing user
82	DOMAIN_OUTGOING_USER_PASSWORD_UPDATE	Update password for outgoing user
83	DOMAIN_EMAIL_SIZE_RESTRICTION_CHANGE	Email size restriction change
84	DOMAIN_BLOCKED_EXTENSIONS_UPDATE	Update blocked extensions
85	DOMAIN_BLOCKED_EXTENSIONS_RESET_TO_DEFAULT	Reset blocked extensions to default
86	DOMAIN_AUDIT_CONFIGURATION_CHANGE	Audit configuration change
87	DOMAIN_LDAP_CONFIGURATION_CHANGE	LDAP configuration change
88	DOMAIN_INCOMING_USER_ADD	Add incoming user
89	DOMAIN_INCOMING_USER_EDIT	Edit incoming user
90	DOMAIN_INCOMING_USER_DELETE	Remove incoming user
91	DOMAIN_INCOMING_USER_UNLOCK	Unlock incoming user
92	DOMAIN_INCOMING_USER_REGENERATE_PASSWORD	Regenerate password for incoming user
93	DOMAIN_INCOMING_USER_PASSWORD_UPDATE	Update password for incoming user
94	DOMAIN_INCOMING_USER_ALIASES_UPDATE	Update incoming user aliases
95	DOMAIN_INCOMING_USER_MOVE_USER_TO_ALIAS	Move user to alias
96	DOMAIN_INCOMING_USER_MOVE_ALIAS_TO_USER	Move alias to incoming user
97	USER_PERMISSIONS_GROUP_ADD	Add user permission group
98	USER_PERMISSIONS_GROUP_DELETE	Remove user permission group
99	USER_PERMISSIONS_GROUP_UPDATE	Update user permission group
100	USER_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default user permission group
101	USER_PERMISSIONS_ASSIGN_GROUP	Assign user permission group by selection

Export Log Report to CSV

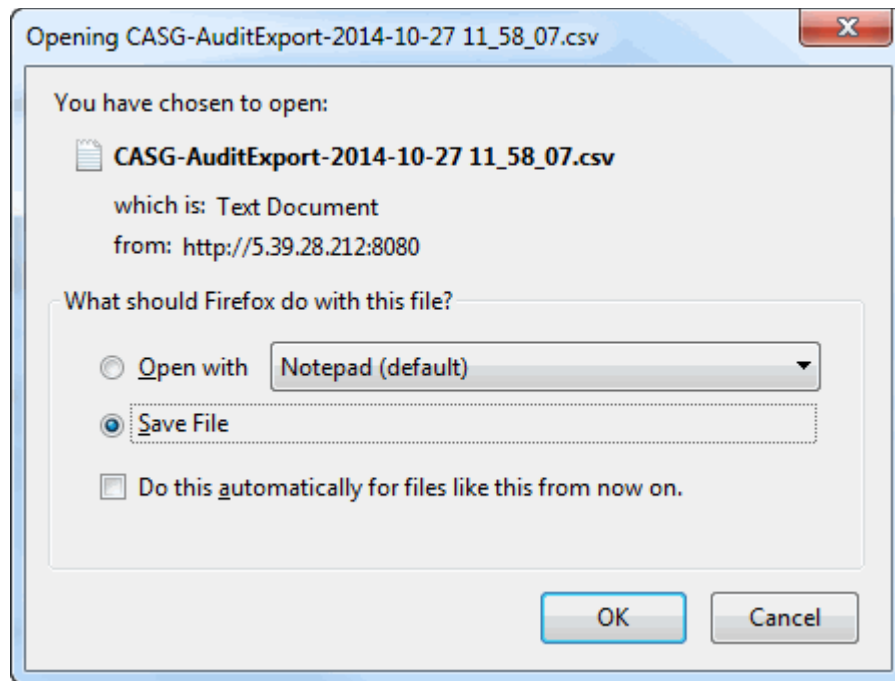
The log report can be exported to a comma separated value (CSV) file and is limited to 10,000 entries per file. If the entries exceed this value, exporting cannot be done and a warning will be displayed. Please note that exported file will display the entries in the same sorted order as in the interface.

To export log report to csv file

- Click the 'Export to CSV by filter' button.



The 'File Download' dialog will be displayed.

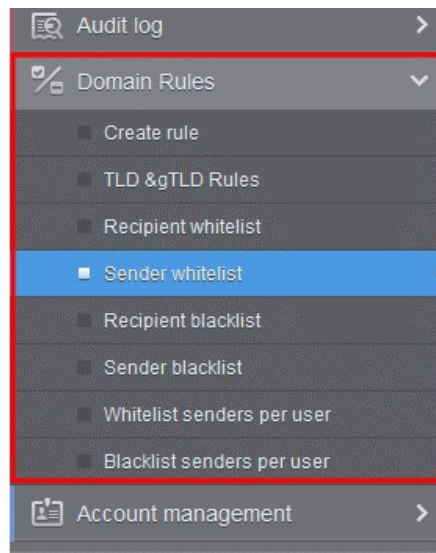


- Click 'Open' to view the file with an appropriate application or click 'OK' to save the file to your computer.

The values in the log report will be separated by commas and this file can be opened with appropriate application such as Excel or Openoffice Calc for easy analysis.

3.2.1.1.4.6 Domain Rules

The domain rules interface allows administrators to create granular filtering rules for each domain in order to blacklist, whitelist or forward mails. Rules can be based on sender, recipient, source/destination server, subject line, suspicious attachments and more.



Note: Under default conditions, CASG will filter all incoming mails to all domains that have been enabled in the 'Domains' area.

The following table offers more details on each rule type:

Rule Type	Description	Notes
Domain Rules ('Create Rule...')	Create granular rules to blacklist, whitelist or forward mail based on one or more criteria.	Criteria include sender, sender mail server, recipient, relay server, subject line and suspicious attachment.
TLD & gTLD Rules	Allow or block mails based on top level domain.	Mail from all TLDs is allowed by default. This interface allows you to block selected TLDs.
Recipient Whitelist	Always allow mail sent to these recipients.	For example, CASG will allow/block mails to/from <code>specific_user@example.com</code> , but will filter as normal email to/from <code>any_other_users@example.com</code>
Sender Whitelist	Always allow mail from these senders.	
Recipient Blacklist	Always block mail sent to these recipients.	You can bulk import email addresses from .csv or add manually.
Sender Blacklist	Always block mail from these senders.	
Whitelist senders per user	Always allow mail from specific email addresses to specific users.	For example, CASG will allow/block mails from <code>specific_sender@example.com</code> to <code>specific_recipient@your_domain.com</code> , but will continue to filter mail from <code>specific_sender@example.com</code> to <code>everybody_else@your_domain.com</code>
Blacklist senders per user	Always block mail from a specific email addresses to specific users.	

		You can bulk import email addresses from .csv or add manually.
--	--	--

General Advice

- If you are troubleshooting issues with a particular email address, please check all interfaces listed under 'Domain Rules'.
- Rule priorities can be summarized as follows:
 1. Email Size Restriction
 2. Domain Whitelist rules
 3. Sender/Recipient Whitelist
 4. Domain Blacklist rules
 5. Sender/Recipient Blacklist
 6. TLD & gTLD blacklist rule
 7. Per user White list
 8. Per user Black list
 9. Email Blocked Extensions

CASG will stop applying rules on first match (if any).
- **'Email Size Restrictions'** have a higher priority than domain rules. CASG will still block mails that exceed 'Email Size Restriction' regardless of any rules.
- **'Email Blocked Extensions'** have a lower priority than domains rules. CASG will not stop mails containing a blocked extension if there is a whitelist rule which green-lights the message.
- White-list domains rules take precedence over blacklist domain rules.
- Whitelist/blacklist rules in the domain rules section take precedence over 'per user' whitelist/blacklist rules.

Click the following links for more details.

- [Rules](#)
- [TLD and gTLD Rules](#)
- [Recipient Whitelist](#)
- [Sender Whitelist](#)
- [Recipient Blacklist](#)
- [Sender Blacklist](#)
- [Whitelist Senders Per User](#)
- [Blacklist Senders Per User](#)

Rules

Administrators can create rules to filter inbound mails based on sender, recipient, source and relay/MTA server, subject line, attachments and so on. There are three types of filtering rules:

- **Blacklist rule** - Blocks inbound mails based on one or more filter criteria. Criteria include sender, recipient, mail servers/relays and specific subject line.
- **Whitelist rule** - Allows mails to pass through, without security checks, based on one or more filter criteria.

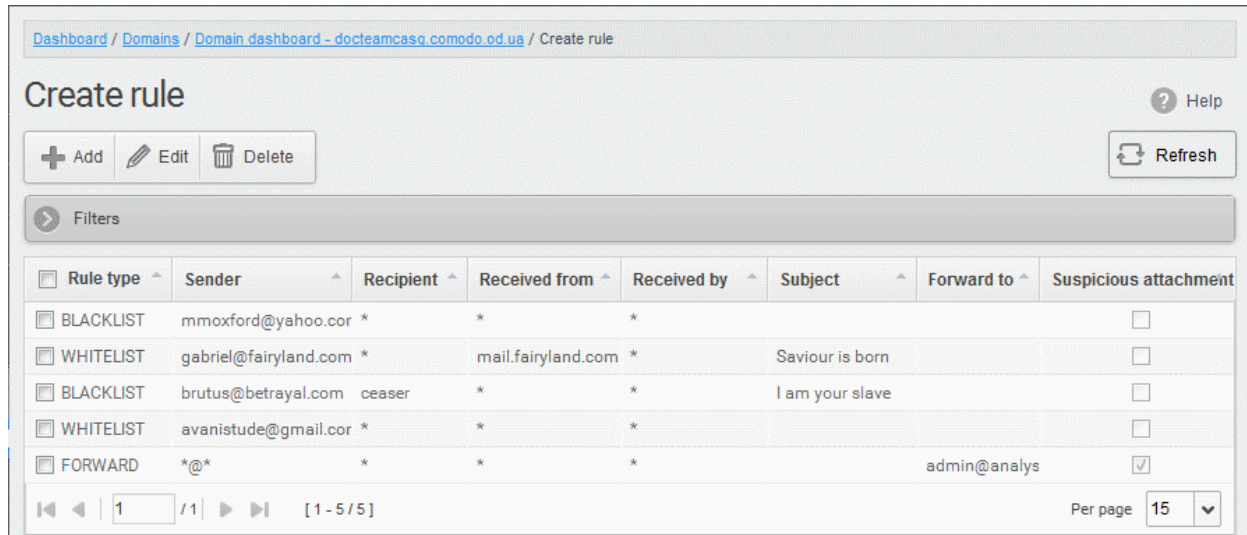
Criteria include sender, recipient, mail servers/relays and specific subject line.

- **Forward rule** - Forwards mails based on one or more filter criteria, to a set email address. Criteria include sender, recipient, mail servers/relays and specific subject line.

For example, you can create rules to block all mails from a specific mail server, allow all mails from a specific sender to a specific recipient, forward all mails containing a specific text string in the subject line and so on.

To open the Create Rule interface

- Click the 'Domain Rules' tab from the left and choose the 'Create rule' sub tab.



The 'Create Rules' interface displays the list of mail filtering rules with the conditional parameters of each rule.

Mail Filtering Rules - Column Descriptions	
Column Header	Description
Rule Type	Indicates whether the rule is for Blacklisting, whitelisting or forwarding.
Sender	The sender whose mails are intercepted by the rule.
Recipient	The recipient at the domain, whose mails are intercepted by the rule.
Received From	All mails sent from the external mail server indicated in this field will be intercepted by the rule.
Received by	All mails forwarded by the sending servers primary relays of the sending server or MTA indicated in this field will be intercepted by the rule.
Subject	Mails containing subject line indicated in this field will be intercepted by the rule.
Forward to	Indicates the email address to which the mails satisfying the conditions are forwarded. (Applies only to Forward Rules.)
Suspicious attachment	Indicates whether the rule should apply only to mails containing suspicious attachments

Sorting the Entries

Clicking any column header except the Suspicious Attachment, sorts the rules on the ascending/descending order of the entries in that column.

Using Filter option to search rules

- Click anywhere on the 'Filters' tab to open the filters area.

The screenshot shows the 'Filters' area with a toolbar containing '+ Add', 'Edit', and 'Delete' buttons, and a 'Refresh' button. Below the toolbar is a 'Filters' tab with a dropdown arrow. Underneath, there is a filter rule configuration area with a green '+' icon on the left. The rule is defined by three fields: 'Rule type' (dropdown), 'equals' (condition dropdown), and 'BLACKLIST' (text field). An 'Apply filter' button is on the right. Below this is a table of filterable fields: Rule type, Sender, Recipient, Received from, Received by, Subject, and Forward to.

- Select the field from the first drop-down, choose the condition from the second drop-down and enter the search criteria in the third field.

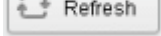
You can add more filters by clicking  for narrowing down your search.

The screenshot shows the 'Filters' area with three filter rules. The first rule is 'Sender' with condition 'contains' and value 'gabriel'. The second rule is 'Subject' with condition 'contains' and value 'saviour'. The third rule is 'Rule type' with condition 'equals' and value 'BLACKLIST'. Each rule has a red '-' icon on the left. An 'Apply filter' button is on the right. Below the rules is the same table of filterable fields as in the previous screenshot.

You can remove a filter by clicking the  icon beside it.

Available filters are:

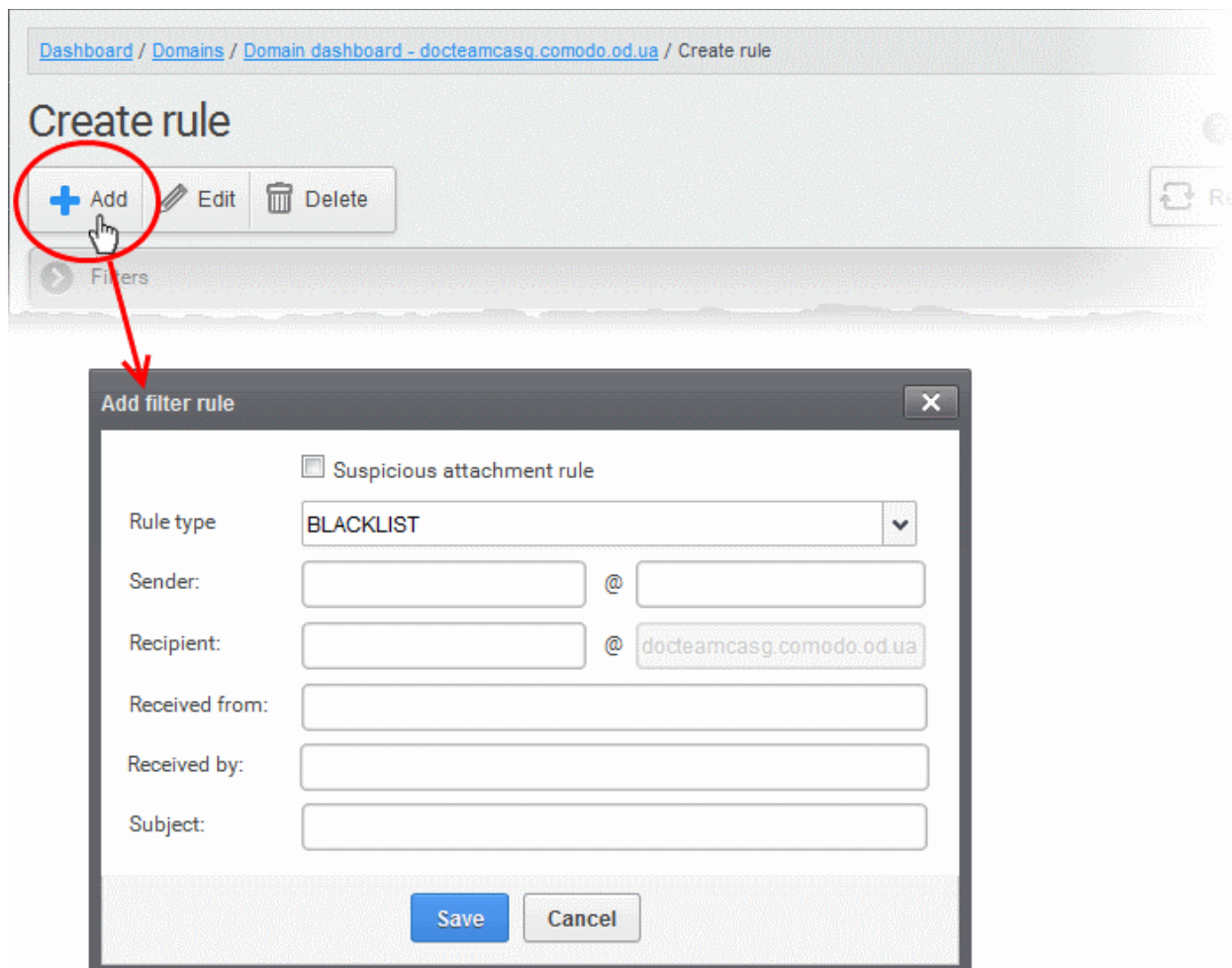
- Rule Type** - Filters rules based on type selected from the right drop-down and the condition selected in middle drop-down.
 - Sender** - Filters rules based on sender's email address entered in part or full, in the right text field and condition chosen from the middle drop-down
 - Recipient** - Filters rules based on recipient's user name entered in part or full, in the right text field and condition chosen from the middle drop-down.
 - Received from** - Filters rules based on hostname or IP address of external mail server entered in part or full, in the right text field and condition chosen from the middle drop-down.
 - Received by** - Filters rules based on hostname or IP address of internal mail server entered in part or full, in the right text field and condition chosen from the middle drop-down.
 - Subject** - Filters rules based on subject line entered in part or full, in the right text field and condition chosen from the middle drop-down.
 - Forward to** - Filters rules based on forward email address entered in part or full, in the right text field and condition chosen from the middle drop-down.
 - Suspicious attachment rule** - Filters rules created for suspicious attachment based on condition chosen from the middle drop-down and option from the checkbox at the right.
- Click 'Apply Filter' after selecting the filters and selecting the conditions to view the filtered results.
 - To close the 'Filters' area, click anywhere on the 'Filters' stripe.

- To remove the filters and to view all the rules, click the Refresh  button after closing the 'Filters' area.

To create a new mail filter rule

- Click the 'Add' button.

The 'Add blacklist rule' dialog will be displayed:



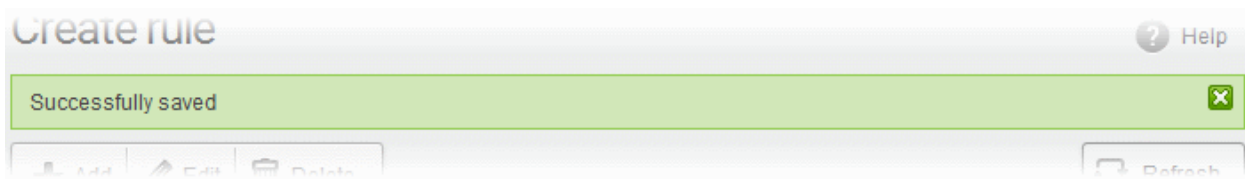
- **Suspicious attachment rule** - By default, all mails containing suspicious attachments like malware and macros will be quarantined by CASG. But you can create Suspicious attachment rule, if you want those mails from a specific sender, addressed to a specific recipient, sent by/received by specific mail servers and / or containing specific subject line, to be forwarded to a specific email address, blocked or allowed. Select this option only if you are creating the rule to intercept the mails containing suspicious attachments, else leave it un-selected.

Note: Selecting 'Suspicious attachment rule' makes the rule to intercept ONLY those mails containing any suspicious attachments AND containing the values as configured for the other parameters for the rule. It will not intercept the mails containing the same values for the parameters but not containing any suspicious attachment(s).

- **Rule type** - Select the rule type. The available options are:
 - BLACKLIST - All mails with fields satisfying the parameters entered in the options below, will be blocked.
 - WHITELIST - All mails with fields satisfying the parameters entered in the options below, will be passed without security checks.
 - FORWARD - All mails with fields satisfying the parameters entered in the options below, will be forwarded to the email address entered in the 'Forward email' field.
- **Sender** - Enter the email address of the sender, mails sent by whom are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter username/domain name in part, so that all mails containing sender address with partial text entered in this field will be intercepted. For

example, entering '*@hell.com' intercepts mails from all users from the domain name 'hell.com', entering 'evilspirit@*', processes all mails with sender name 'evilspirit' from any domain and entering '*@*' intercepts all the mails with parameters entered in the fields below.

- **Recipient** - Enter the username part of the email address of the recipient, mails sent to whom are to be intercepted by the rule. The domain name part will be auto-populated with the domain name from which the rule is created. You can use wildcard characters (*, ?) to enter username in part, so that all mails containing 'To' address with partial text entered in this field will be intercepted.
 - **Received from** - Enter the hostname or IP address of the external mail server, mails sent from which, are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter server name in part. For example, entering 'mailxxx*' will intercept all mails that contain "mailxxx" in part in the 'Received From' field of the mail header. To specify all sender mail servers, enter just the wildcard character.
 - **Received by** - Enter the primary relay of the sending server or the MTA, mails sent through which, are to be intercepted by the rule. You can use wildcard characters (*, ?) to enter server name in part. For example, entering 'mailyyy*' will intercept all mails that contain "mailyyy" in part in the 'Received By' field of the mail header. To specify all mail servers, enter just the wildcard character.
 - **Subject** - Enter the subject line, so that the system displays all quarantined mails that contain the words entered in the text box.
 - **Forward email** - This field is available only for 'FORWARD' rule. Enter the email address to which the emails containing values in the email header as configured in the fields above are to be forwarded.
- Click 'Save' to add the rule to the list of rules.

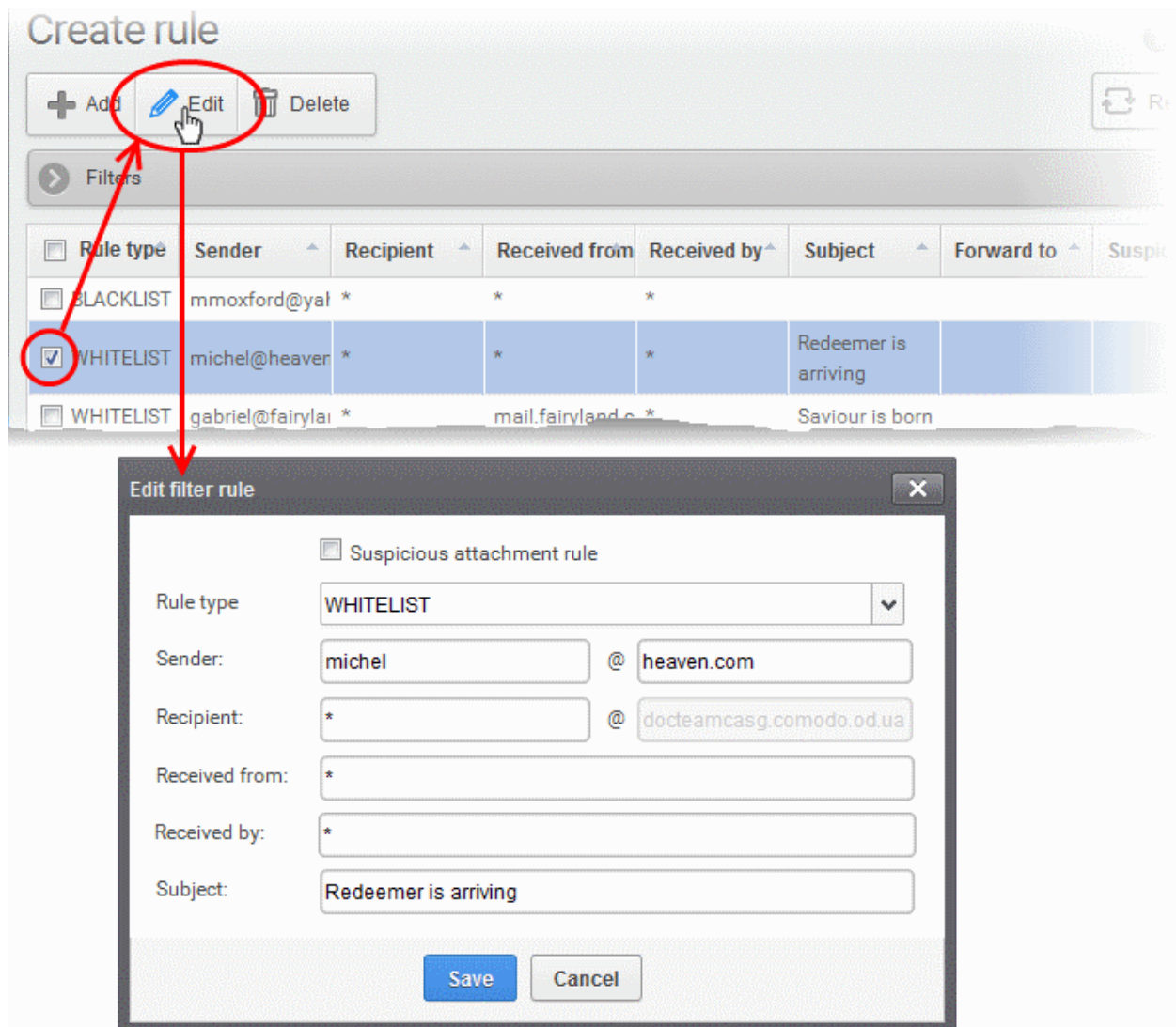


To edit a rule

- Click the 'Domain Rules' tab from the left of the 'Domain Management' interface and choose the 'Create rule' sub tab.

The list of rules configured for the domain will be displayed.

- Select the rule to be edited and click the 'Edit' button from the top.



The 'Edit filter rule' dialog will appear for the rule. This dialog is similar to Add Rule dialog. For descriptions of the options in this dialog, refer to the explanation [above](#).

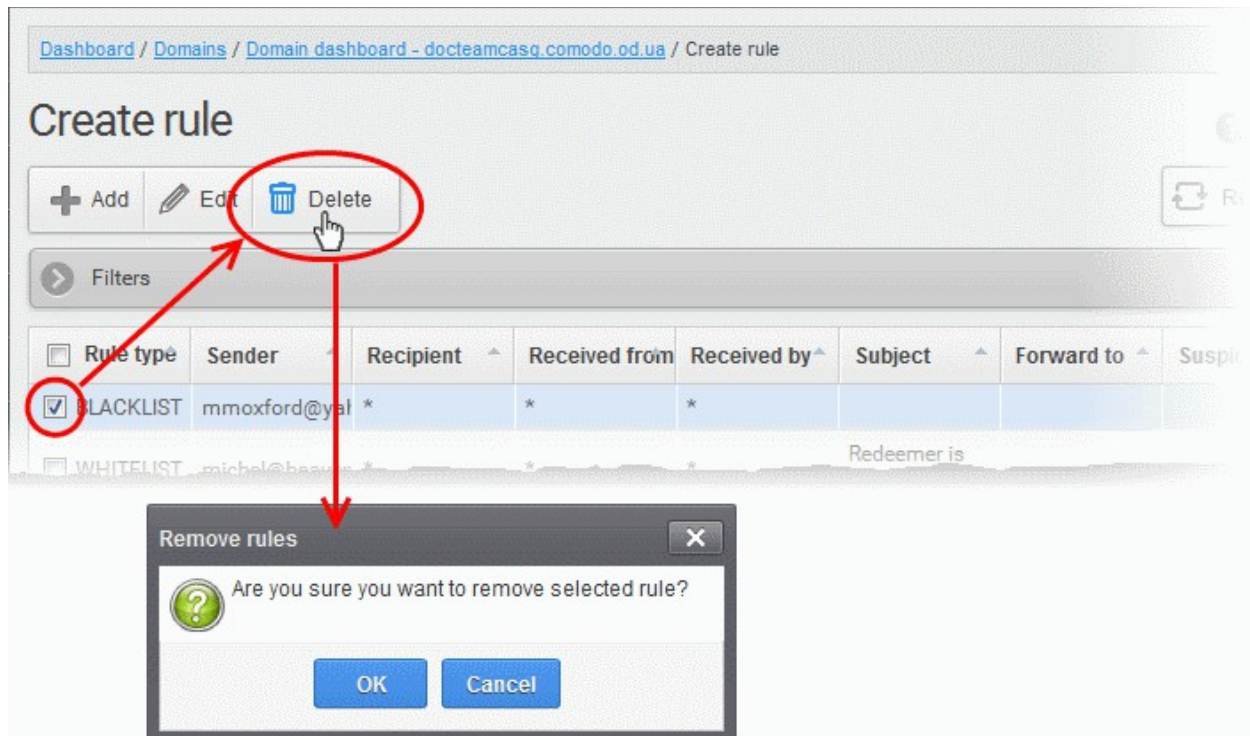
- Edit the values in the fields as required and click 'Save'.

To remove a rule

- Click the 'Domain Rules' tab from the left of the 'Domain Management' interface and choose the 'Create rule' sub tab.

The list of rules configured for the domain will be displayed.

- Select the rule to be removed and click the 'Delete' button from the top.



A confirmation dialog will appear.

- Click 'OK' to remove the rule.

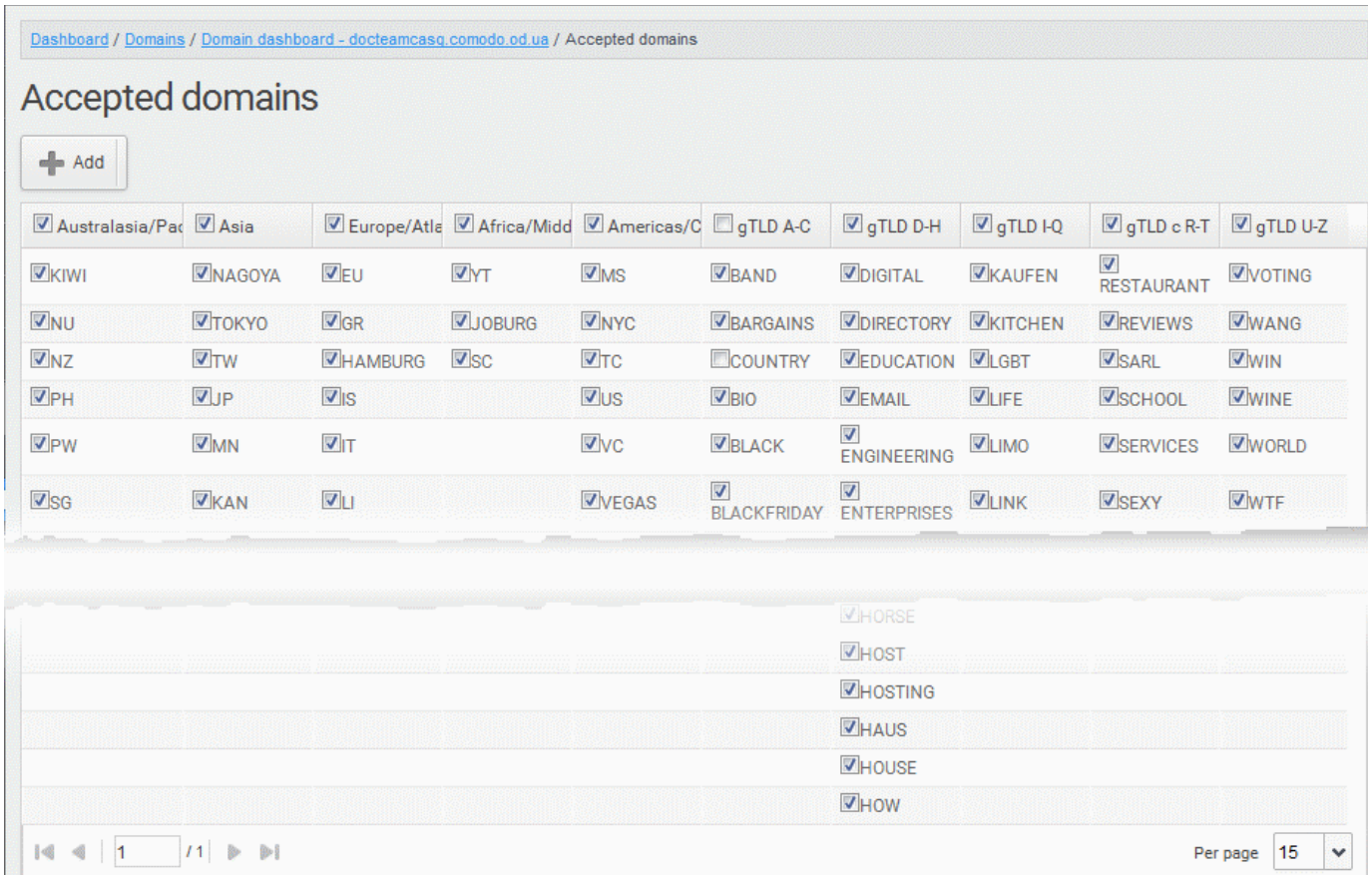
TLD and gTLD Rules

CASG allows administrators to restrict mails based on top level domain (TLD) names of mail servers. By default CASG accepts mails from servers with all TLD names. Administrators can choose to allow mails only from selected TLDs and block mails from others. Administrators can also add custom TLDs and configure to accept or block mails from them.

The 'TLD and gTLD Rules' interface displays the list of TLDs for the administrator to select TLDs from which the mails can be allowed.

To open the TLD and gTLD Rules interface

- Click the 'Domain Rules' tab from the left and choose the 'TLD and gTLD Rules' sub tab.

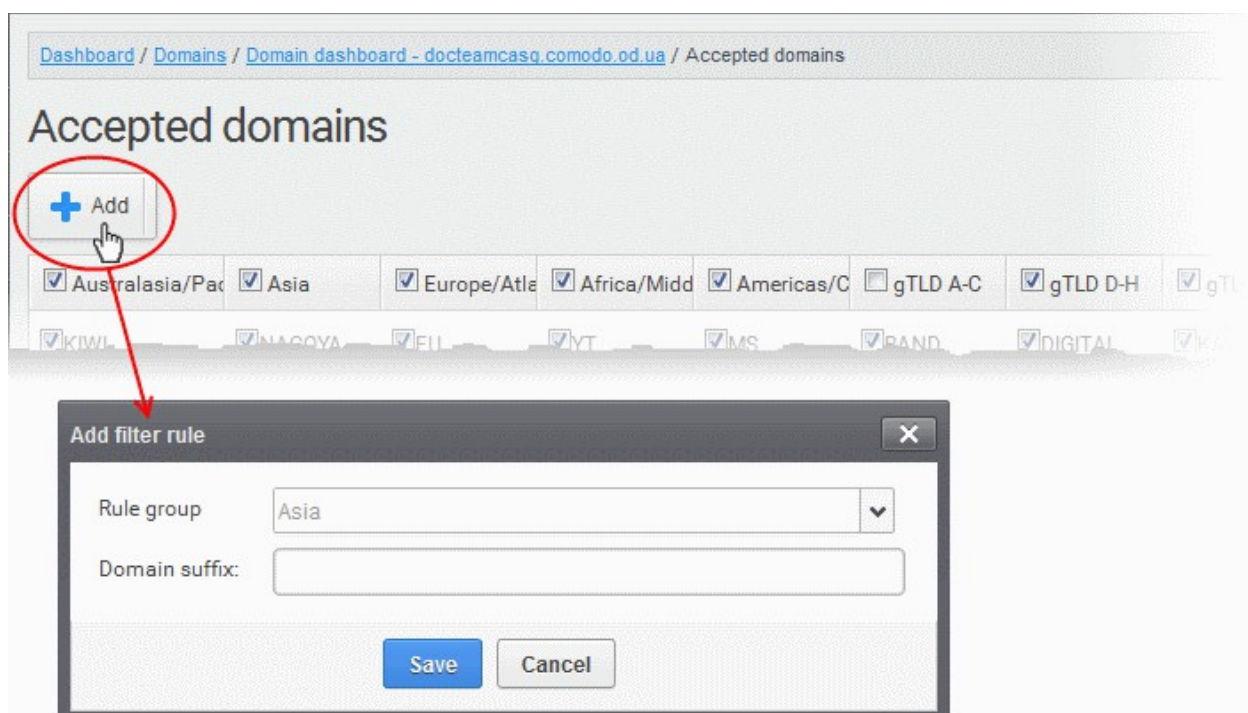


The 'Accepted domains' interface displays groups of TLDs under geographical location categories and alphabetical order. All TLDs are selected by default. The interface allows the administrator to:

- **Add new custom TLDs**
- **Configure TLD based mail filtering**

To add new custom TLDs

- Click 'Add' from the Accepted domains interface



The 'Add filter rule dialog' will appear.

- Choose the category from the Rule group drop-down
- Enter the TLD name, without the '.' prefix, in the Domain suffix text field
- Click Save to add the TLD to the list
 - To allow the emails from mail servers with the new TLD, leave it selected
 - To block the emails from the mail servers with the new TLD, de-select it.

To configure TLD based mail filter

- Deselect the TLDs from which you wish to block emails and leave allowed TLDs selected.

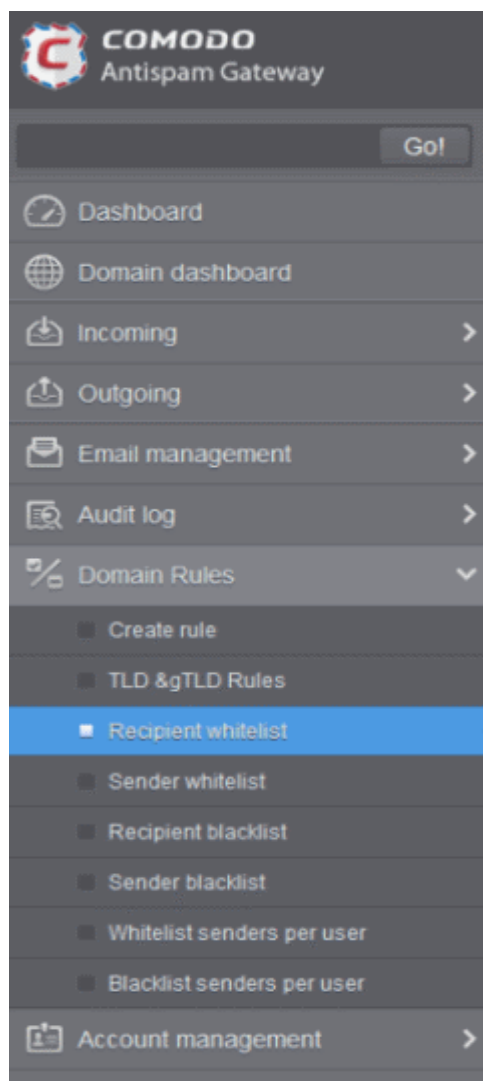
Recipient Whitelist

Since all filtering checks for the whitelisted recipients are disabled, CASG recommends to use the option only for certain cases such as postmaster or abuse@domain.com. The Administrator can:

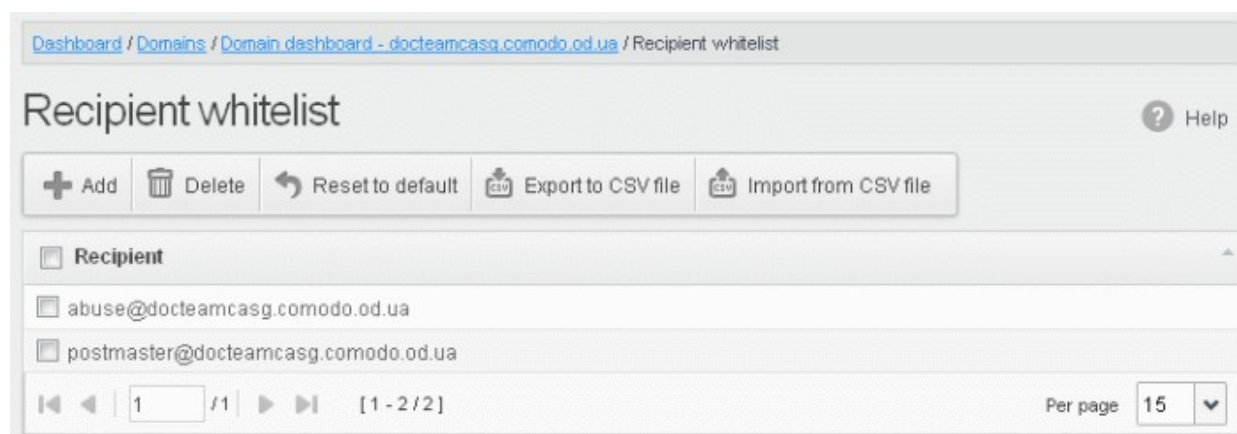
- **Add users to recipient whitelist**
- **Export the list to CSV file for use in future**
- **Remove users from recipient whitelist**
- **Reset the list** - Delete all whitelisted recipients except the default recipients by clicking the 'Reset to default' button

To configure recipient whitelist

- Click the 'Domain Rules' tab on the left hand side navigation to expand and then click the 'Recipient whitelist' sub tab.



The 'Recipient whitelist' interface of the selected domain will be displayed:



By default, the selected domain will have 'abuse' and 'postmaster' as whitelisted recipients.

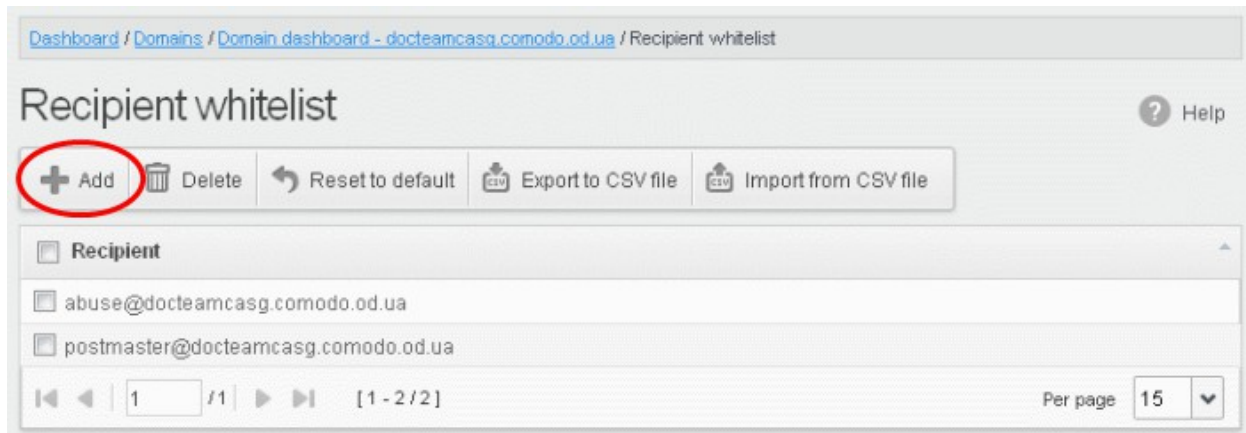
Adding Users to Recipient List

You can add recipients to white list in the following ways:

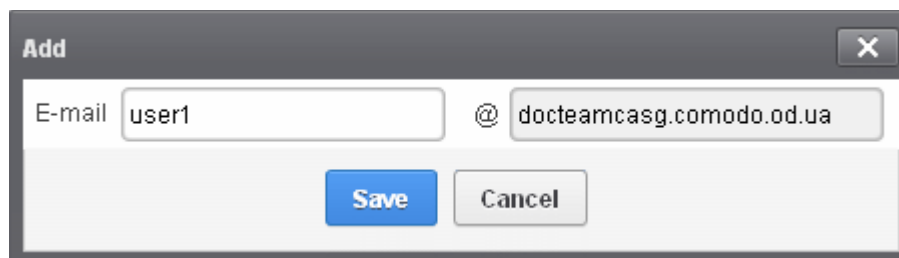
- **Manually adding the recipients**
- **Importing from a CSV file**

To manually add recipients

- Click 'Add' to add a new user to the list

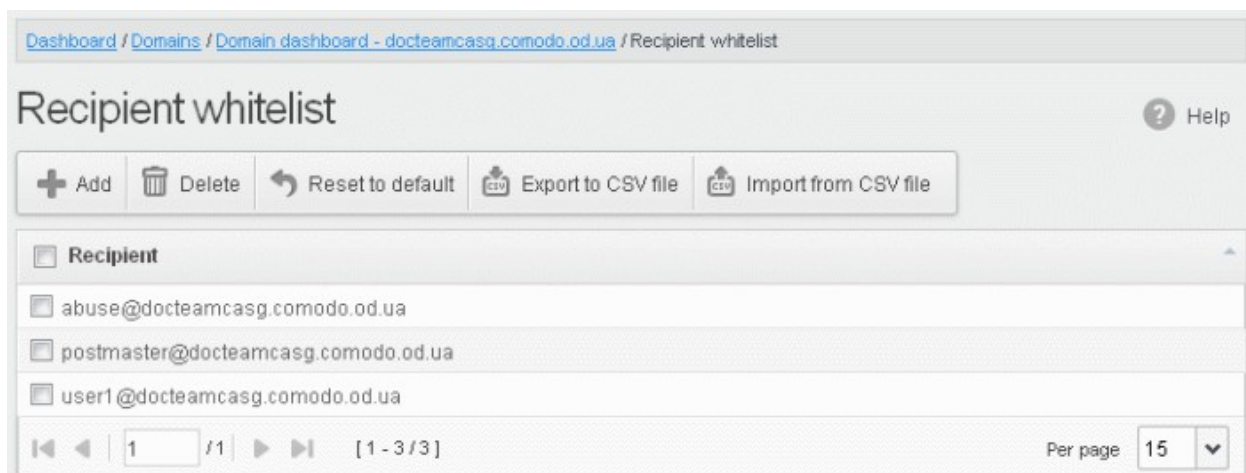


The 'Add' dialog box will be displayed:



- Enter the recipient's name in the E-mail text field and click the 'Save' button.
- To add a particular set of recipients to whitelist, prefix or suffix the wildcard * in the E-mail text field. For example, enter *.stores for all the recipients in stores department to be whitelisted.
- To add a whole domain to whitelist, enter the wildcard * in the E-mail text field and click the 'Save' button. Now all the recipients in that domain will be whitelisted.

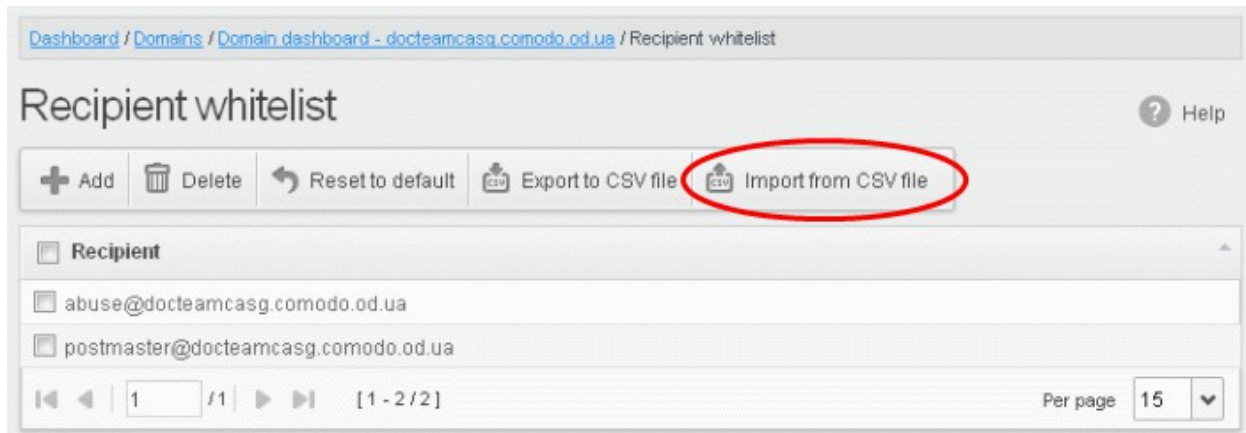
The recipient's name will be added to the list.



To import users to whitelist from CSV file

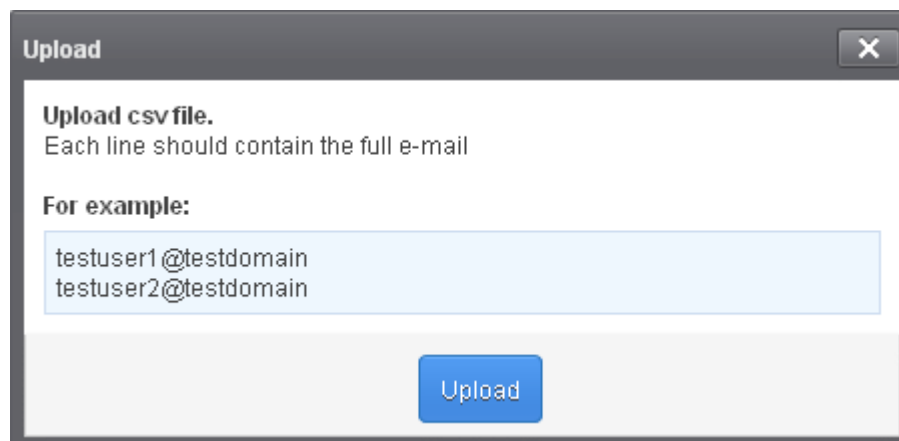
Administrators can import many users from a file to Recipient whitelist at a time. The users should be saved in the

format shown below as an example:
user1@testdomain
user2@testdomain
user3@testdomain



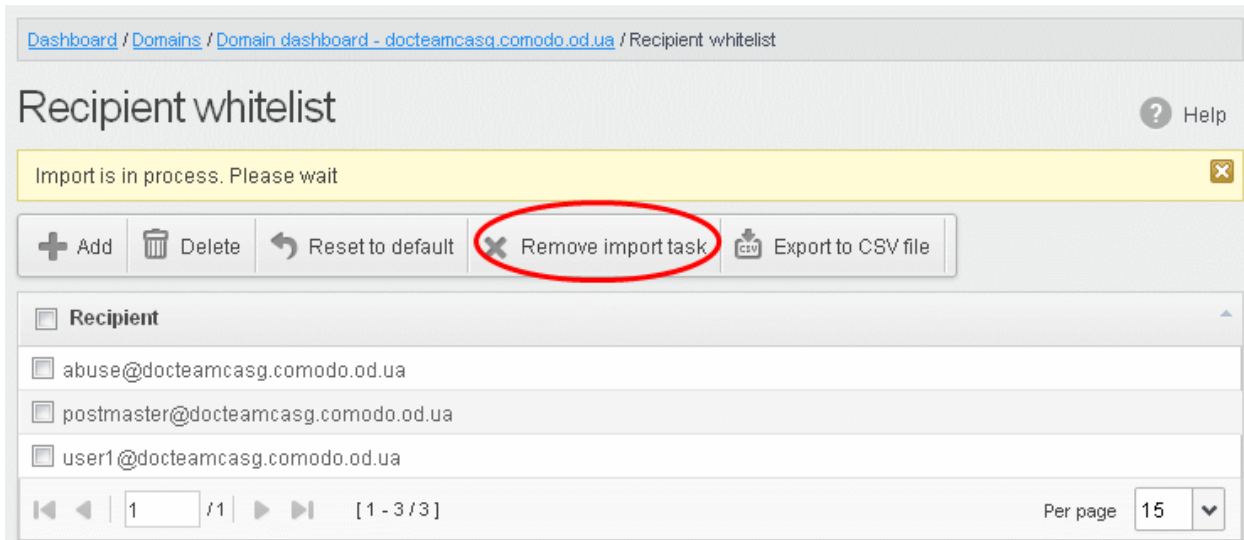
- Click the 'Import from CSV file' to import users to whitelist from a CSV file

The Upload dialog will be displayed.



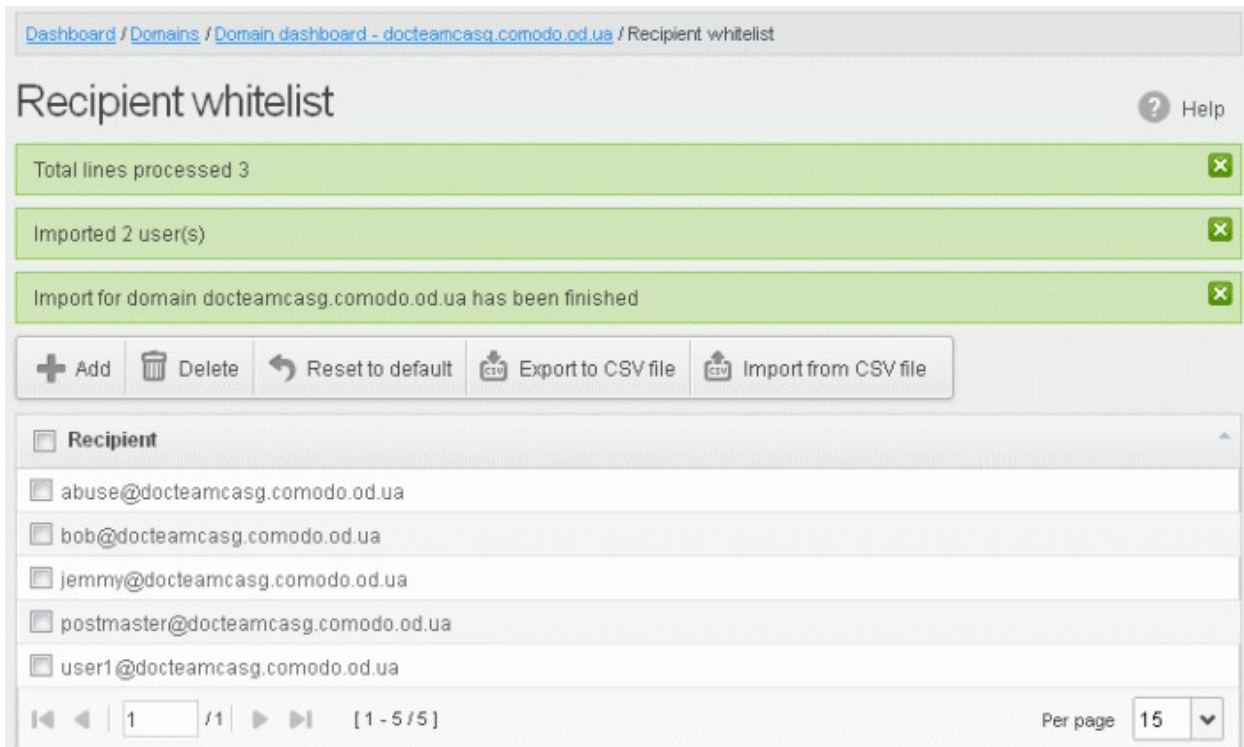
- Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



The screenshot shows the 'Recipient whitelist' page. At the top, a breadcrumb trail reads: Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Recipient whitelist. The page title is 'Recipient whitelist' with a help icon. A yellow notification bar at the top states 'Import is in process. Please wait'. Below this is a toolbar with buttons: '+ Add', 'Delete', 'Reset to default', 'Remove import task' (circled in red), and 'Export to CSV file'. The main content area is titled 'Recipient' and contains a table with three rows of email addresses: abuse@docteamcasg.comodo.od.ua, postmaster@docteamcasg.comodo.od.ua, and user1@docteamcasg.comodo.od.ua. At the bottom, there are pagination controls showing '1 / 1' and '[1 - 3 / 3]', and a 'Per page' dropdown set to '15'.

On completion of the upload process, the results will be displayed.



The screenshot shows the 'Recipient whitelist' page after a successful import. The breadcrumb trail is the same. The page title is 'Recipient whitelist' with a help icon. Three green notification bars are visible: 'Total lines processed 3', 'Imported 2 user(s)', and 'Import for domain docteamcasg.comodo.od.ua has been finished'. The toolbar now includes '+ Add', 'Delete', 'Reset to default', 'Export to CSV file', and 'Import from CSV file'. The main content area is titled 'Recipient' and contains a table with five rows of email addresses: abuse@docteamcasg.comodo.od.ua, bob@docteamcasg.comodo.od.ua, jemmy@docteamcasg.comodo.od.ua, postmaster@docteamcasg.comodo.od.ua, and user1@docteamcasg.comodo.od.ua. At the bottom, the pagination controls show '1 / 1' and '[1 - 5 / 5]', and the 'Per page' dropdown is still set to '15'.

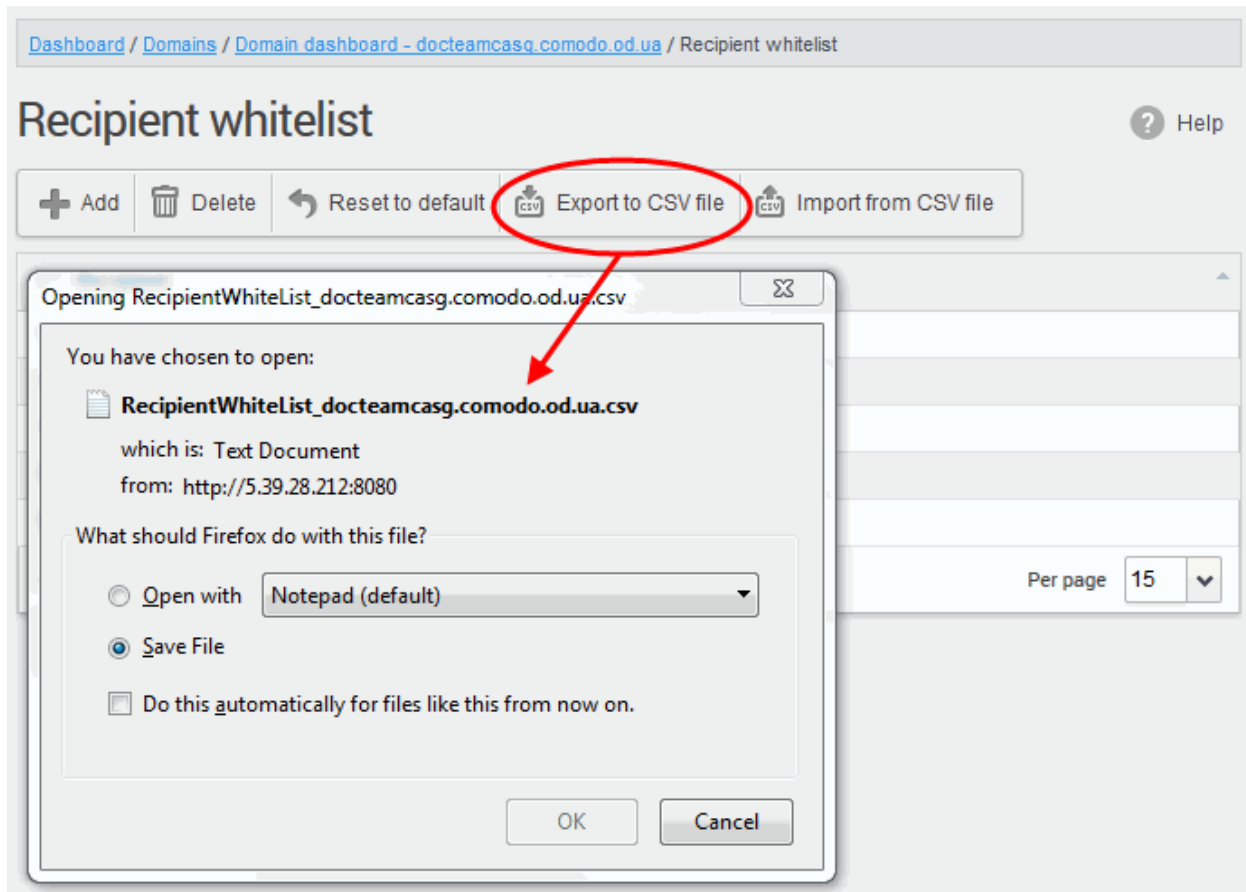
The recipient whiteslist from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

Exporting the Recipient Whitelist to CSV file

The administrator can save the configured recipient whitelist by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

To export the list

- Click the 'Export to CSV file' button to save the list of whitelisted recipients as a CSV file

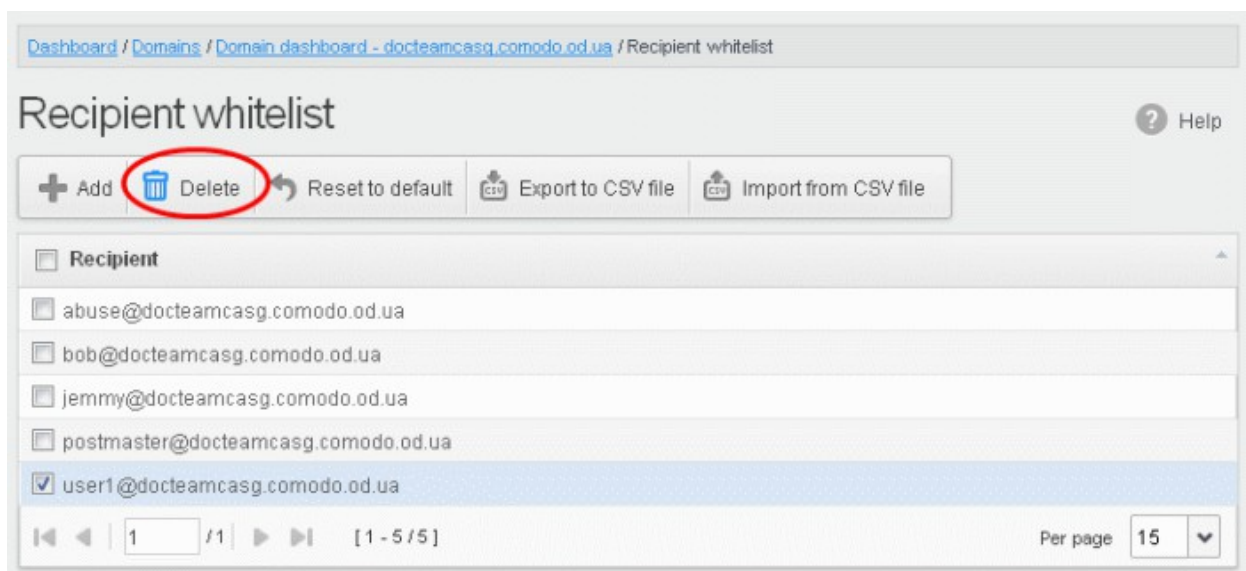


A file download dialog will be displayed.

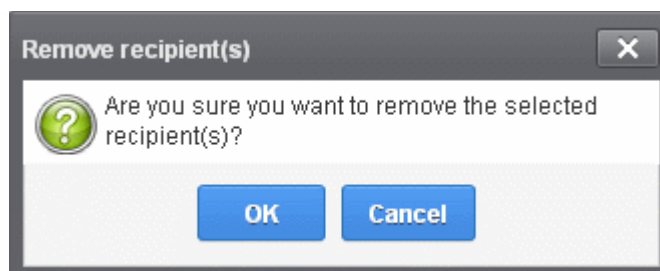
- Click 'OK' and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

Deleting Users from the Recipient Whitelist

- To delete a recipient from the whitelist, select the recipient from the list and click the 'Delete' button



- Click 'OK' to confirm your changes



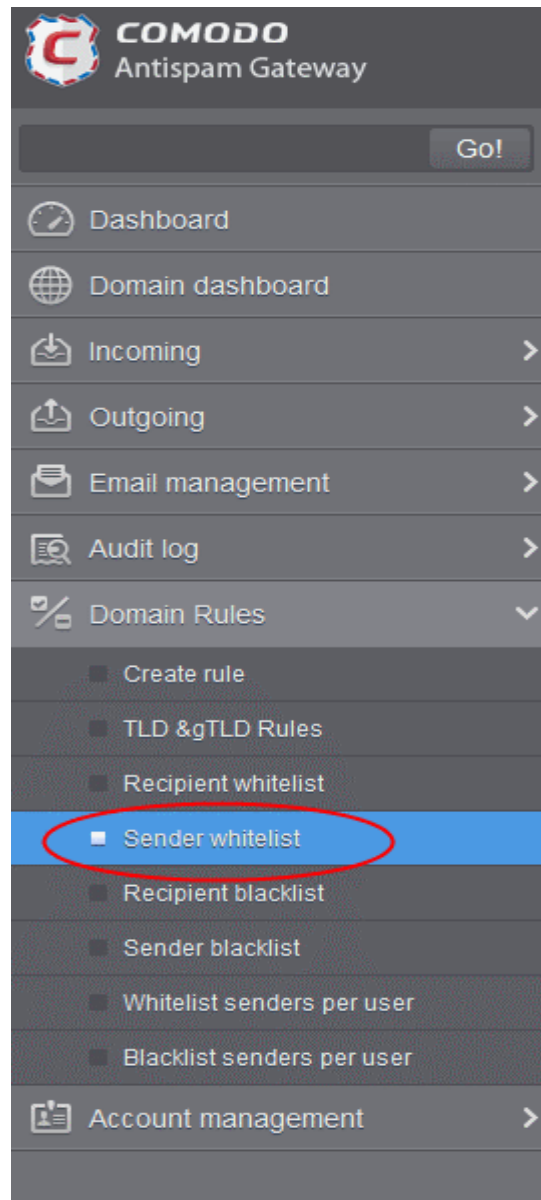
Sender Whitelist

All filtering is disabled for whitelisted senders of mail to recipients at the selected domain. Comodo strongly recommends to use this option only when the system wrongly blocks emails from a certain trusted sender. Whitelisted senders for a domain over-rules 'Blacklist senders per user'. Refer to the section **Blacklist Senders Per User** for more details. The Administrator can:

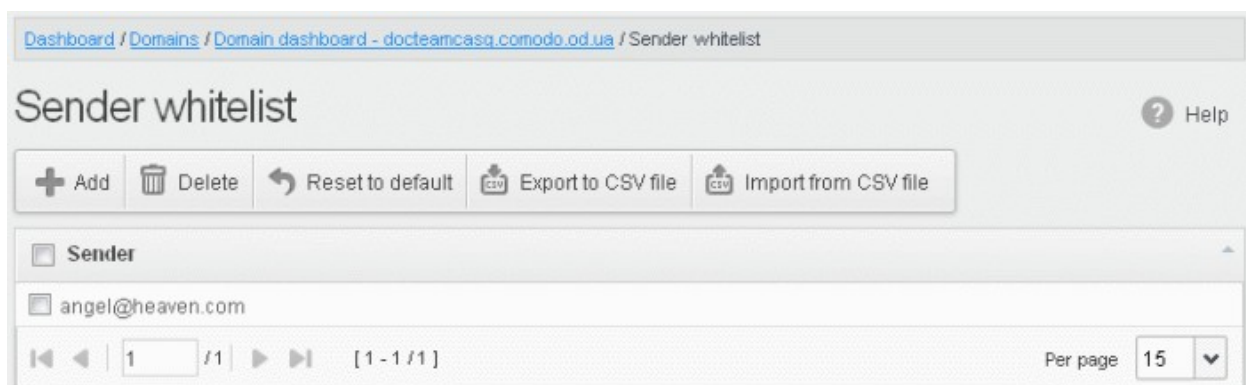
- **Add users to Sender whitelist**
- **Export the list to CSV file for use in future**
- **Remove users from Sender whitelist**
- **Reset the list** - Delete all whitelisted senders and make the list empty by clicking the 'Reset to default' button

To configure sender whitelist

- Click the 'Whitelist / Blacklist' tab on the left hand side navigation to expand and then click the 'Sender whitelist' sub tab.



The 'Sender whitelist' interface of the selected domain will be displayed:



Adding Users to Sender Whitelist

You can add recipients to white list in the following ways:

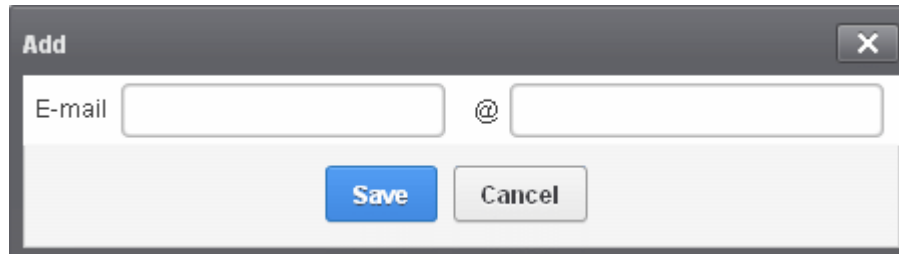
- **Manually adding the senders**

- **Importing from a CSV file**

To manually add senders

- Click 'Add' to add a new whitelisted sender

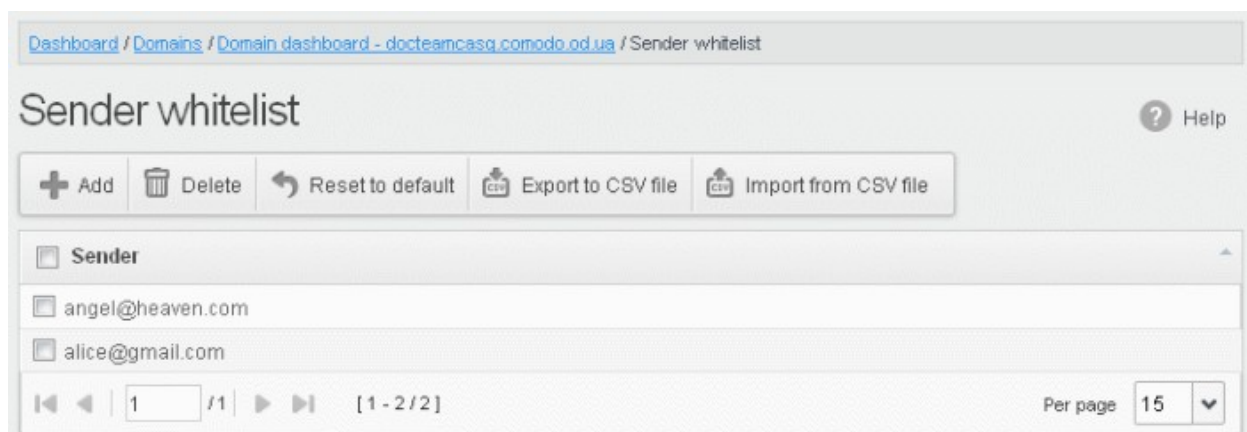
The 'Add' dialog box will be displayed:



The 'Add' dialog box is a small window with a title bar containing the word 'Add' and a close button (X). It features two text input fields: the first is labeled 'E-mail' and the second is preceded by an '@' symbol. Below the input fields are two buttons: 'Save' (highlighted in blue) and 'Cancel'.

- Enter the sender name in the E-mail textbox and sender's email domain name after the @ symbol and click the 'Save' button. Repeat the process to add more whitelisted senders.
- To add a particular set of senders to whitelist, prefix or suffix the wildcard character * in the E-mail text field and senders' email domain name after the @ symbol. For example, enter *stores.com for all the senders in stores department to be whitelisted.
- To add a specific username from any mail domain to the whitelist, enter the username in the mail text field and the wildcard character * after the @ symbol. For example, enter john@* for whitelisting the username 'john' with any email domain name.
- To add a set of users or specific username from any email domain with a specific top level domain (TLD) name like .com, .org, enter the wildcard character * or username in the Email text field and enter * followed by the TLD after the @ symbol. For example, '*@*.com' will whitelist all the senders from all the email domains ending with '.com'.
- To add a whole domain to whitelist, enter the wildcard character * in the E-mail text field and email domain after the @ symbol and click the 'Save' button. Now all the senders with the entered domain name will be whitelisted.

The list of whitelisted senders will be displayed.



The screenshot shows the 'Sender whitelist' interface. At the top, there is a breadcrumb trail: 'Dashboard / Domains / Domain dashboard - docteamcasq.comodo.od.ua / Sender whitelist'. Below this is the title 'Sender whitelist' and a 'Help' button. A toolbar contains five icons: '+ Add', 'Delete', 'Reset to default', 'Export to CSV file', and 'Import from CSV file'. Below the toolbar is a table with a header 'Sender' and two rows of data: 'angel@heaven.com' and 'alice@gmail.com'. At the bottom, there is a pagination control showing '1 / 1' and '[1 - 2 / 2]', and a 'Per page' dropdown set to '15'.

To import senders to whitelist from CSV file

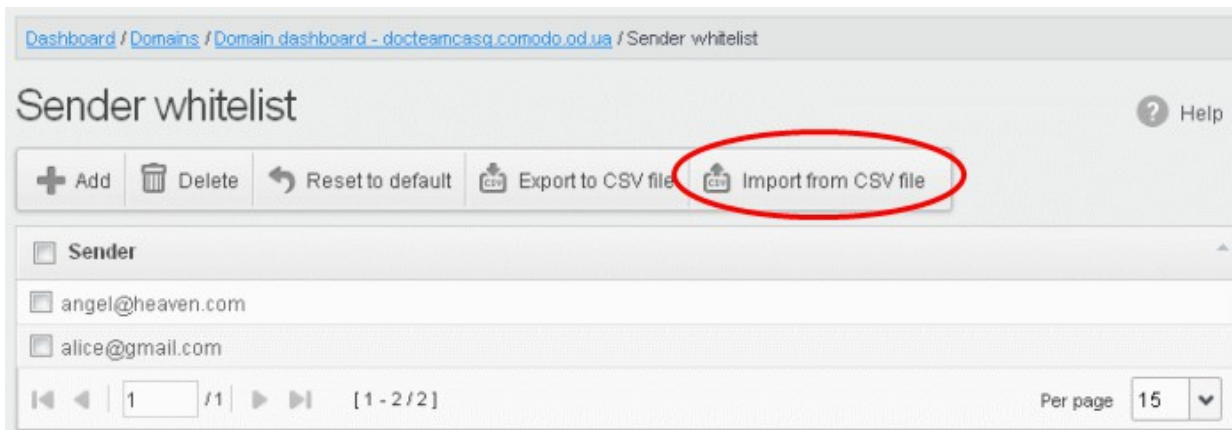
Administrators can import many senders from a file to Sender whitelist at a time. The senders' address should be saved in the format shown below as an example:

sender1@domainname1

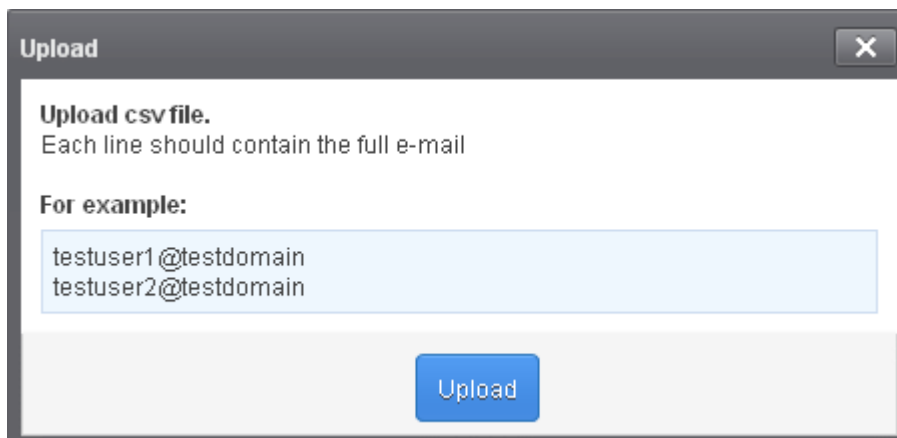
sender2@domainname2

sender3@domainname3

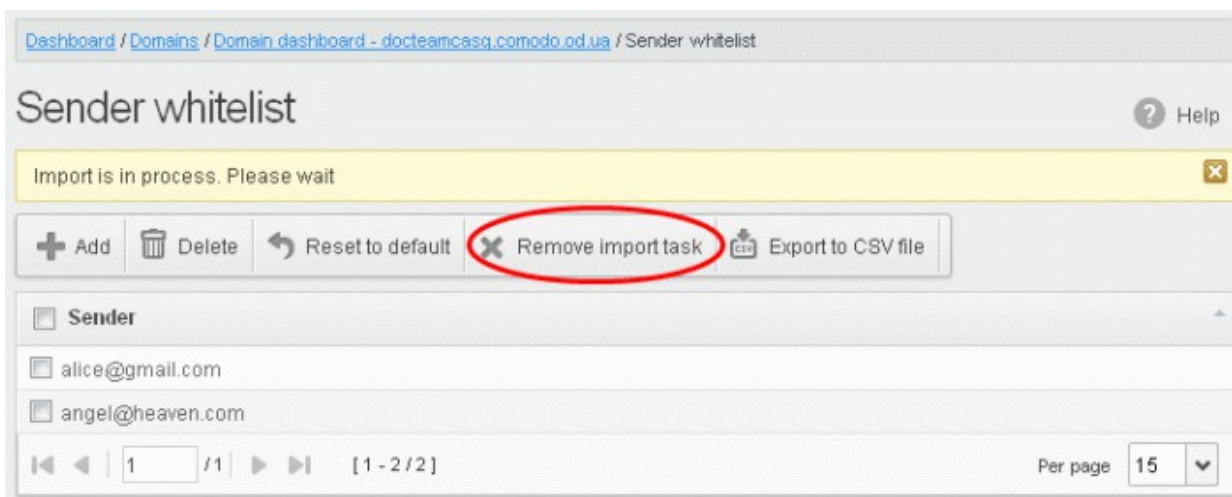
- Click the 'Import from CSV file' to import senders to whitelist from a CSV file.



- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.



The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, the results will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Sender whitelist

Sender whitelist Help

Total lines processed 4

Imported 3 user(s)

Import for domain docteamcasg.comodo.od.ua has been finished

+ Add Delete Reset to default Export to CSV file Import from CSV file

<input type="checkbox"/> Sender
<input type="checkbox"/> alice@gmail.com
<input type="checkbox"/> angel@heaven.com
<input type="checkbox"/> falcon@hotmail.com
<input type="checkbox"/> smith@rediff.com
<input type="checkbox"/> wilecoyte696@yahoo.com

1 / 1 [1 - 5 / 5] Per page 15

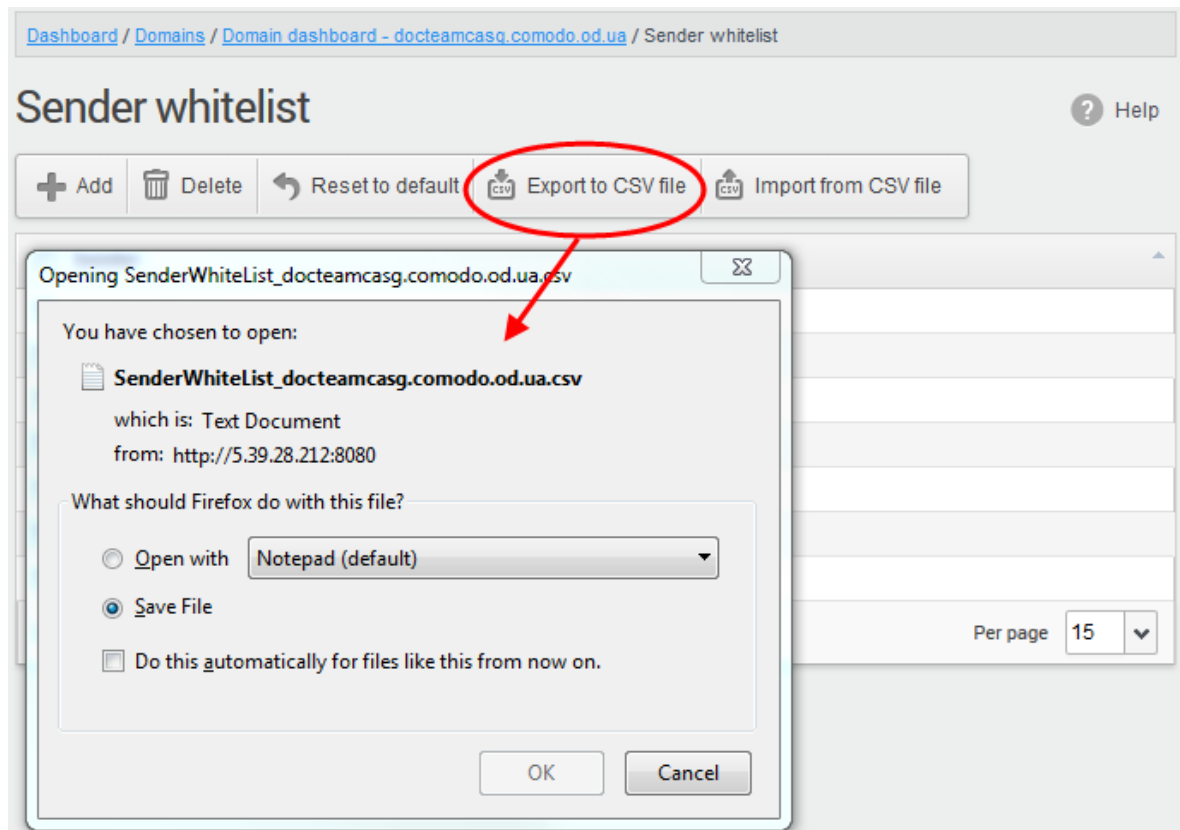
The sender whietlist from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

Exporting the Sender Whitelist to CSV file

The administrator can save the configured sender whitelist by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

To export the list

- Click the 'Export to CSV file' to save the list of whitelisted senders as a CSV file

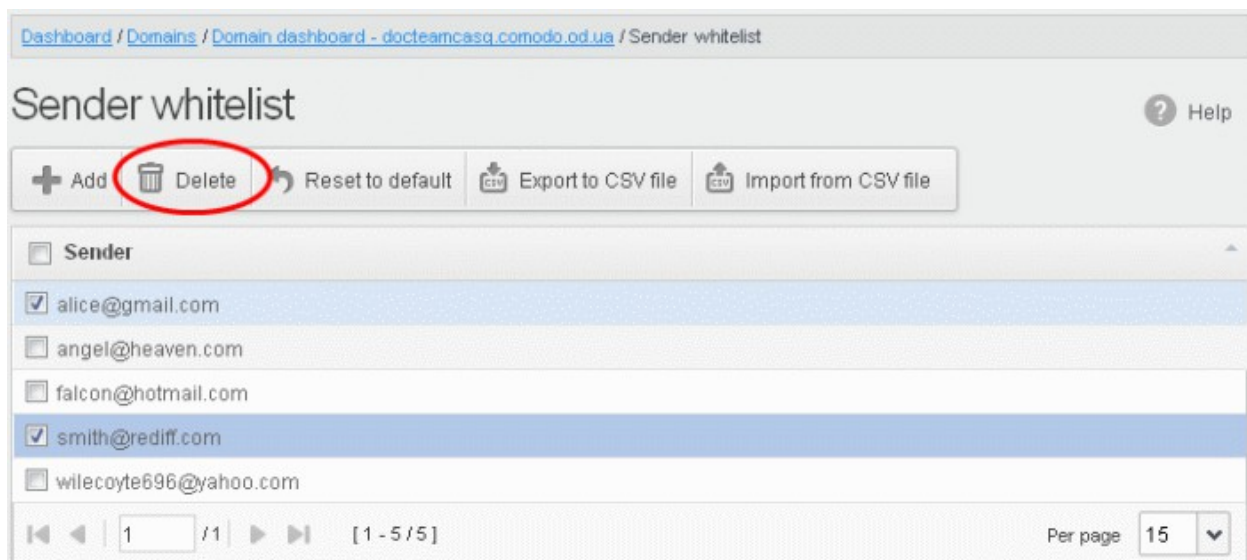


A file download dialog will be displayed.

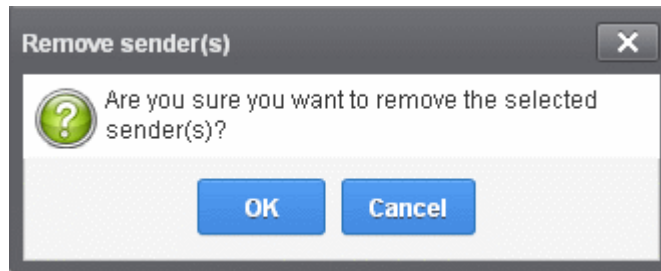
- Click 'OK' and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

Deleting Users from the Sender Whitelist

- To delete a sender from the whitelist, select the sender from the list and click the 'Delete' button.



- Click 'OK' to confirm your changes.



Recipient Blacklist

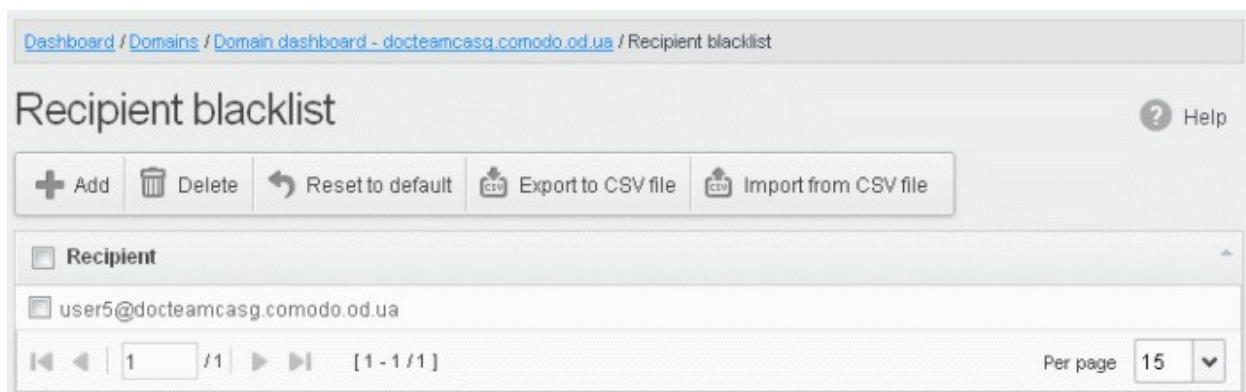
CASG will automatically block all emails to blacklisted recipients. Please note that the messages will not be quarantined and legitimate email sending SMTP servers will send a bounce message to the sender. The Administrator can:

- **Add users to recipient blacklist**
- **Export the list to CSV file for use in future**
- **Remove users from recipient blacklist**
- **Reset the list** - Delete all blacklisted senders and make the list empty by clicking the 'Reset to default' button

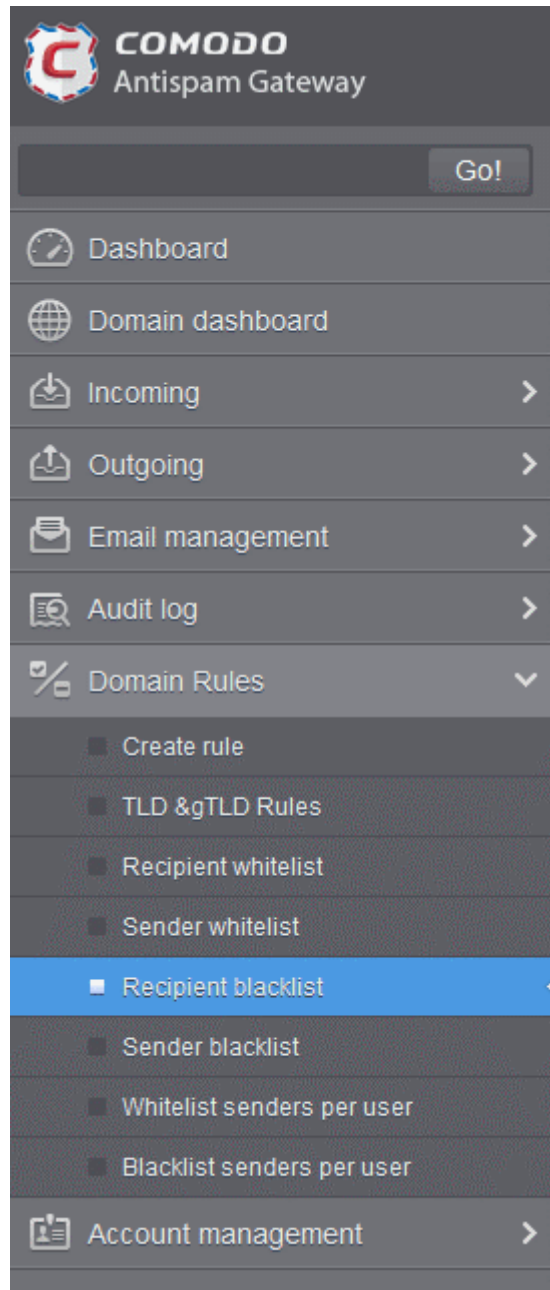
To configure recipient blacklist

- Click the 'Whitelist / Blacklist' tab on the left hand side navigation to expand and then click the 'Recipient blacklist' sub tab.

The 'Recipient blacklist' interface of the selected domain will be displayed:



Adding Users to Recipient Blacklist



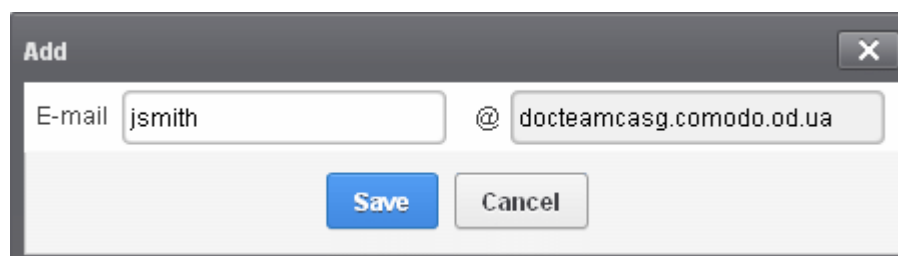
You can add recipients to the black list in the following ways:

- **Manually adding the recipients**
- **Importing from a CSV file**

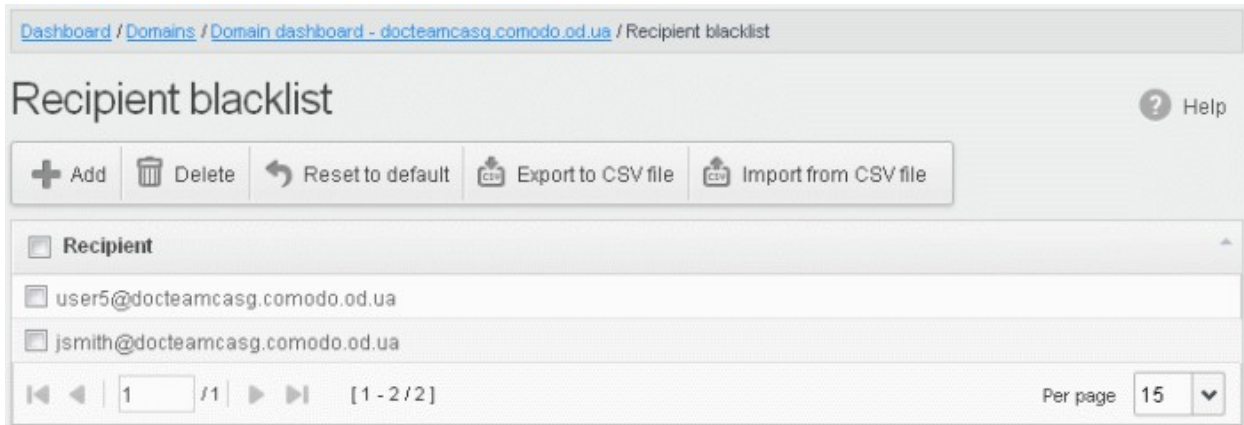
To manually add recipients

- Click 'Add' to add a new user to the list

The 'Add' dialog box will open.



- Enter the recipient name in the E-mail textbox and click the 'Save' button. Repeat the process to add more recipients to blacklist.
- To add a particular set of recipients to blacklist, prefix or suffix the wildcard * in the E-mail text field. For example, enter *.stores for all the recipients in stores department to be blacklisted.
- To add a whole domain to blacklist, enter the wildcard * in the E-mail text field and click the 'Save' button. Now all the recipients in that domain will be blacklisted.



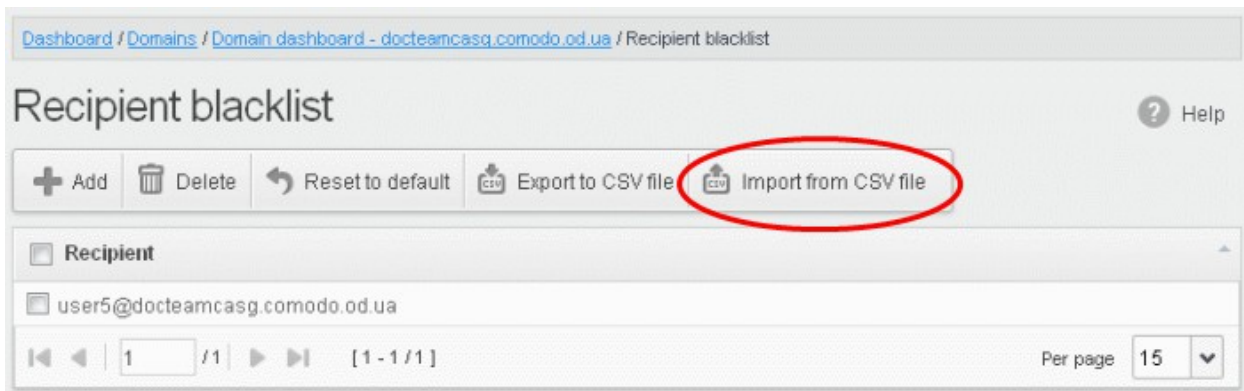
The list of blacklisted recipients will be displayed.

To import users to blacklist from CSV file

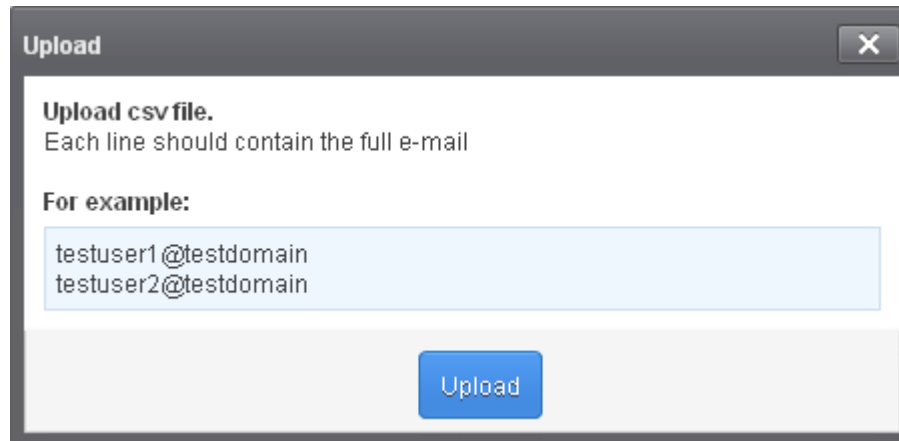
Administrators can import many users from a file to Recipient blacklist at a time. The users should be saved in the format shown below as an example:

```
user1@testdomain  
user2@testdomain  
user3@testdomain
```

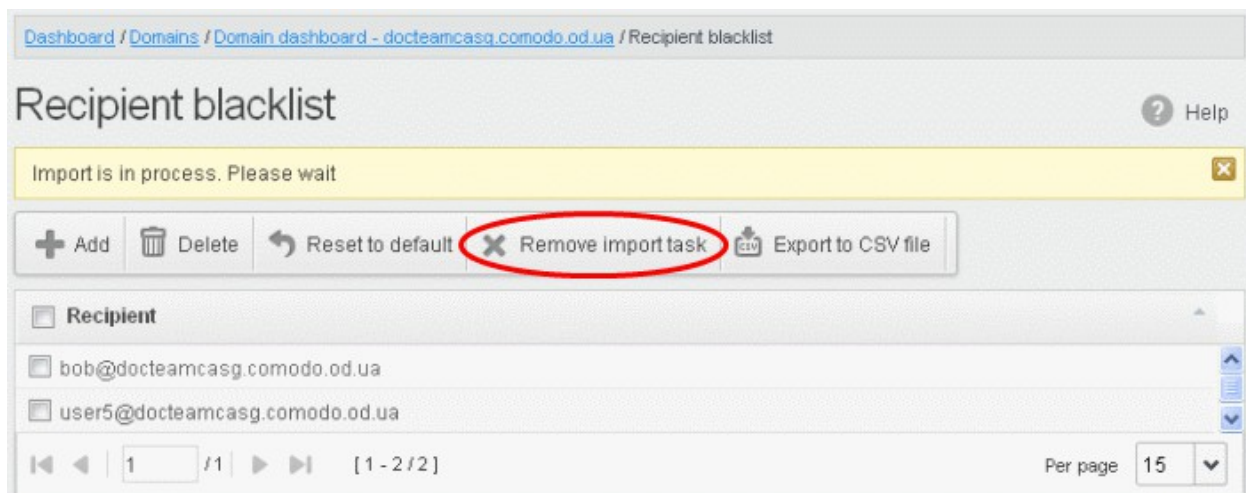
- Click the 'Import from CSV file' button to import users to blacklist from a CSV file.



- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.



The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, the results will be displayed.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Recipient blacklist

Recipient blacklist Help

Total lines processed 4 ✕

Imported 4 user(s) ✕

Import for domain docteamcasg.comodo.od.ua has been finished ✕

+ Add 🗑 Delete ↶ Reset to default 📄 Export to CSV file 📄 Import from CSV file

<input type="checkbox"/> Recipient
<input type="checkbox"/> black@docteamcasg.comodo.od.ua
<input type="checkbox"/> bob@docteamcasg.comodo.od.ua
<input type="checkbox"/> duncan@docteamcasg.comodo.od.ua
<input type="checkbox"/> jsmith@docteamcasg.comodo.od.ua
<input type="checkbox"/> user5@docteamcasg.comodo.od.ua

1 / 1 [1 - 5 / 5] Per page 15

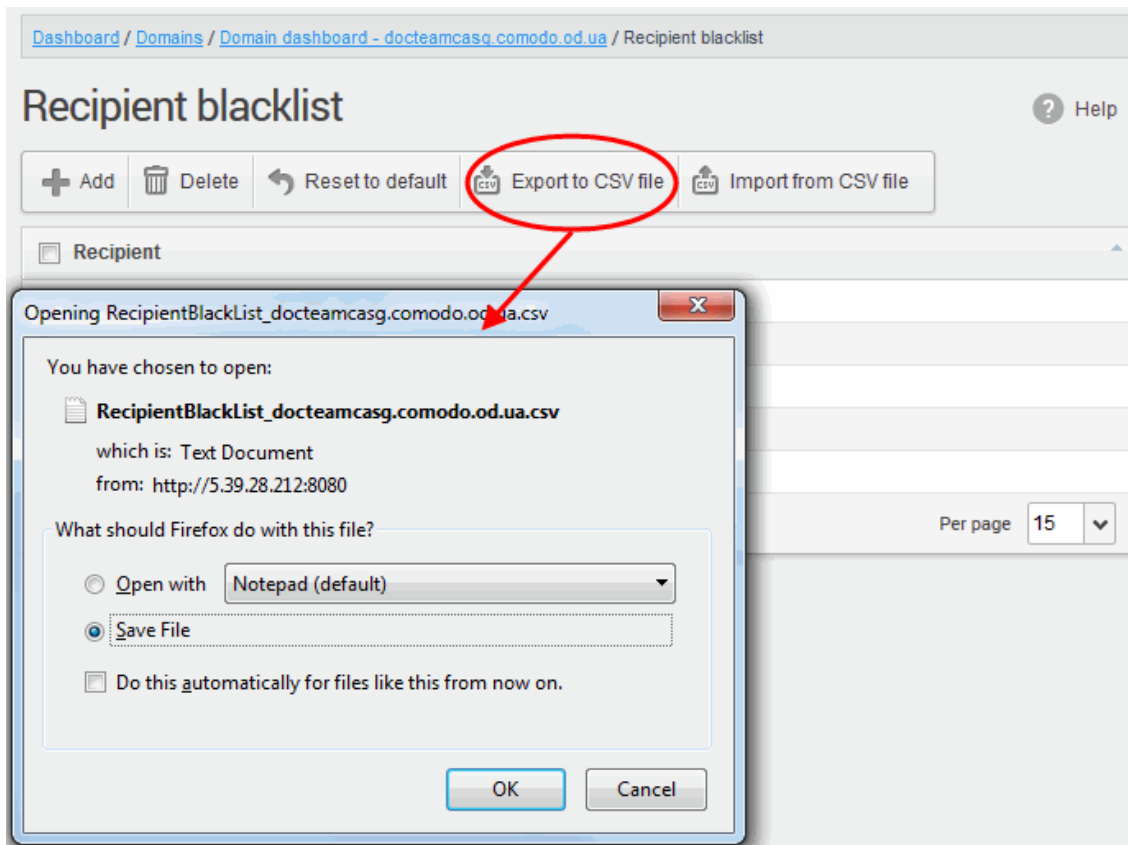
The recipient blacklist from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

Exporting the Recipient Blacklist to CSV file

The administrator can save the configured recipient blacklist by exporting it as a CSV file. If required in future, the administrator can import the users from the csv file, for example for a new account or after a reset.

To export the list

- Click the 'Export to CSV file' to save the list of blacklisted recipients as a CSV file

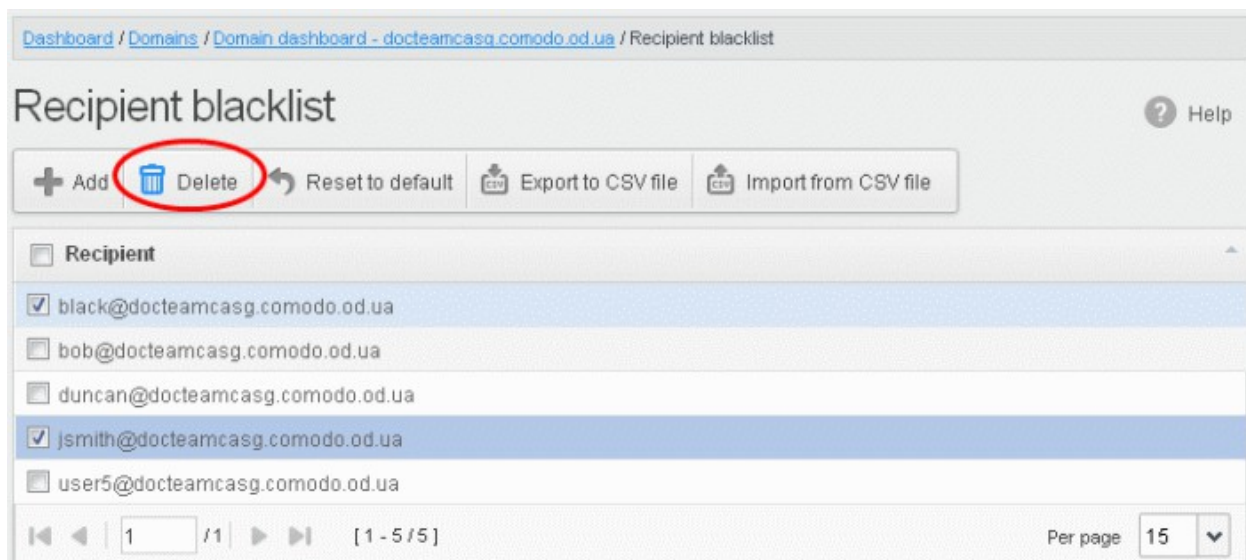


A file download dialog will be displayed.

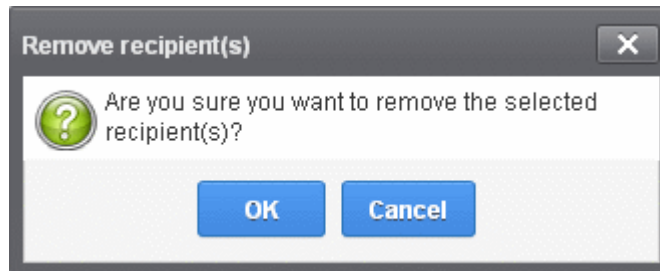
- Click 'OK' and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

Deleting Users from the Recipient Blacklist

- To delete a recipient from the blacklist, select the recipient from the list and click the 'Delete' button



- Click 'OK' to confirm your changes. The user will be removed from the blacklist and the mails addressed to the user will be allowed as per the existing filter settings in CASG.



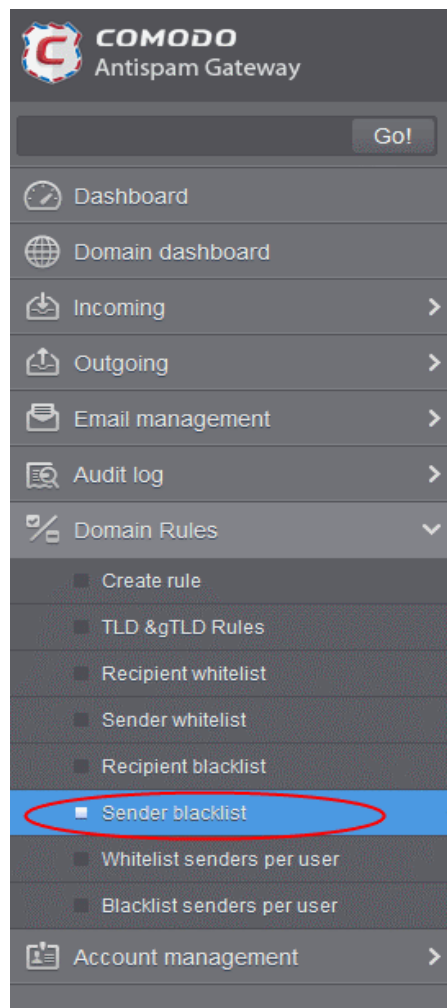
Sender Blacklist

CASG will automatically block all emails from blacklisted senders. Please note that the messages will not be quarantined and legitimate email sending SMTP servers will send a bounce message to the sender. The administrator can:

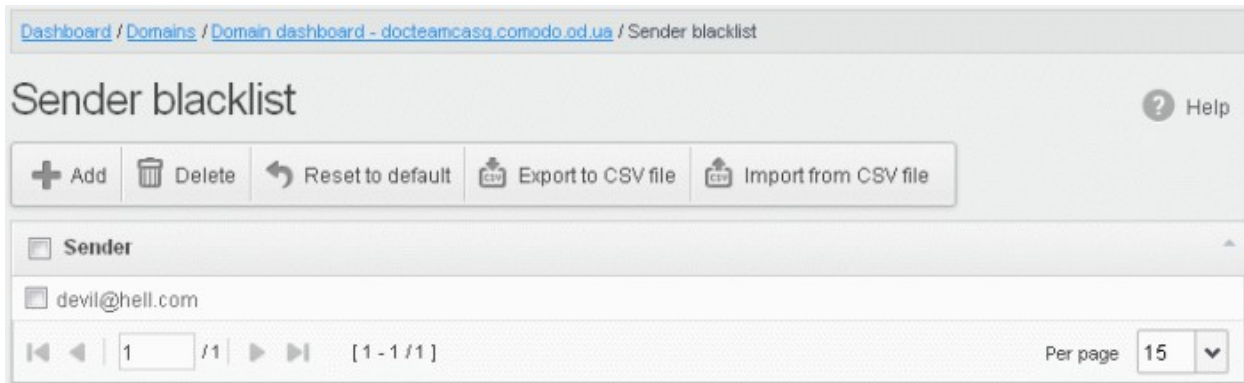
- **Add users to sender blacklist**
- **Export the list to CSV file for use in future**
- **Remove users from sender blacklist**
- **Reset the list** - Delete all blacklisted senders and make the list empty by clicking the 'Reset to default' button

To configure sender blacklist

- Click the 'Whitelist / Blacklist' tab on the left hand side navigation to expand and then click the 'Sender blacklist' sub tab.



The 'Sender blacklist' interface of the selected domain will be displayed:



Adding Users to Senders Blacklist

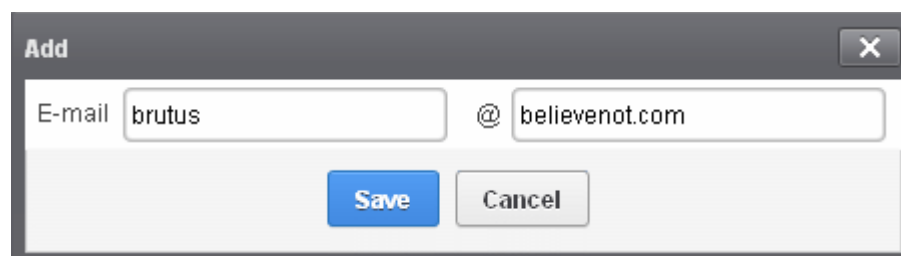
You can add senders to black list in the following ways:

- **Manually adding the senders**
- **Importing from a CSV file**

To manually add senders

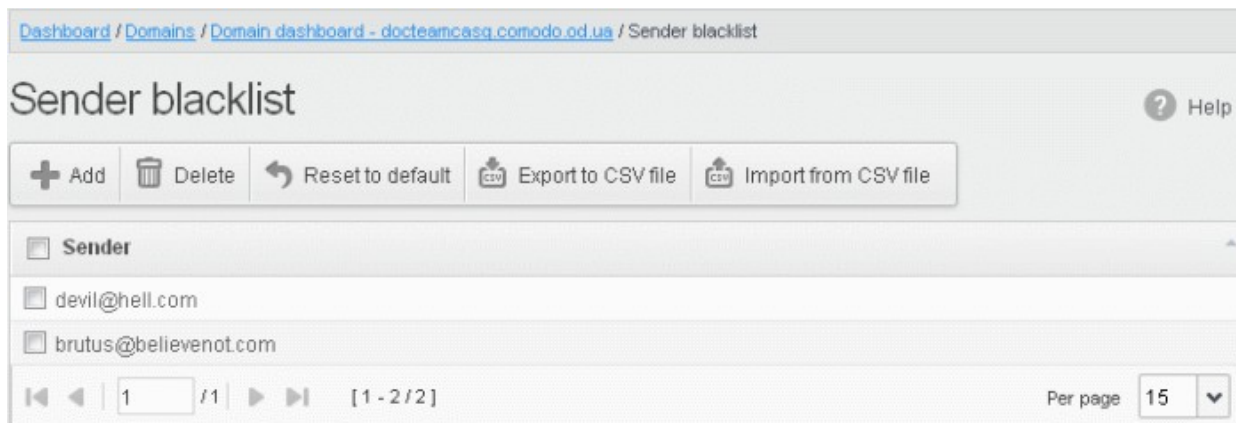
- Click 'Add' to add a new blacklisted sender

The 'Add' dialog box will be displayed:



- Enter the sender name in the E-mail textbox and sender's email domain name after the @ symbol and click the 'Save' button. Repeat the process to add more blacklisted senders.
- To add a particular set of senders to blacklist, prefix or suffix the wildcard character * in the E-mail text field and senders' email domain name after the @ symbol. For example, enter *stores.com for all the senders in stores department to be blacklisted.
- To add a specific username from any mail domain to the blacklist, enter the username in the mail text field and the wildcard character * after the @ symbol. For example, enter john@* for blacklisting the username 'john' with any email domain name.
- To add a set of users or specific username from any email domain with a specific top level domain (TLD) name like .com, .org, enter the wildcard character * or username in the Email text field and enter * followed by the TLD after the @ symbol. For example, '*@*.com' will whitelist all the senders from all the email domains ending with '.com'.
- To add a whole domain to whitelist, enter the wildcard character * in the E-mail text field and email domain after the @ symbol and click the 'Save' button. Now all the senders with the entered domain name will be whitelisted.
- To add a particular set of senders to blacklist, prefix or suffix the wildcard * in the E-mail text field and senders' email domain name after the @ symbol. For example, enter *.stores for all the senders in stores department to be blacklisted.
- To add a whole domain to blacklist, enter the wildcard * in the E-mail text field and email domain after the @

symbol and click the 'Save' button. Now all the senders with the domain name entered will be blacklisted. The list of blacklisted senders will be displayed.

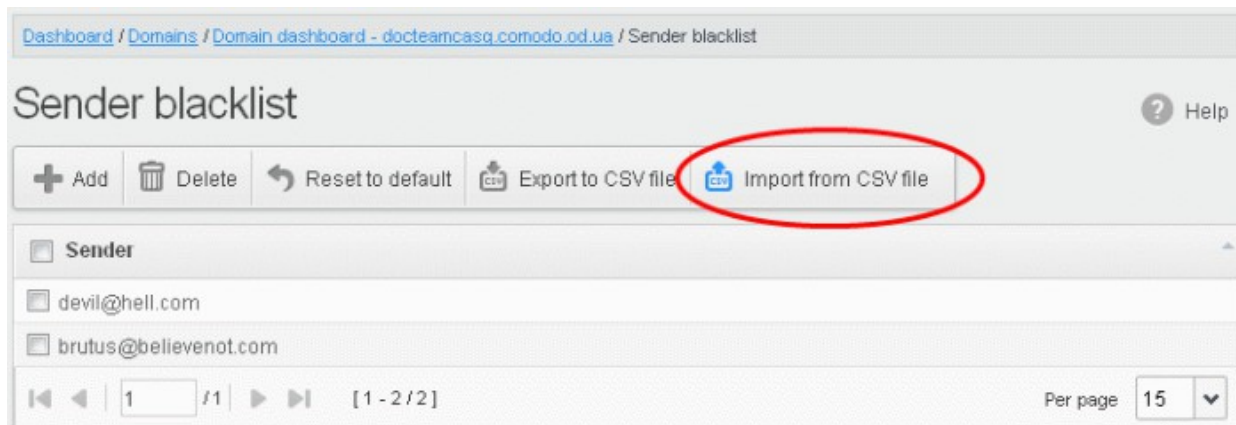


To import senders to blacklist from CSV file

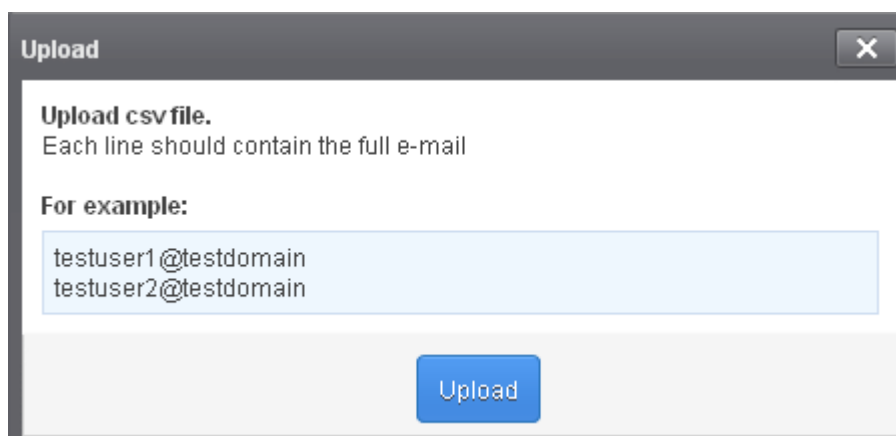
Administrators can import many senders from a file to Sender blacklist at a time. The senders' address should be saved in the format shown below as an example:

```
sender1@domainname1
sender2@domainname2
sender3@domainname3
```

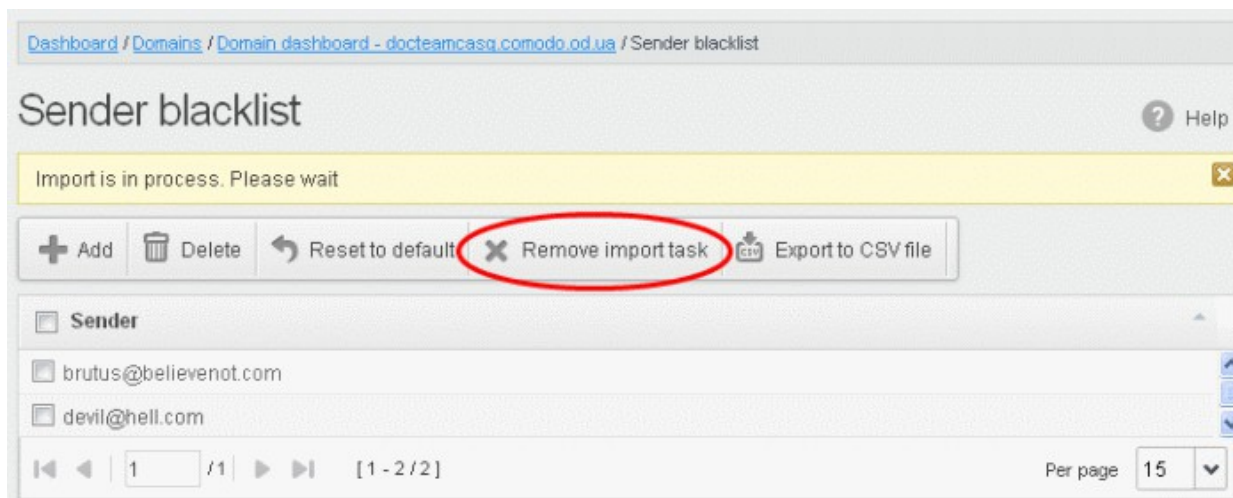
- Click the 'Import from CSV file' to import senders to blacklist from a CSV file.



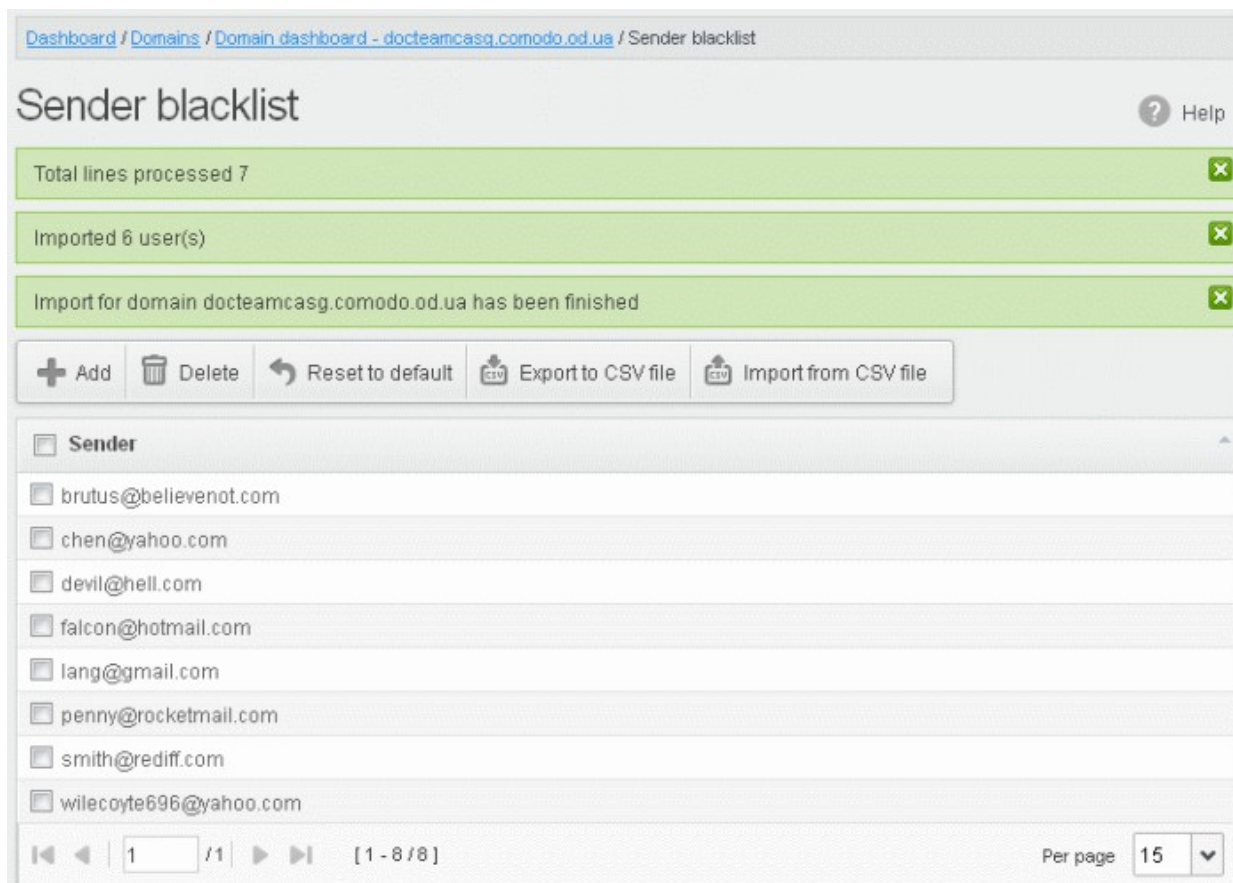
- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.



The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes *only* a remaining part of not imported task.



On completion of the upload process, the results will be displayed.



The sender blacklist from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

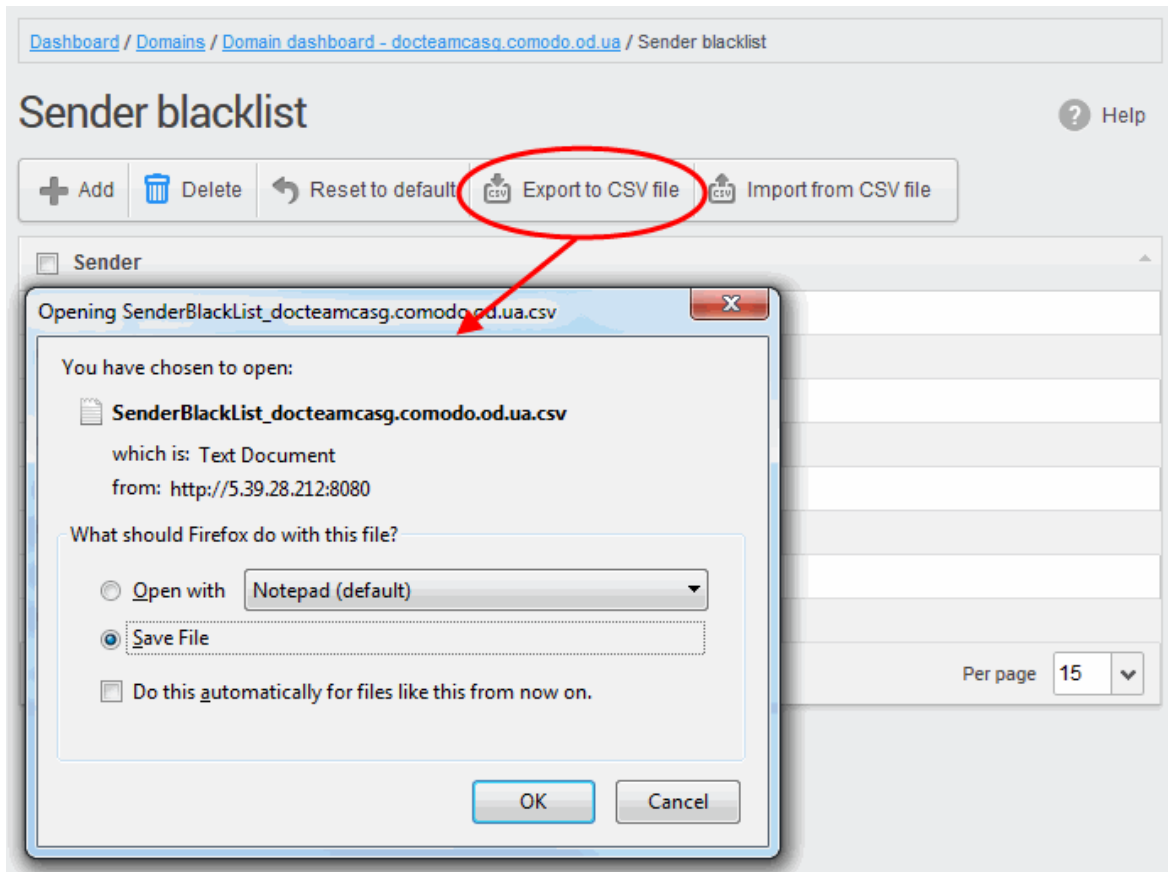
Exporting the Sender Blacklist to CSV file

The administrator can save the configured sender blacklist by exporting it as a CSV file. If required in future, the

administrator can import the users from the csv file, for example for a new account or after a reset.

To export the list

- Click the 'Export to CSV file' to save the list of blacklisted senders as a CSV file

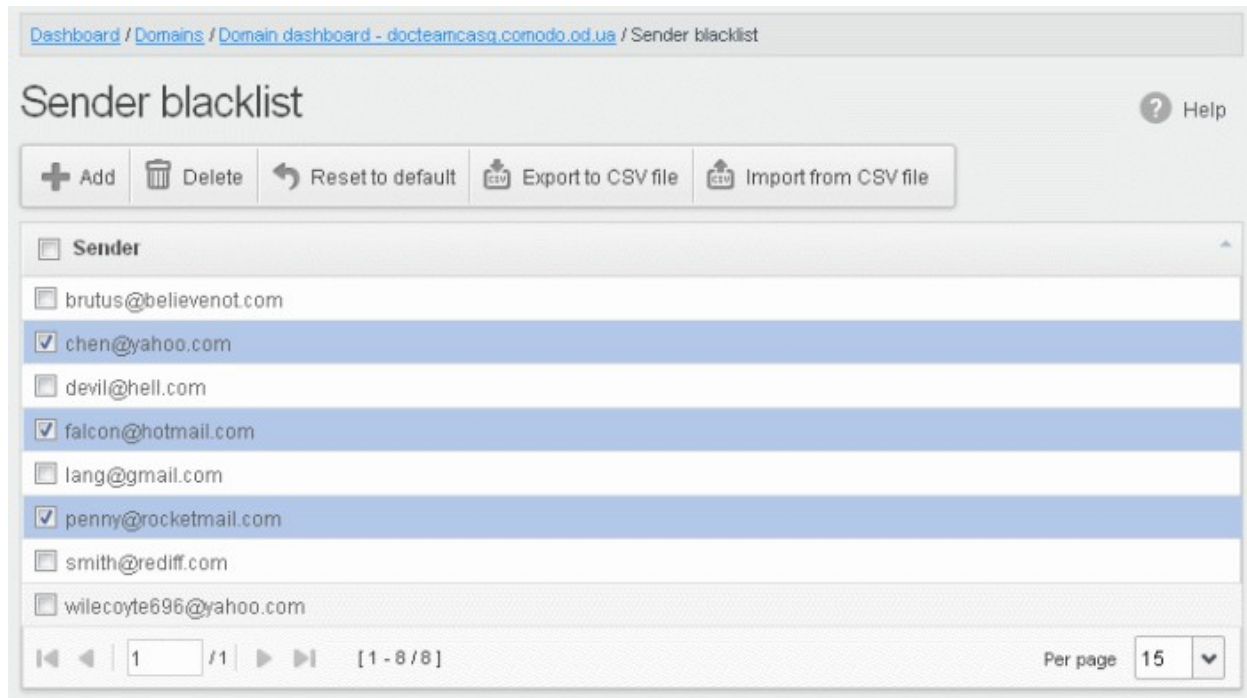


A file download dialog will be displayed.

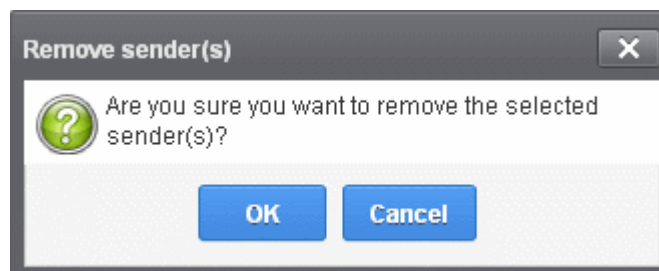
- Click 'OK' and navigate to the location in your computer and save the file or the file will be downloaded to your download folder.

Deleting Users from the Sender Blacklist

- To delete a sender from the blacklist, select the sender from the list and click the 'Delete' button.



- Click 'OK' to confirm your changes. The sender(s) will be removed from the blacklist. The emails from the senders will be allowed as per the existing filter settings in CASG.

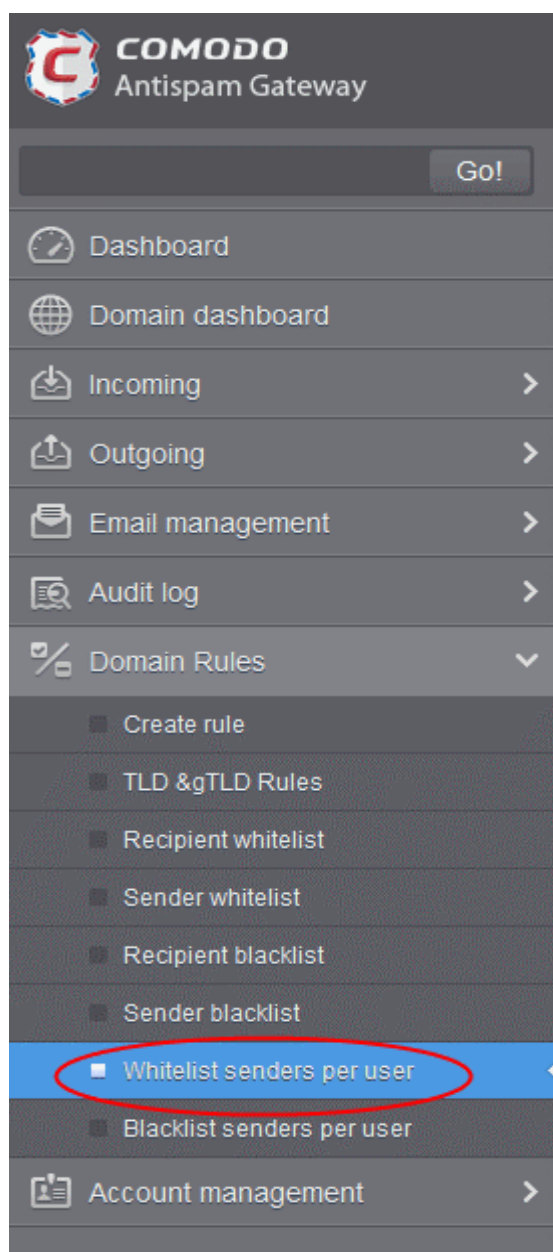


Whitelist Senders Per User

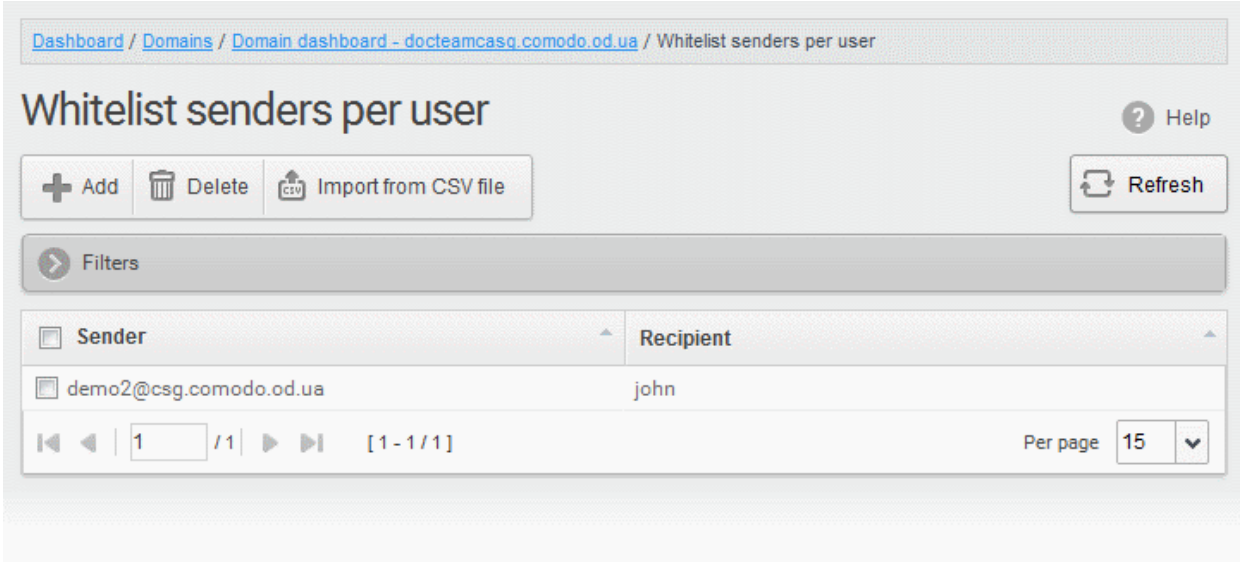
CASG allows administrators to add senders to whitelist on per user basis. Whitelisted senders for specific recipients can be added manually, importing from a .csv file and from the users' requests. All the filtering checks for whitelisted senders to the requested / added recipients of the selected domain are disabled. Comodo strongly recommends to use this option after analyzing the request is genuine and warranted.

To configure sender whitelist per user

- Select the 'Whitelist / Blacklist' tab from the left hand side navigation to expand it and then click the 'Whitelist senders per user' sub tab.



The 'Whitelist senders per user' interface will be displayed:



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Whitelist senders per user

Whitelist senders per user

Help

+ Add Delete Import from CSV file Refresh

Filters

Sender	Recipient
<input type="checkbox"/> demo2@csg.comodo.od.ua	john

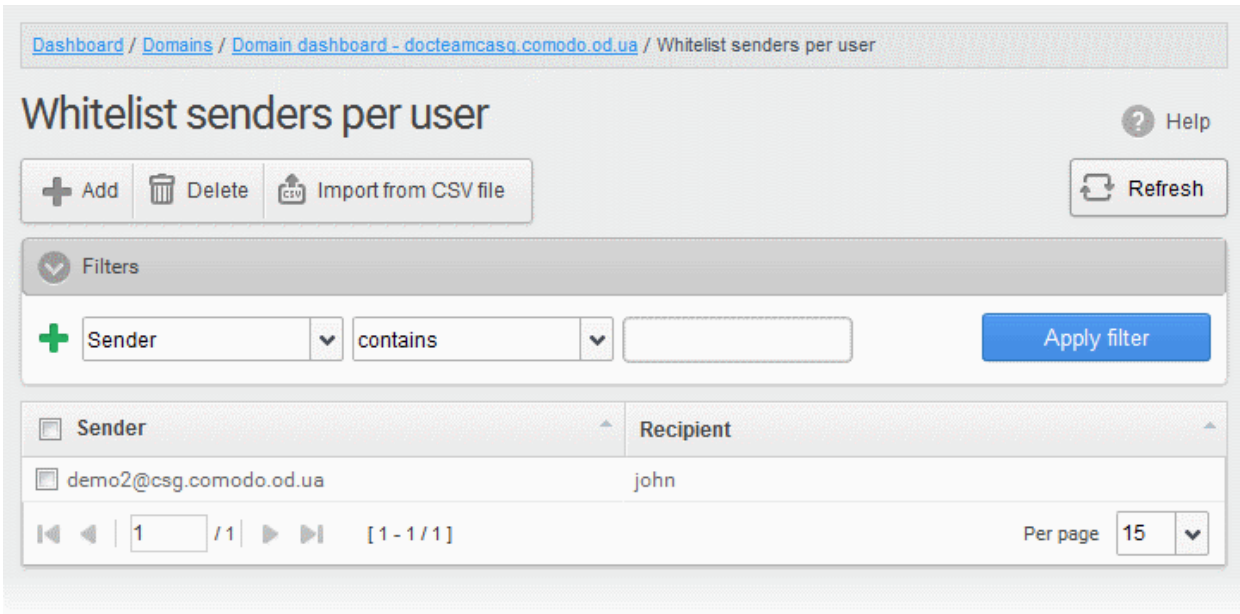
1 / 1 [1 - 1 / 1] Per page 15

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using the Filter option to search senders and recipients

Click anywhere on the Filters tab to open the filters area.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Whitelist senders per user

Whitelist senders per user

Help

+ Add Delete Import from CSV file Refresh

Filters

+ Sender contains

Apply filter

Sender	Recipient
<input type="checkbox"/> demo2@csg.comodo.od.ua	john

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

You can add more filters by clicking **+** for narrowing down your search.

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Sender:** Will execute a search of senders according to the text in the text box (column 3) and the condition selected in column 2.
- **Recipient:** Will execute a search of recipients according to the text in the text box (column 3) and the condition selected in column 2.

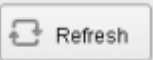
The following conditions are available:

- **Equals:** Displays all senders / recipients that match the text entered in the text box.
- **Not Equals:** Displays all senders / recipients except the one entered in the text box.
- **Contains:** Displays all senders / recipients that contain the words entered in the text box.
- **Not Contains:** Displays all senders / recipients that do not contain the words entered in the text box.
- **Starts With:** Displays all senders / recipients that start with the words entered in the text box.
- **Ends With:** Displays all the senders / recipients that end with the words entered in the text box.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.

Click the  button to display all users.

Note: To display all the Whitelist senders after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

From this interface administrators can:

- **Add senders to whitelist per user**
- **Remove senders from Whitelist senders per user list**

Adding Senders to Whitelist Per User

You can add senders to whitelist in the following ways:

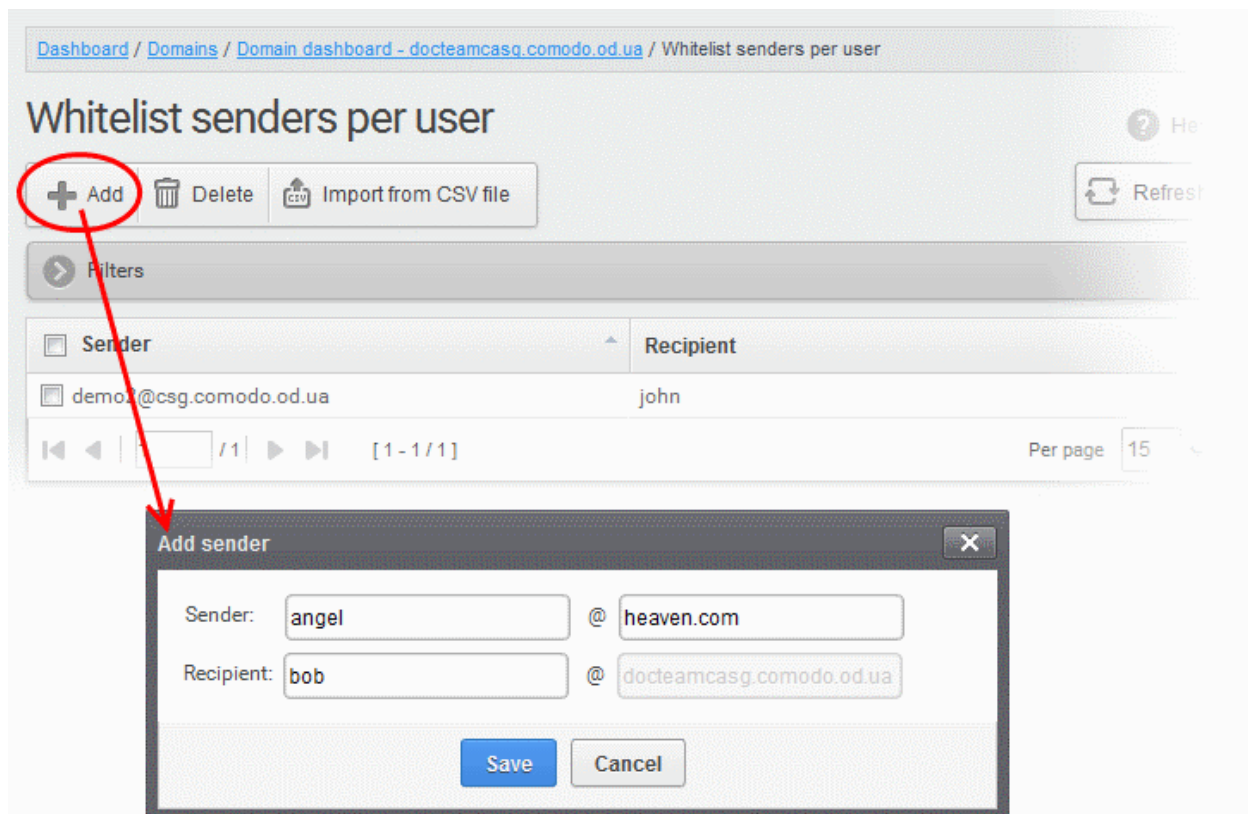
- **Manually adding the senders**
- **Importing senders from a CSV file**
- **Adding from Whitelist requests from users**

Manually adding the senders

The administrator can manually specify the whitelisted sender and corresponding recipient one-by-one to be added.

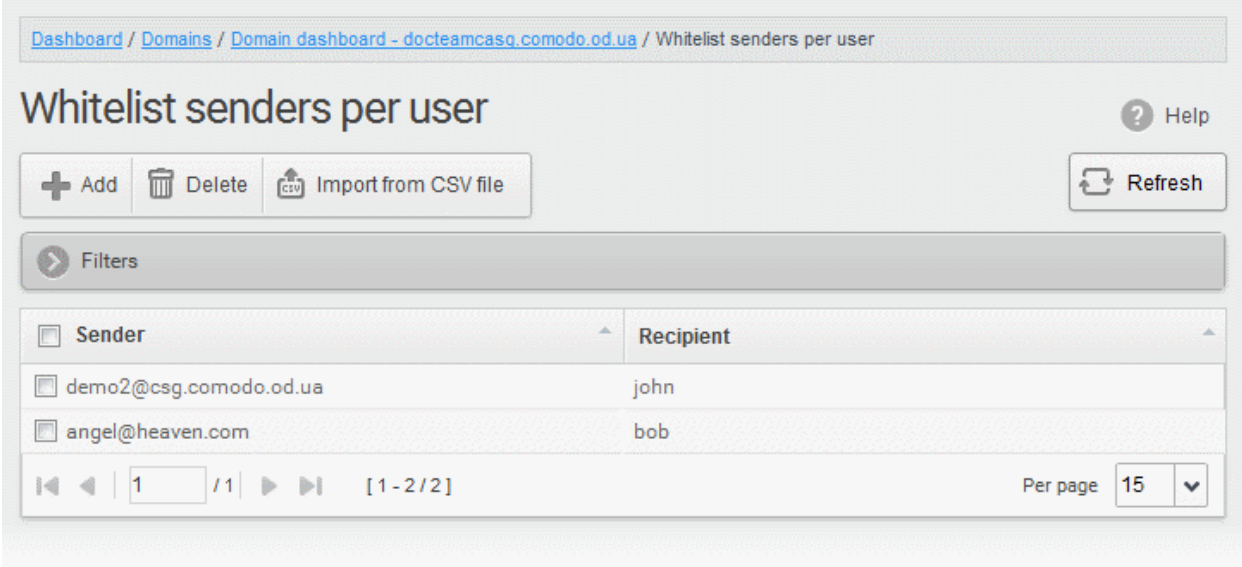
To manually add senders to whitelist per user basis

- Click 'Add' to add a new sender to the list. The 'Add sender' dialog box will be displayed:



- Enter the sender's username in the E-mail textbox and sender's email domain name after the @ symbol in the first row.
- Enter the recipient's name in the Recipient text box in the second row. **Note:** The recipient should be a valid user.
- Click the 'Save' button. Repeat the process to add more whitelisted senders for the user.

The list of whitelisted senders will be displayed.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Whitelist senders per user

Whitelist senders per user

Help

+ Add Delete Import from CSV file Refresh

Filters

Sender	Recipient
<input type="checkbox"/> demo2@csg.comodo.od.ua	john
<input type="checkbox"/> angel@heaven.com	bob

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

Importing senders from a CSV file

Administrators can import a multiple senders at a time from a comma separated values (CSV) file to Sender whitelist per user. The list of whitelisted senders and respective recipients can be created using notepad or a spreadsheet application like MS Excel or OpenOffice Calc and saved in .csv format. Each line in the .csv file should contain the sender's email address and the username of the recipient or sender's email address and the recipient's email address, separated by a comma. An example is shown below:

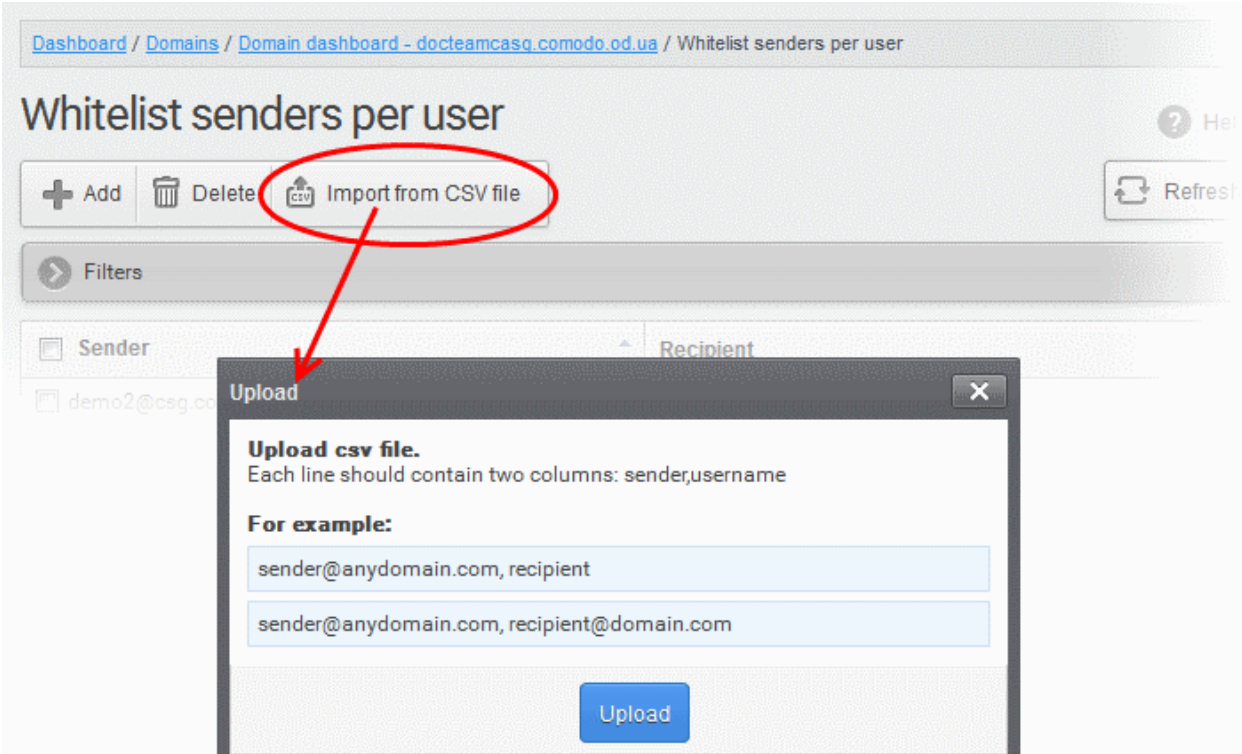
sender1@anydomain.com, recipient1

sender2@anydomain.com, recipient2@domain.com

sender3@somedomain.com, recipient3

To import senders to whitelist from CSV file

- Click the 'Import from CSV file' from the 'Whitelist senders per user' interface. The 'Upload' dialog will appear.



Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Whitelist senders per user

Whitelist senders per user

Help

+ Add Delete Import from CSV file Refresh

Filters

Sender	Recipient
<input type="checkbox"/> demo2@csg.co	

Upload

Upload csv file.
Each line should contain two columns: sender,username

For example:

sender@anydomain.com, recipient

sender@anydomain.com, recipient@domain.com

Upload

- Click 'Upload', navigate to the location where the file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes only a remaining part of not imported task.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Whitelist senders per user

Whitelist senders per user

Import is in process. Please wait

+ Add Delete **Cancel import from CSV file** Refresh

Filters

Sender	Recipient
demo2@csg.comodo.od.ua	john

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

On completion of the upload process, the results will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Whitelist senders per user

Whitelist senders per user

Total lines processed 2

Imported 2 senders as whitelisted

Import for domain docteamcasg.comodo.od.ua has been finished

+ Add Delete Import from CSV file Refresh

Filters

Sender	Recipient
peter@pearlygates.com	john
demo2@csg.comodo.od.ua	john
alice@heaven.com	bob

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

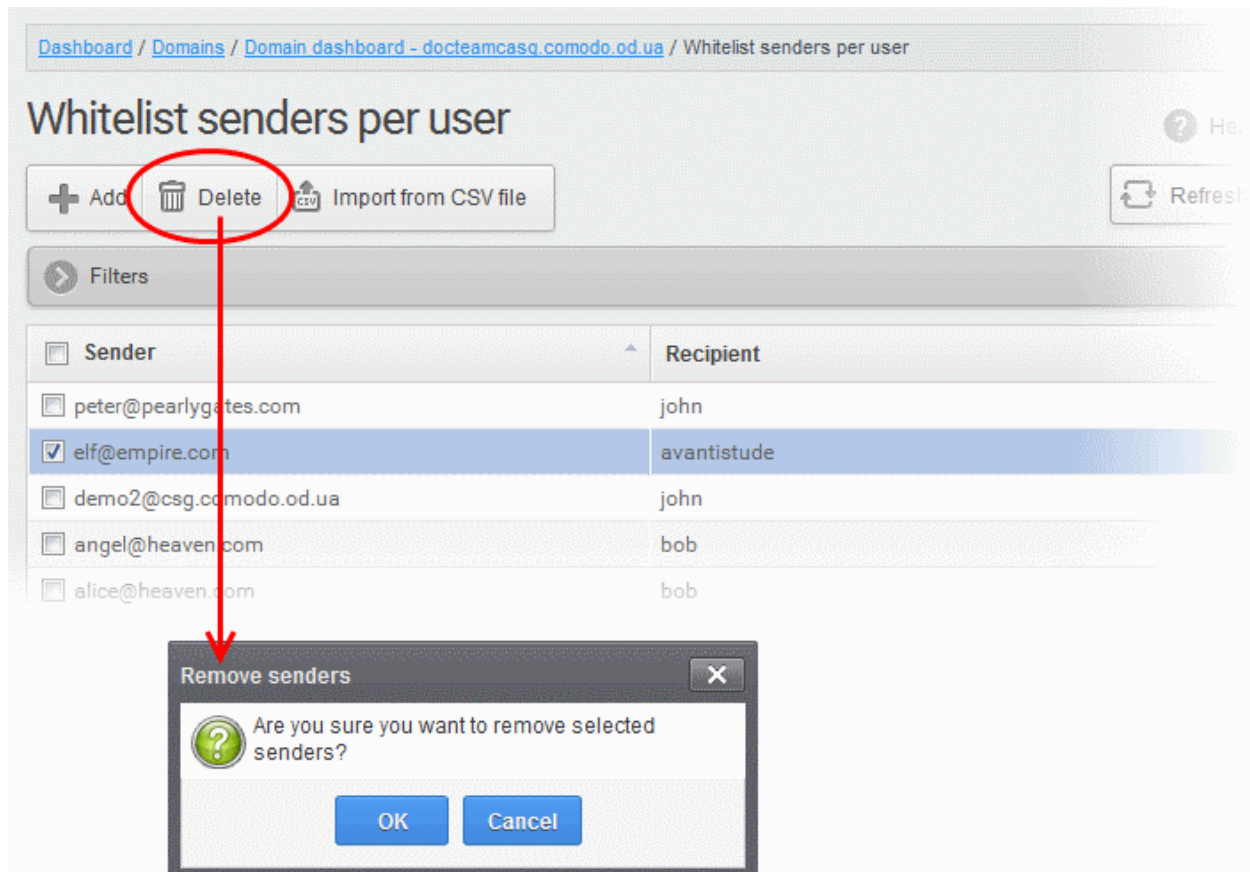
The sender whitelist per user from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

Adding from Whitelist requests from users

The administrator can add senders to whitelist based on the requests of the users. Refer to the section **Email Management > Whitelisted Requests** for more details.

Deleting Senders from Whitelist

- To delete a sender from the whitelist, select the sender from the list and click the 'Delete' button.



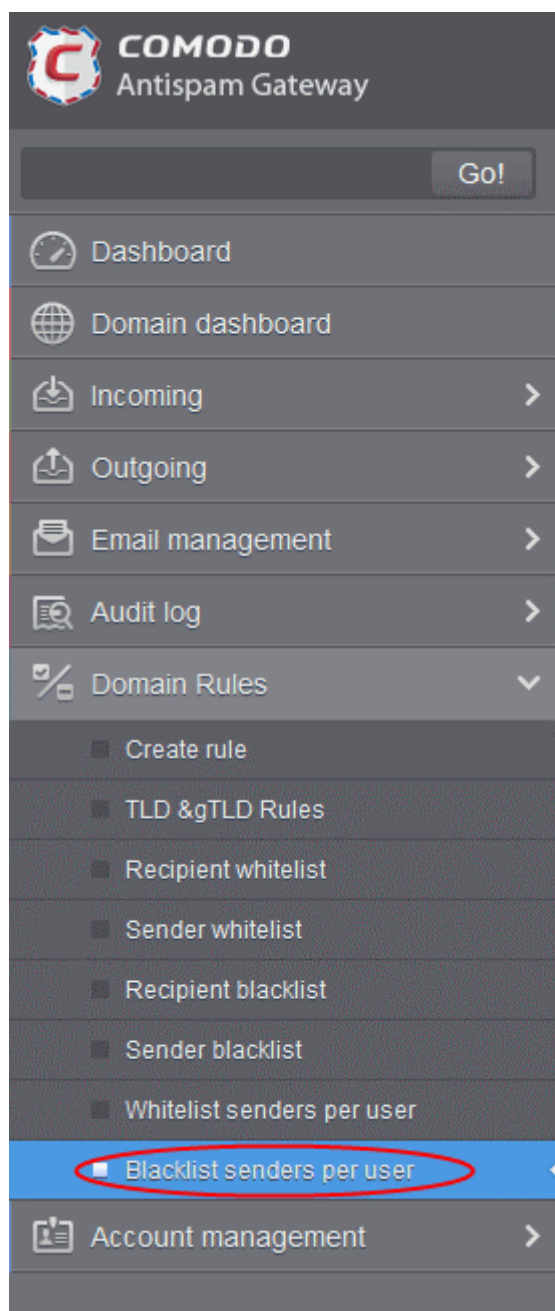
- Click 'OK' in the confirmation dialog.

Blacklist Senders Per User

CASG allows administrators to add senders to blacklist on per user basis. This feature is useful in scenarios where you want to allow mails from a particular sender to all users in the domain but want to block the sender for a particular recipient in the domain. Senders for blacklisting for specific recipients can be added manually, importing from a .csv file and from the users' requests.

To configure sender blacklist per user

- Select the 'Whitelist / Blacklist' tab from the left hand side navigation to expand it and then click the 'Blacklist senders per user' sub tab.



The 'Blacklist senders per user' interface will be displayed:

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Blacklist senders per user

Blacklist senders per user

Help

+ Add Delete Import from CSV file Refresh

Filters

Sender	Recipient
demo1@csg.comodo.od.ua	john

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

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Using the Filter option to search senders and recipients

- Click anywhere on the Filters tab to open the filters area.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Blacklist senders per user

Blacklist senders per user

Help

+ Add Delete Import from CSV file Refresh

Filters

+ Sender contains

Apply filter

Sender	Recipient
demo1@csg.comodo.od.ua	john

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

You can add more filters by clicking **+** for narrowing down your search.

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Sender:** Will execute a search of senders according to the text in the text box (column 3) and the condition selected in column 2.
- **Recipient:** Will execute a search of recipients according to the text in the text box (column 3) and the condition selected in column 2.

The following conditions are available:

- **Equals:** Displays all senders / recipients that match the text entered in the text box.
 - **Not Equals:** Displays all senders / recipients except the one entered in the text box.
 - **Contains:** Displays all senders / recipients that contain the words entered in the text box.
 - **Not Contains:** Displays all senders / recipients that do not contain the words entered in the text box.
 - **Starts With:** Displays all senders / recipients that start with the words entered in the text box.
 - **Ends With:** Displays all the senders / recipients that end with the words entered in the text box.
- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all users.

Note: To display all the Blacklist senders after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

From this interface administrators can:

- **Add senders to blacklist per user**
- **Remove senders from blacklist senders per user list**

Adding Senders to Blacklist Per User

You can add senders to blacklist in the following ways:

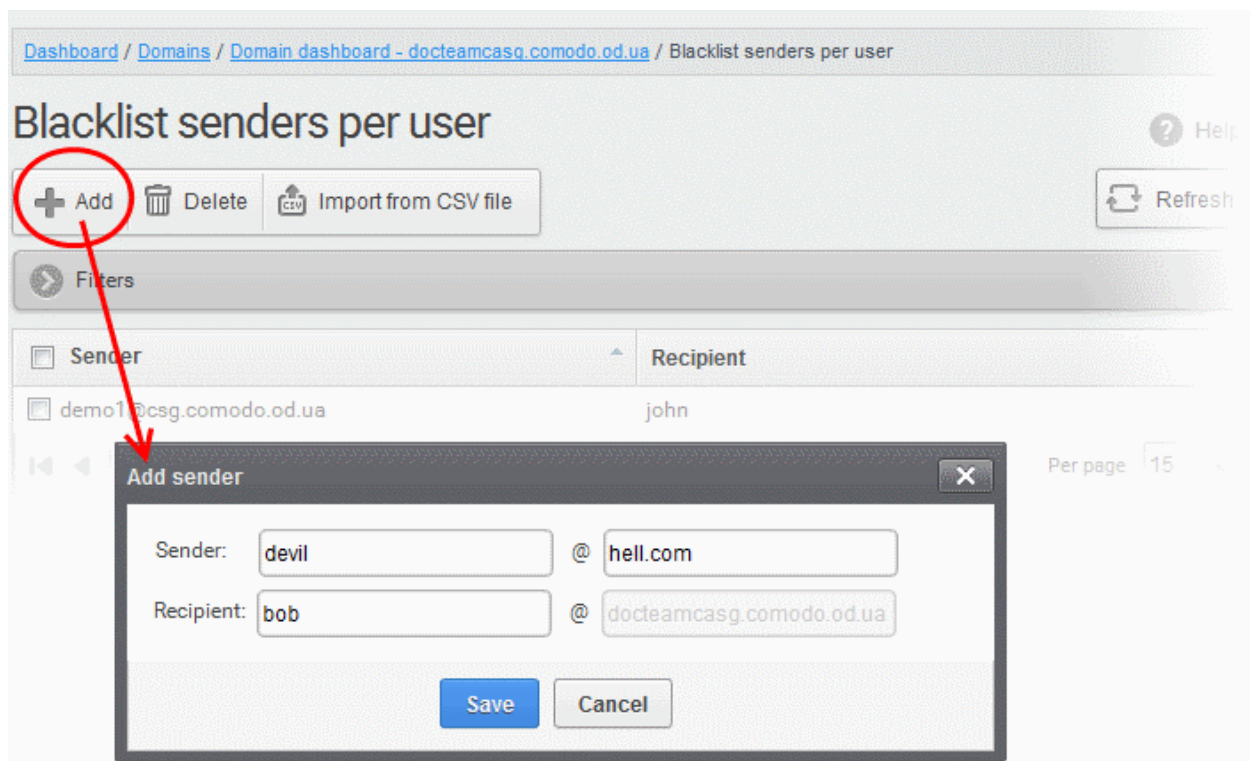
- **Manually adding the senders**
- **Importing senders from a CSV file**
- **Adding senders from Blacklist requests from users**

Manually adding the senders

The administrator can manually specify the senders to be whitelisted for specific recipients, one-by-one to be added.

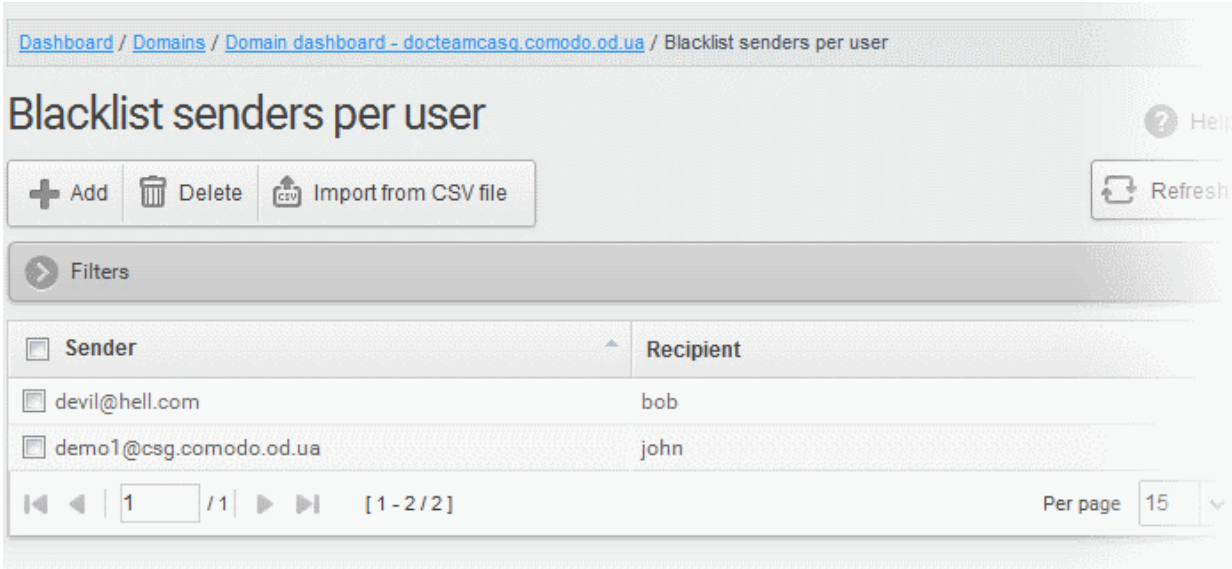
To manually add senders to blacklist per user basis

- Click 'Add' to add a new sender to the list. The 'Add sender' dialog box will be displayed:



- Enter the sender's username in the E-mail textbox and sender's email domain name after the @ symbol in the first row.
- Enter the recipient's name in the Recipient text box in the second row. **Note:** The recipient should be a valid user.
- Click the 'Save' button. Repeat the process to add more blacklisted senders for the user.

The list of blacklisted senders will be displayed.



Dashboard / Domains / Domain dashboard - docteamcsg.comodo.od.ua / Blacklist senders per user

Blacklist senders per user

[+ Add](#) [Delete](#) [Import from CSV file](#) [Refresh](#)

Filters

Sender	Recipient
<input type="checkbox"/> devil@hell.com	bob
<input type="checkbox"/> demo1@csg.comodo.od.ua	john

[1 - 2 / 2] Per page 15

Importing senders from a CSV file

Administrators can import a multiple senders at a time from a comma separated values (CSV) file to Sender blacklist per user. The list of blacklisted senders and respective recipients can be created using notepad or a spreadsheet application like MS Excel or OpenOffice Calc and saved in .csv format. Each line in the .csv file should contain the sender's email address and the username of the recipient or sender's email address and the recipient's email address, separated by a comma. An example is shown below:

```
sender1@anydomain.com, recipient1
```

```
sender2@anydomain.com, recipient2@domain.com
```

```
sender3@somedomain.com, recipient3
```

To import senders to Blacklist from CSV file

- Click the 'Import from CSV file' from the 'Blacklist senders per user' interface. The 'Upload' dialog will appear.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Blacklist senders per user

Blacklist senders per user

Filters

Sender	Recipient
devil@hell.com	bob
demo1@csg.comodo.od.ua	john

Per page 15

Upload [X]

Upload csv file.
Each line should contain two columns: sender,username

For example:

sender@anydomain.com, recipient

sender@anydomain.com, recipient@domain.com

- Click 'Upload', navigate to the location where the .csv file is saved and click the 'Open' button. The maximum size of the file that can be uploaded is 9 MB.

The upload will be placed in import tasks queue and the progress of the upload will be displayed. If you want to remove the upload from the queue, click the 'Remove import task' button. The 'Remove import task' deletes only a remaining part of not imported task.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Blacklist senders per user

Blacklist senders per user

Import is in process. Please wait [X]

Filters

Sender	Recipient
devil@hell.com	bob
demo1@csg.comodo.od.ua	john

/ 1 [1 - 2 / 2]
 Per page 15 [v]

On completion of the upload process, the results will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Blacklist senders per user

Blacklist senders per user Help

Total lines processed 3 ✕

Imported 3 senders as blacklisted ✕

Import for domain docteamcasg.comodo.od.ua has been finished ✕

+ Add ✕ Delete 📄 Import from CSV file 🔄 Refresh

Filters

<input type="checkbox"/> Sender	<input type="checkbox"/> Recipient
<input type="checkbox"/> judas@betrayal.com	john
<input type="checkbox"/> devil@hell.com	bob
<input type="checkbox"/> demo1@csg.comodo.od.ua	john
<input type="checkbox"/> brutus@treason.com	john
<input type="checkbox"/> bluto@ironcastle.com	bob

1 / 1 [1 - 5 / 5] Per page 15

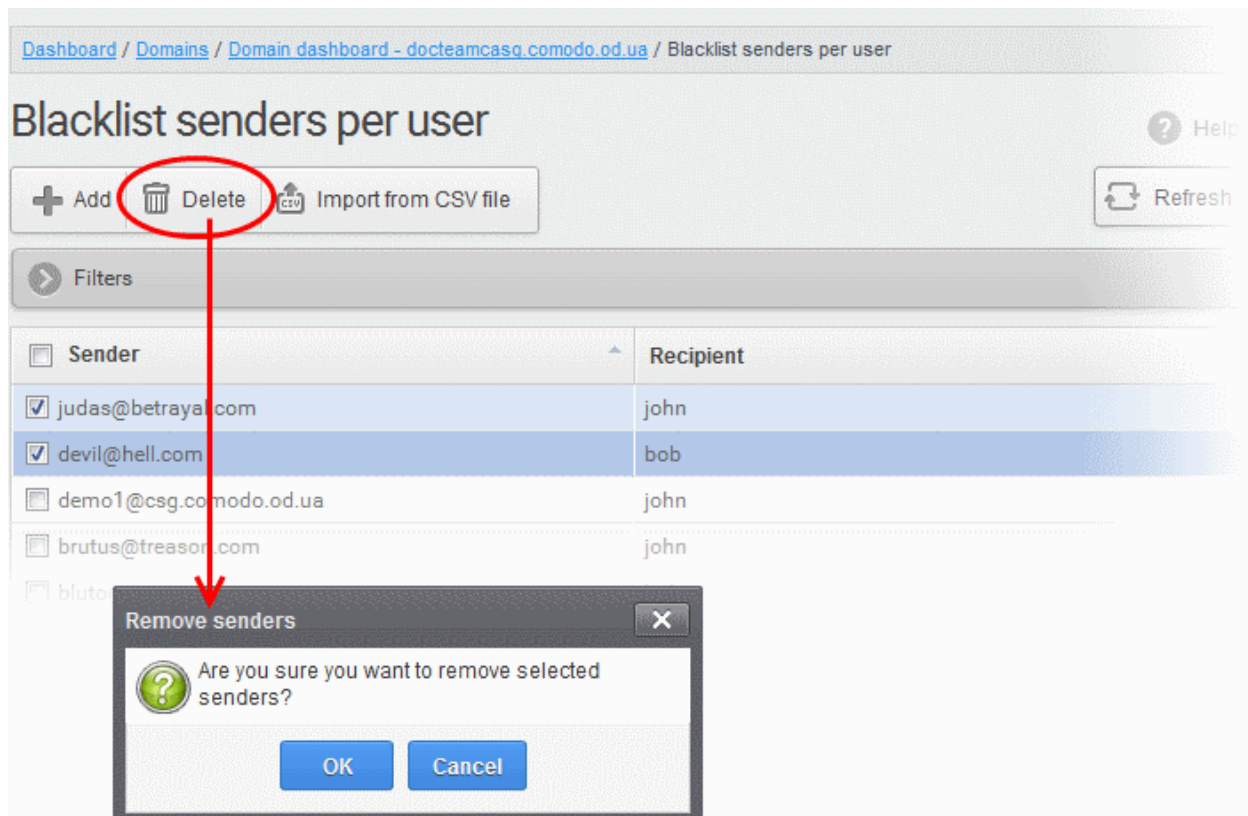
The sender blacklist per user from .csv file will be uploaded and the administrator who carried out the task will receive a notification about the import task completion.

Adding senders from Blacklist requests from users

The administrator can add senders to blacklist based on the requests of the users. Refer to the section [Email Management > Blacklisted Requests](#) for more details.

Deleting Senders from Blacklist

- To delete a sender from the blacklist, select the sender from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.

3.2.1.1.4.7 Account Management

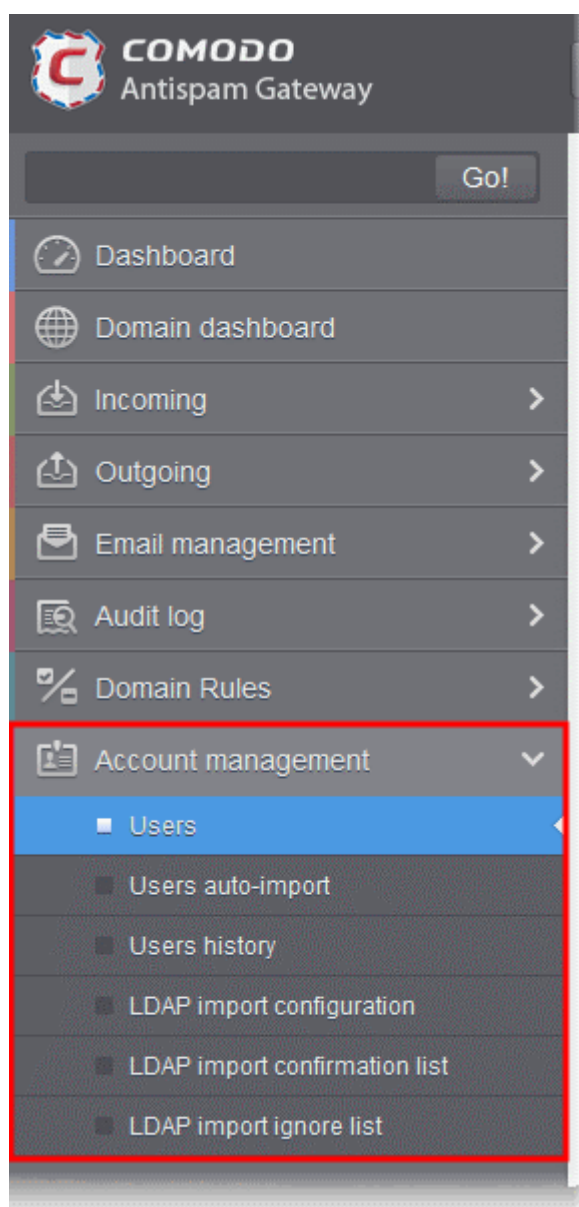
In the Account Management interface, an administrator can manage the users for the selected domain. From this interface, you can reset passwords for users, allow or deny permission for users to access their account, can import CSV file containing the list of users, import users from your the Active Directory (AD) server of the domain through Lightweight Directory Access Protocol (LDAP), add and move your aliases. In the Users history interface, an administrator can view users login history. Refer to [User History](#) for more details.

Click the following links for more details:

- [Users](#)
- [User auto-import](#)
- [Users history](#)
- [Importing Users from LDAP](#)

3.2.1.1.4.7.1 User Account Management

The 'Users' area allows administrators with appropriate privileges to manage users for the selected domain. This includes adding/importing users, deleting users, editing user accounts, resetting passwords and configuring user permissions. Admins can also configure email aliases from this interface.

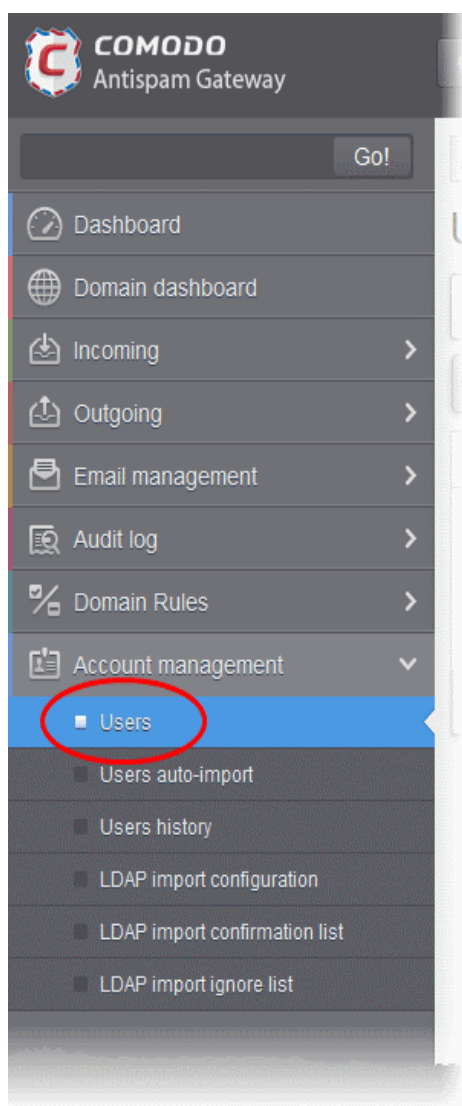


Click the following links for more details:

- [Managing Users](#)
- [Adding New Users](#)
- [Deleting Users](#)
- [Editing Users](#)
- [Unlocking Users](#)
- [Importing from CSV file](#)
- [Managing Permissions](#)
- [Aliases](#)
- [Moving to Aliases](#)
- [Importing Aliases from CSV file](#)
- [Forwarding mails to another user](#)
- [Other actions](#)

Managing Users

- Click 'Account management' on the left then click 'Users':



The 'Users' interface of the selected domain will be displayed.

Dashboard / Domains / Domain dashboard - docteamcaso.comodo.od.ua / Users

Users

Help

+ Add Delete Edit Unlock More actions

Refresh

Filters

Username	Enabled	Last login	Aliases	Group	Forward to
bob	Yes	2015-06-29 08:24:00		Power Users	
john	Yes	2015-06-29 11:32:54		Users	
alice	Yes			Users	

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

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. The sorting option is not available for 'Aliases and Group' columns.

Using the filter option to search users

Click anywhere on the Filters tab to open the filters area.

Dashboard / Domains / Domain dashboard - docteamcaso.comodo.od.ua / Users

Users

Help

+ Add Delete Edit Unlock More actions

Refresh

Filters

+ Username contains

Apply filter

Username	Enabled	Last login	Aliases	Group	Forward to
bob	Yes	2015-06-29 08:24:00		Power Users	
john	Yes	2015-06-29 11:32:54		Users	
alice	Yes			Users	

You can add more filters by clicking **+** for narrowing down your search.

Dashboard / Domains / Domain dashboard - docteamcaso.comodo.od.ua / Users

Users

Help

+ Add Delete Edit Unlock More actions

Refresh

Filters

+ Username contains

- Enabled equals

Apply filter

Username	Enabled	Last login	Aliases	Group	Forward to
bob	Yes	2015-06-29 08:24:00		Power Users	
john	Yes	2015-06-29 11:32:54		Users	
alice	Yes			Users	

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

You can remove a filter by clicking the **-** icon beside it.

Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

If 'Username' is selected, the following conditions are available:

- **Equals:** Displays all usernames that match the text entered in the text box.
- **Not Equals:** Displays all users except the one entered in the text box.
- **Contains:** Displays all username(s) that contain the words entered in the text box.
- **Not Contains:** Displays all username(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all username(s) that start with the words entered in the text box.
- **Ends With:** Displays all the username(s) that end with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Enabled:** Sorts the results based on whether a user is enabled or disabled.

When you select this option in the first drop-down, 'equals' is the only option available in the second drop-down:

- **Equals:** Displays the results of enabled users when the checkbox beside it is selected. When the checkbox is not selected, it displays the list of users who are not enabled.
- **Last Login:** Sorts the results based on the last login details of users.

When you select this option in the first drop-down, the following filters are available:

- **Equals:** Displays the list of users whose last login date is the same as the selected date in the third box from the calendar.
- **Less than:** Displays the list of users whose last login date is less than the selected date in the third box from the calendar.
- **Greater than:** Displays the list of users whose last login date is greater than the selected date in the third box from the calendar.
- **Alias username:** Will execute a search of user alias name according to the text in the text box (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available:

- **Contains:** Displays all users with alias name(s) that contain the words entered in the text box.
- **Equals:** Displays all users with alias names that match the text entered in the text box.
- **Not Equals:** Displays all users except those with the alias name entered in the text box.
- **Not Contains:** Displays all user alias name(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all user alias name(s) that start with the words entered in the text box.
- **Ends With:** Displays all the user alias name(s) that end with the words entered in the text box.
- **Alias Domain:** Will execute a search of domain alias name according to the text in the text box (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available:

- **Contains:** Displays all users with domain alias name(s) that contain the words entered in the text box.
- **Equals:** Displays all users with domain alias names that match the text entered in the text box.
- **Not Equals:** Displays all users except those with the domain alias name entered in the text box.
- **Not Contains:** Displays all user domain alias name(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all user domain alias name(s) that start with the words entered in the text box.
- **Ends With:** Displays all the user domain alias name(s) that end with the words entered in the text

box.

- **Forward to:** Will execute a search of forwarded to user names according to the text in the text box (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available:

- **Equals:** Displays all usernames that match the text entered in the text box.
- **Not Equals:** Displays all users except the one entered in the text box.
- **Contains:** Displays all username(s) that contain the words entered in the text box.
- **Not Contains:** Displays all username(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all username(s) that start with the words entered in the text box.
- **Ends With:** Displays all the username(s) that end with the words entered in the text box.
- **Group:** Will execute a search of users belonging to the user group selected from the drop-down in the third column and the condition selected in column 2.

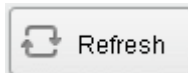
When you select this option in the first drop-down, the following filters are available:

- **Equals:** Displays all users from the group selected from the third drop-down.
- **Not Equals:** Displays all the users excluding those belonging to the group selected from the third drop-down.

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.



Click the  button to display all users.

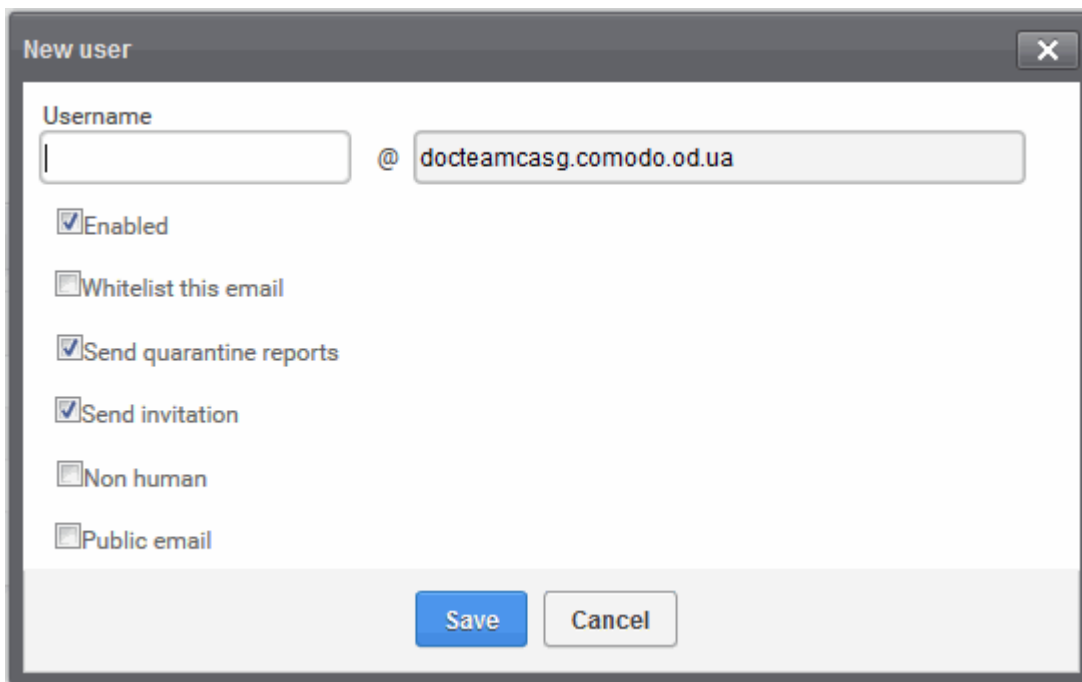
Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add a new user

- Click the 'Add' button.

A screenshot of the 'Users' management page in the Comodo Antispam Gateway. The page title is 'Users' and the breadcrumb is 'Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.us / Users'. There is a 'Help' icon in the top right. Below the title, there is a toolbar with buttons: '+ Add' (circled in red), 'Delete', 'Edit', 'Unlock', and 'More actions'. A 'Refresh' button is also present. Below the toolbar is a 'Filters' section. The main content is a table with columns: Username, Enabled, Last login, Aliases, Group, and Forward to. The table contains three rows: 'alice' (Enabled: Yes), 'bob' (Enabled: Yes, Last login: 2015-06-29 08:24:00, Group: Power Users, Forward to: john@docteamcasg.comodo.od.us), and 'john' (Enabled: Yes, Last login: 2015-06-29 11:32:54, Group: Users).

The 'New user' dialog will be displayed:



- Enter the username of a new user that will be first part of the email address. For example, if you type 'alice', the email address of the user will be 'alice@domainname.com'.

By default, the user will be enabled. Clear the 'Enabled' box to deny the new user access to CASG. You can enable the user in the **Edit user** interface later on.

You can choose to add the new user to **Recipient Whitelist** from this interface itself. Select the checkbox beside the 'Whitelist email' to add the user to **Recipient Whitelist**.

The administrators can also determine whether the users will get the reports or not. By default, it is enabled.

- Uncheck 'Send quarantine reports' box to disable this option.
- Checking 'Send invitation' box will send the invitation mail to the email recipient address entered in the 'Username' text box.
- Check 'Non human' if the address is a no-reply or common mailing list such as 'sales@...'
- Check 'Public email' if the address is published somewhere, for example on a customer facing website. Enabling this box will allow CASG to more accurately filter spam for this type of email address.
- Click the 'Save' button.

Note: If the user is disabled and subscribed for periodical Quarantine Reports, the subscription will also be canceled.

An email to the added user will be sent automatically containing password to access CASG. The password can be reset in the **edit interface**. The added user will be displayed in the list.

Dashboard / Domains / Domain_dashboard - docteamcasg.comodo.od.ua / Users

Users

Help

+ Add Delete Edit Unlock More actions

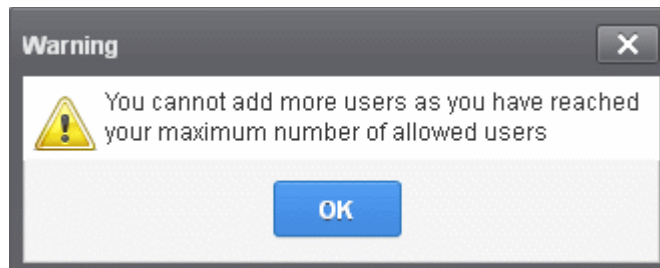
Refresh

Filters

Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	
bob	Yes	2015-06-29 08:24:00		Power Users	john@docteamcasg.comodo
john	Yes	2015-06-29 11:32:54		Users	
henry	Yes			Users	

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

Note: The number of users that can be added depends on the plan subscribed by you and the maximum number of users limit configured for the domain in the **Add Domains** / **Edit Domains** / **Domain Settings** interfaces. When you exceed the limit of users, the following will be displayed while adding a new user.



To delete an existing user

- Select the user you want to delete from the list and click the 'Delete' button

Dashboard / Domains / Domain_dashboard - docteamcasg.comodo.od.ua / Users

Users

Help

+ Add Delete Edit Unlock More actions

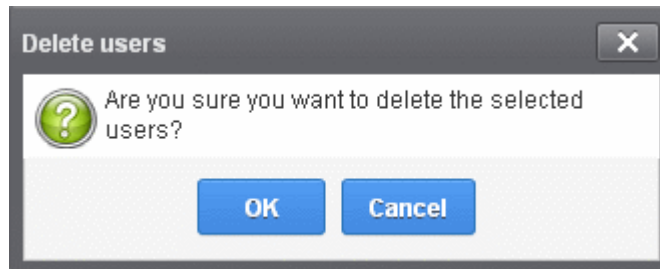
Refresh

Filters

Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	
bob	Yes	2015-06-29 08:24:00		Power Users	john@docteamcasg.comodo
john	Yes	2015-06-29 11:32:54		Users	
henry	Yes			Users	

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

- Click 'OK' to confirm your changes.

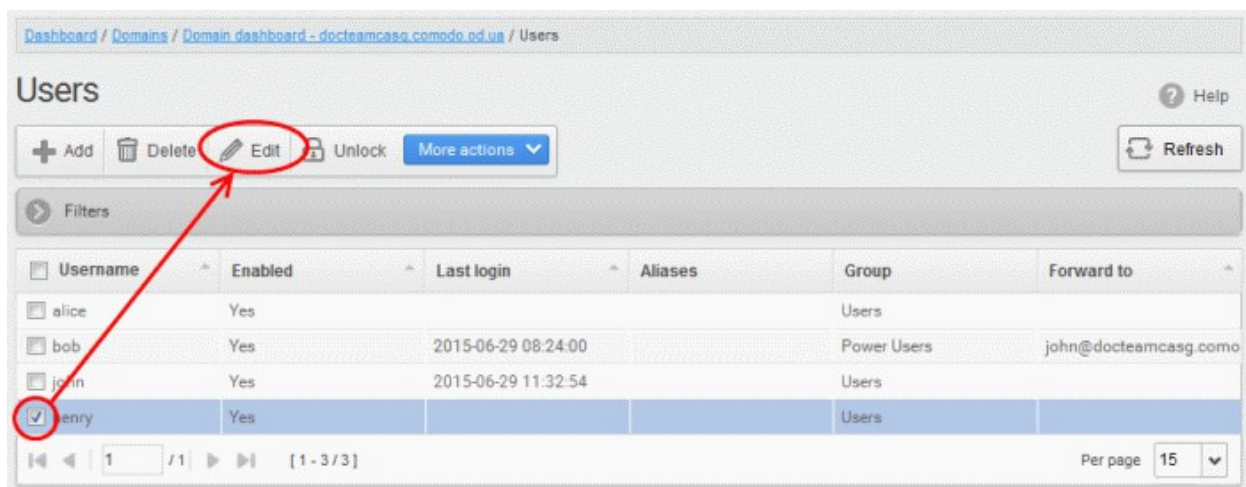


The user(s) will be removed from the list.

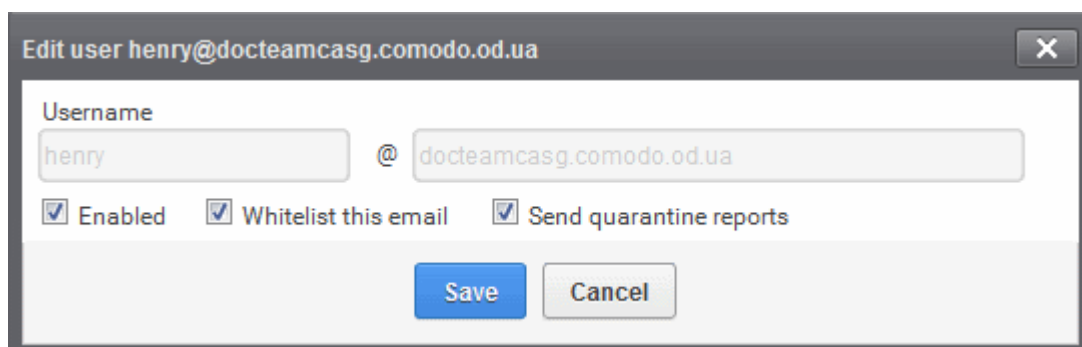
To edit an existing user

You can select to allow or deny permission for the users to access their CASG account in the edit interface as well as enable or disable quarantine report generation for the user.

- Select the user you want to edit from the list and click the 'Edit' button.



The 'Edit user' dialog box will be displayed.



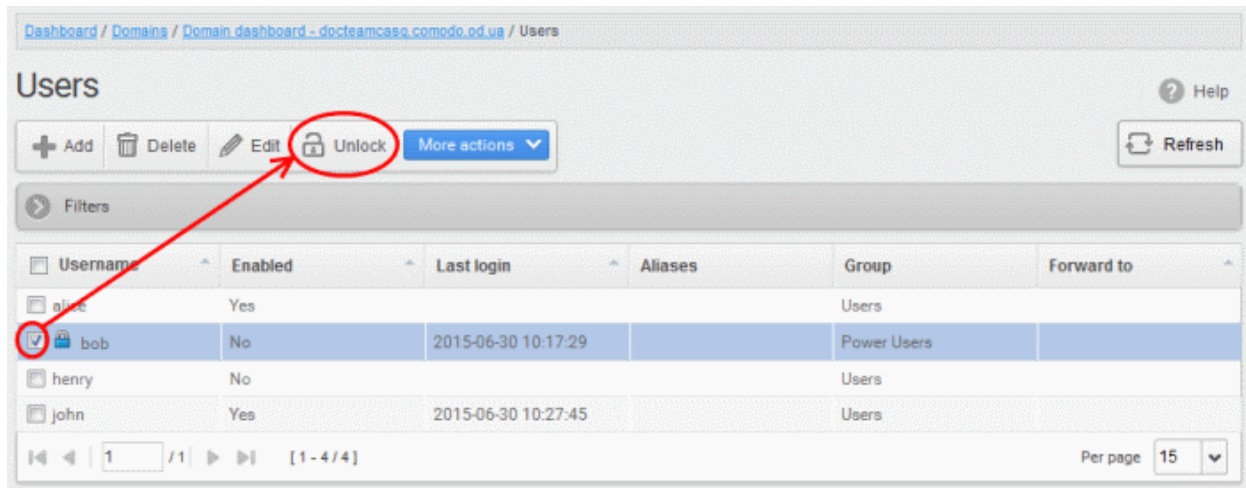
- **Enabled** - Select the checkbox to allow or deny access to the CASG interface.
- **Whitelist email** - Select this checkbox to add the user to **Recipient Whitelist**.
- Disable '**Send quarantine reports**' checkbox, if you do not want the user to get quarantine reports. By default it is enabled.
- Click the 'Save' button to confirm your changes.

Note: If the user is disabled and if the user has subscribed for periodical Quarantine Reports, the subscription will be canceled.

To unlock users

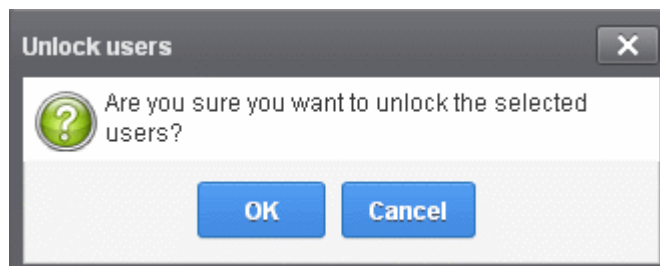
Users who try to login to CASG with wrong credentials will be automatically locked after three unsuccessful attempts. They will be able to try again only after 30 minutes from the time of lockout. CASG administrators can unlock these users immediately without waiting for the timeout period to end, so that the users can try to login again to CASG.

The locked out users will be displayed with a lock icon beside them.



- Select the locked user from the list and click the 'Unlock' button.

A confirmation dialog will be displayed.



- Click 'OK' to unlock the selected locked user.

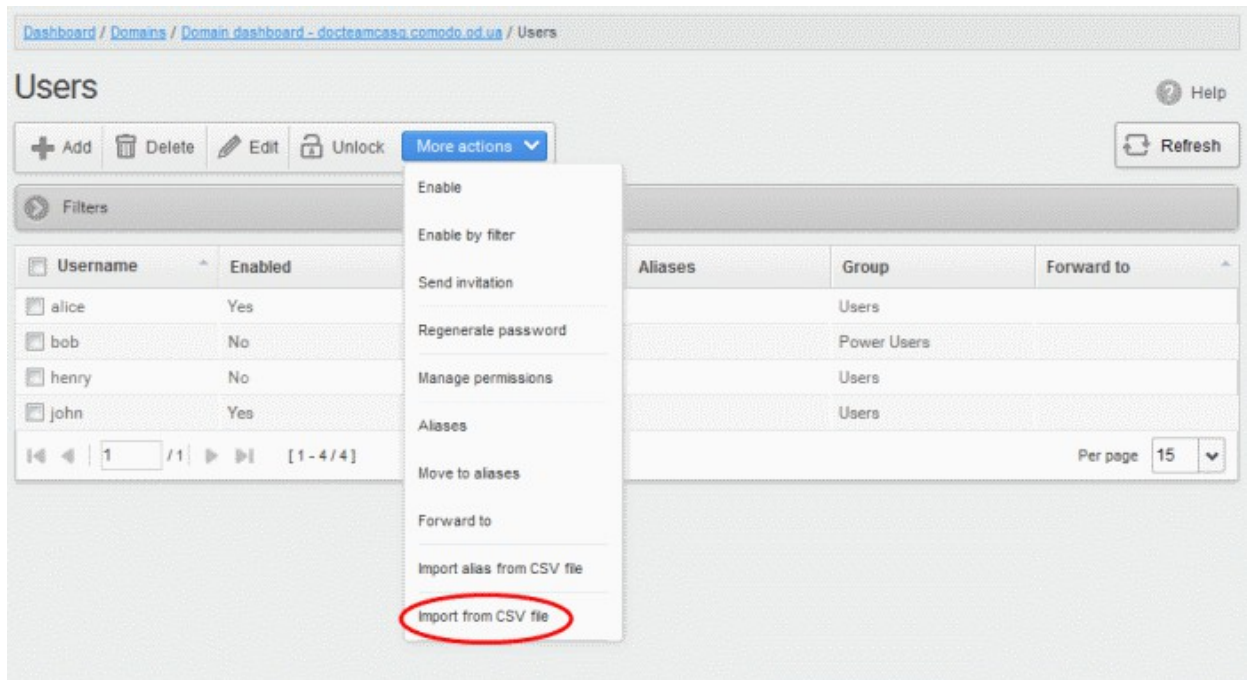
The user now can try to login again without waiting for the lockout time period to end.

To import users from CSV file

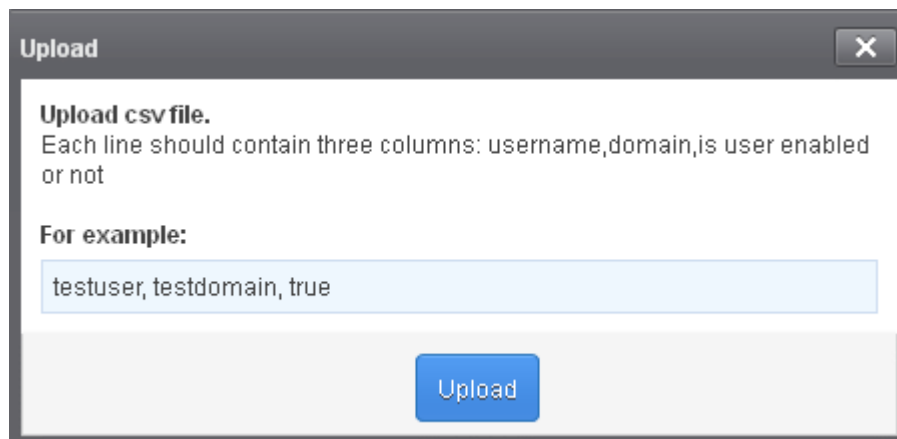
You can add many new users at a time by importing from a file. The users should be saved in 'comma separated value' (CSV) as shown below:

```
username1,domainname,true  
username2,domainname,false
```

- To import new users from a CSV file click More actions > Import from CSV file

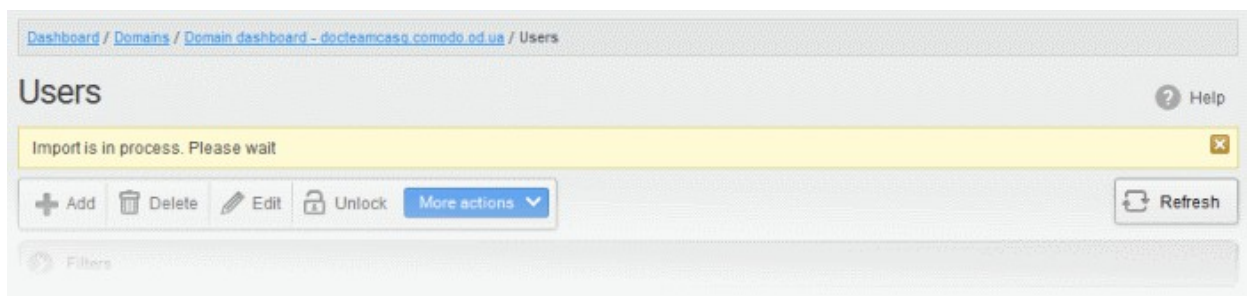


The Upload dialog will be displayed.



- Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button.

The upload progress will be displayed...



...and when completed, the results will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.ed.ua / Users

Users ? Help

Imported 1 user(s) ✕

1 users already exist ✕

+ Add
🗑 Delete
✎ Edit
🔒 Unlock
More actions ▾
🔄 Refresh

Filters

<input type="checkbox"/> Username	Enabled	Last login	Aliases	Group	Forward to
<input type="checkbox"/> alice	Yes			Users	
<input type="checkbox"/> bob	Yes	2015-06-30 10:17:29		Power Users	
<input type="checkbox"/> henry	No			Users	
<input type="checkbox"/> john	Yes	2015-06-30 10:27:45		Users	
<input type="checkbox"/> jsmith	No			Users	

⏪
⏩
1 / 1
⏪
⏩
[1 - 5 / 5]
Per page 15 ▾

The administrator who carried out the task will receive a notification about the import task completion.

Note: The number of users that can be added depends on the plan subscribed by you and the maximum number of users limit configured for the domain in the **Add Domains / Edit Domains / Domain Settings** interface. CASG will stop importing users after the number of users allowed for the account is reached and a warning will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.ed.ua / Users

Users ? Help

Imported 1 user(s) ✕

You cannot add more users as you have reached your maximum number of allowed users by license limitation, 1 users were imported ✕

+ Add
🗑 Delete
✎ Edit
🔒 Unlock
More actions ▾
🔄 Refresh

Filters

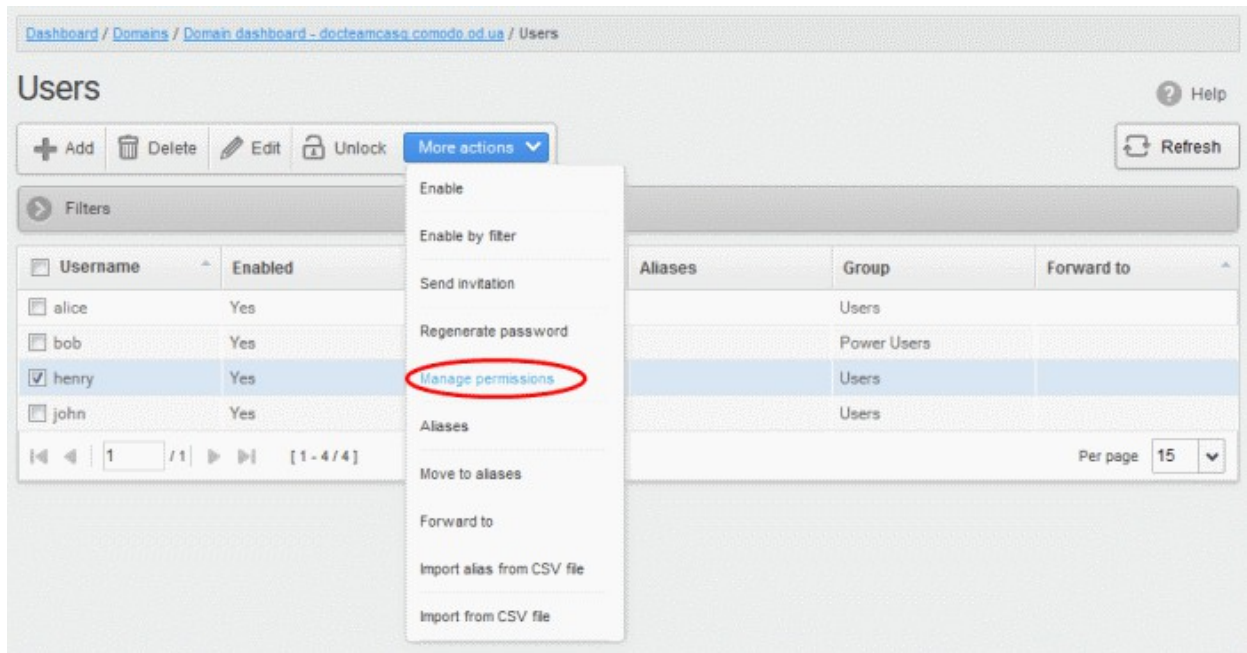
<input type="checkbox"/> Username	Enabled	Last login	Aliases	Group	Forward to
<input type="checkbox"/> alice	Yes			Users	

Managing Permissions for users

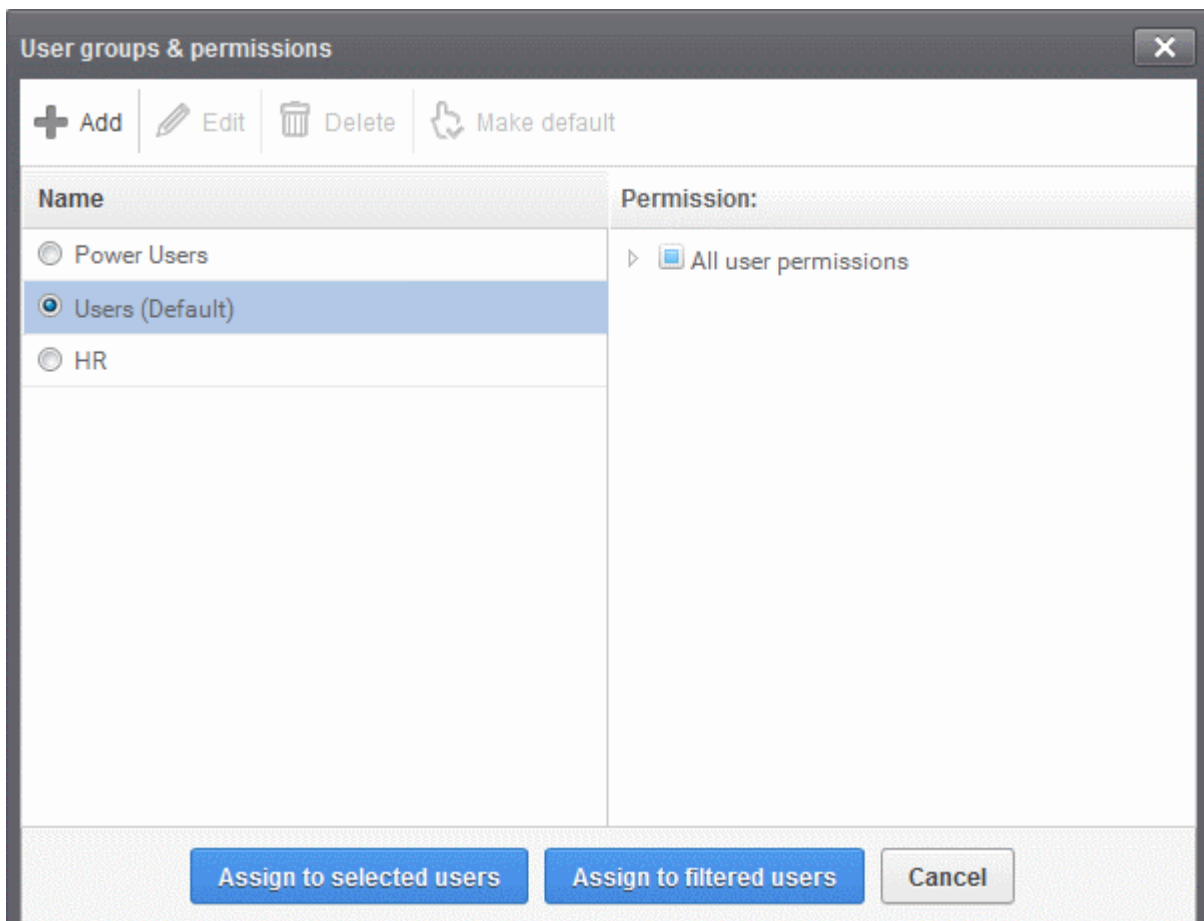
CASG allow administrators to assign permissions for users that will determine what the users can do and cannot do while logged into their respective CASG user interface. The administrators can create policies and assign them to users from this interface. See the section **'User Groups & Permissions'** for more details on how to create groups and policies. A new user will be automatically assigned default permission settings.

To assign permissions for a user

- Select the user(s) that you want assign permissions and click More actions > Manage permissions

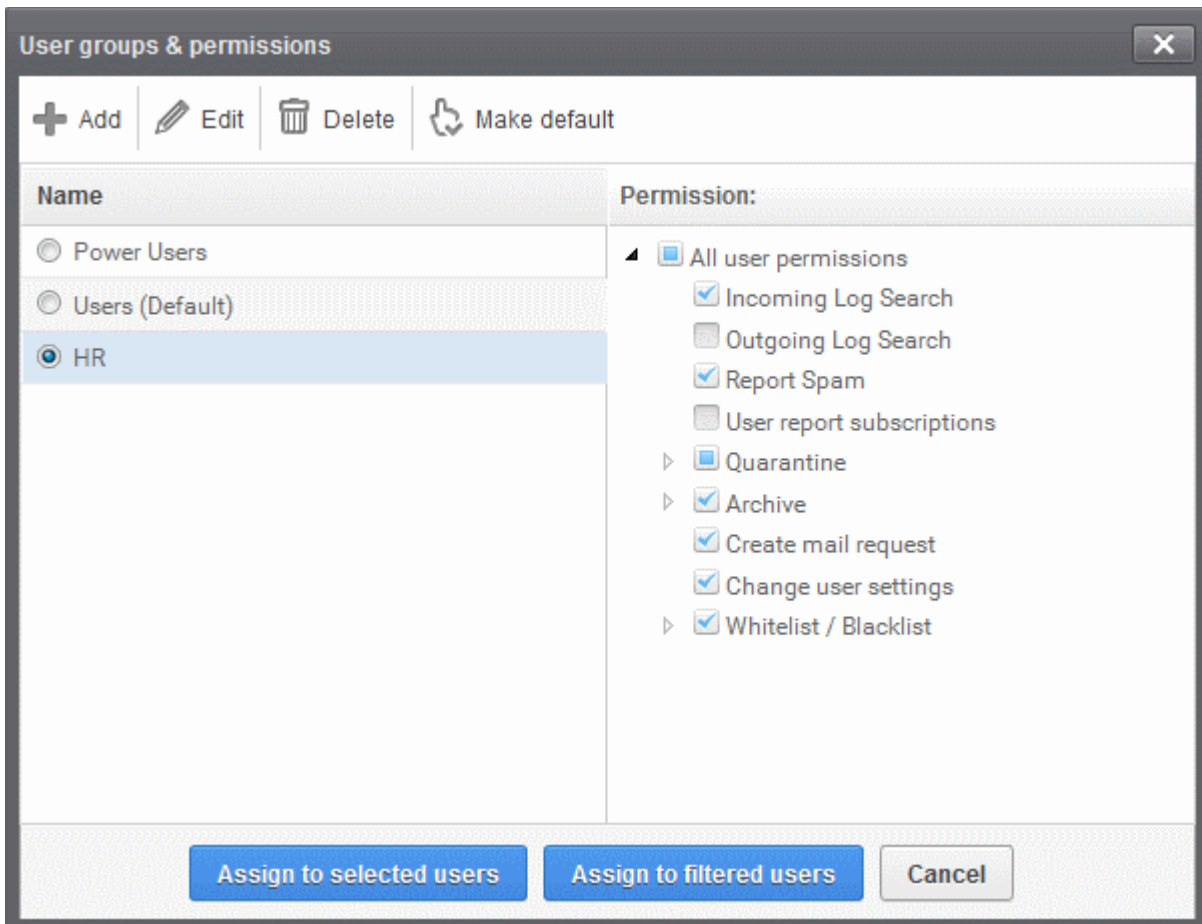


The 'User Groups & permissions' interface will be displayed.



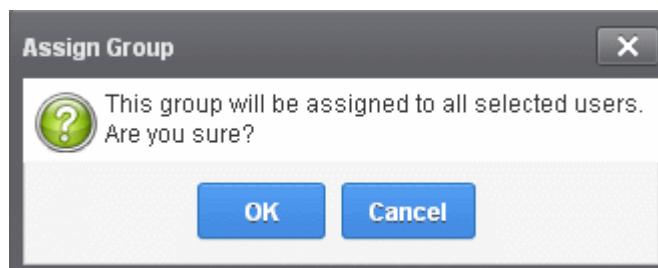
The interface displays the list of groups available with same or different permission levels for each group. By default, 'User (Default)' and 'Power User' groups will be available and administrators can add, edit groups and assign permissions to users. See the section **'Groups & Permissions'** for more details.

- Select the group from the list.



The permissions set for this group will be displayed on the right side.

- Click the 'Assign to selected users' button to set permissions for selected user or multiple users.
- Click 'Assign to filtered users' button to set permissions for selected group to all users or to all users found by filter.
- Click 'OK' in the confirmation window.



The selected user(s) will be assigned to the group and successfully assigned message will be displayed.

Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	
bob	Yes	2015-06-30 10:17:29		Power Users	
henry	Yes			HR	
john	Yes	2015-06-30 10:27:45		HR	

The interface also displays the new group assigned for the selected user under the 'Group' column.

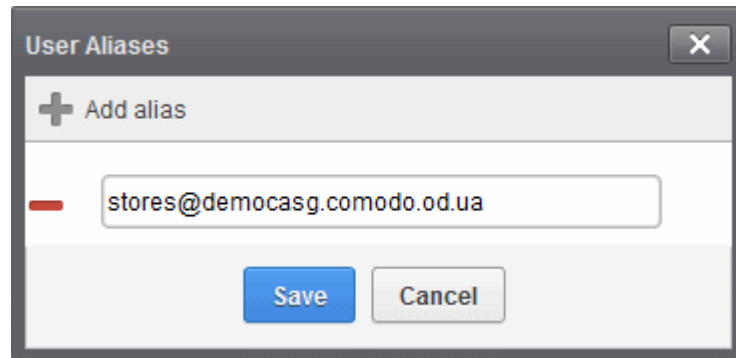
Adding the user aliases

CASG allows admins to add a user alias name to organize emails related to different groups or functions into a single email inbox automatically. The users can protect their real email address.

- Select a user and click 'More actions' > 'Aliases' to add user aliases.



Username	Enabled	Last login	Aliases	Group	Forward to
alice	Yes			Users	
bob	Yes	2015-06-30 10:17:29		Power Users	
henry	Yes			HR	
john	Yes	2015-06-30 10:27:45		HR	

- Enter the full email alias address of the user. Note: The alias email address must be of any domain belonging to the account.



- Click the Save button.

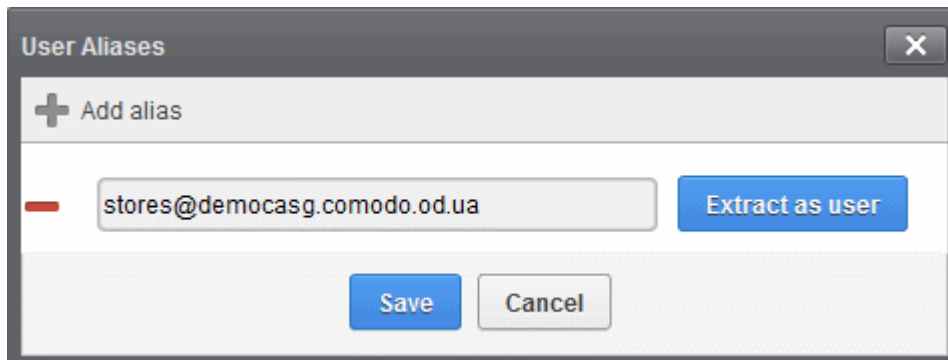
Note: Users cannot add an alias by themselves.

- To add multiple aliases click the  button.
- To remove an added alias row click the  icon beside it.

After adding a user to an alias, admins can extract him/her as a user.

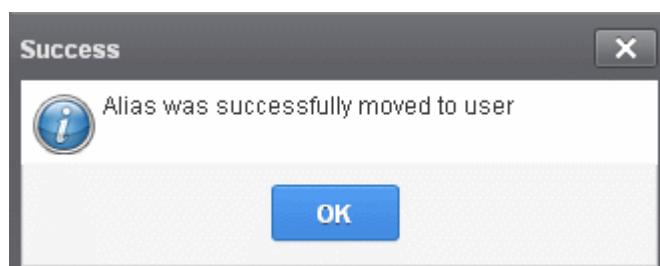
- Click the 'Aliases' button after selecting the user.

In the 'User Aliases' dialog next to the added alias row, the 'Extract as user' button will be displayed.



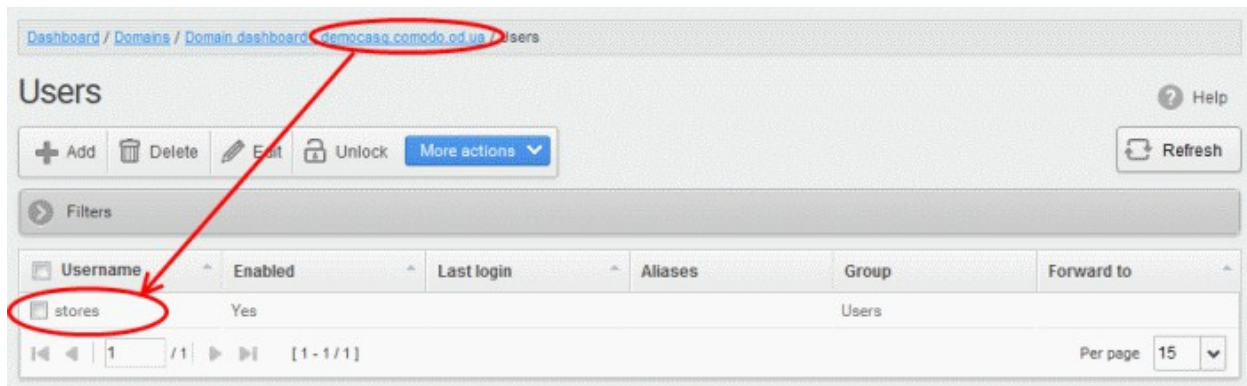
- Click the 'Extract as user' button.

The alias successfully moved message will be displayed.



- Click 'OK'

The user extracted from the 'User Aliases' dialog box will be added to list of users in the respective domain added as alias and will be placed in the default group.

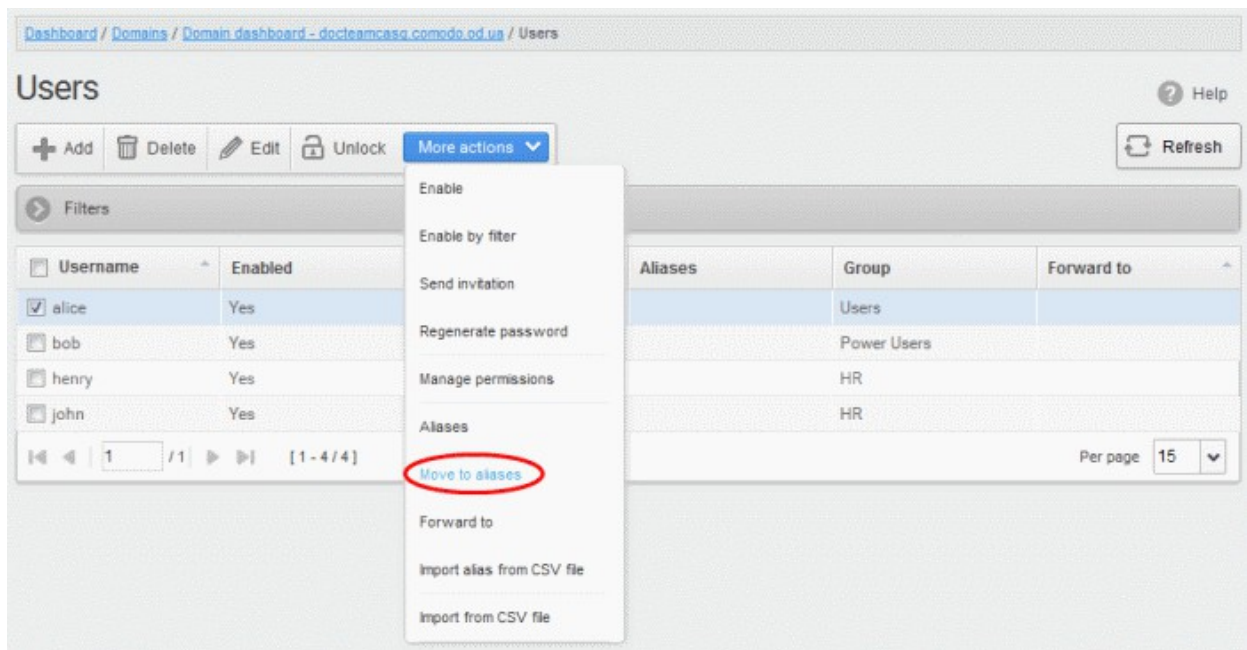


Note: The number of users that can be added for an account depends on the plan subscribed by you. When you exceed the limit of users, a warning will be displayed.

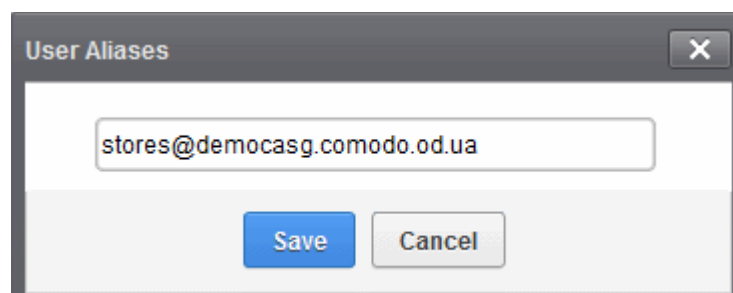
Moving user account to aliases

CASG allows admins to move an existing user as an alias for another user for any domain available in your account.

- Select the user that has to be moved as an alias and then click 'More actions' > 'Move to aliases'

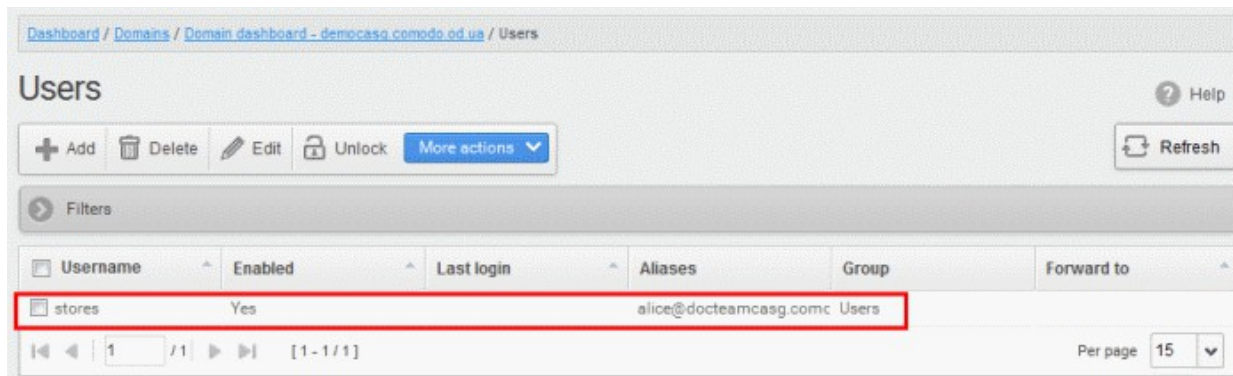


- Type the full email address of the user for whom the alias has to be added. Note: The user and domain should be valid and belong to your account.



- Click the 'Save' button.

Now, the selected user has become an alias of another user. (This could be for the same domain or another domain belonging to your account.)



Importing alias from CSV file

You can add many aliases to existing user(s) at a time for the selected domain and / or for other domains available for your account by importing from a file. The aliases should be saved in 'comma separated value' (CSV) as shown below:

Example 1

The following example shows how you can add alias for two users for the selected domain.

```
alias@domain.com username1, username2
```

Example 2

The following example shows how you can add alias for users for the selected domain and other domains available for your account.

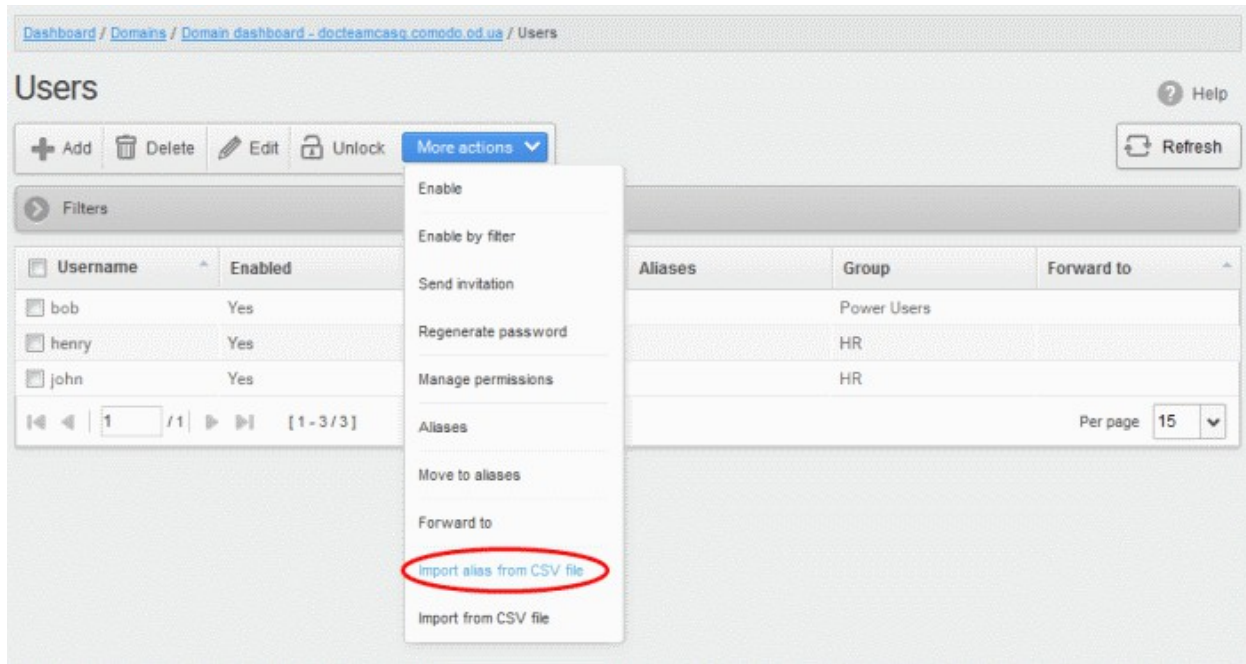
```
alias@domain.com username1, username2, username3@domain2
```

Please note that for adding many aliases at a time, each alias should be separated by a paragraph line. For example:

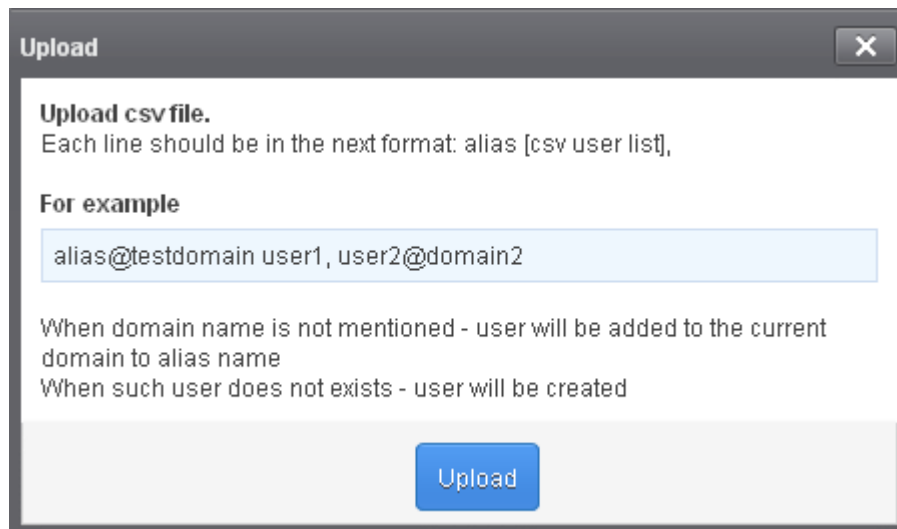
```
alias1@domain.com username1, username2
```

```
alias2@domain.com username1, username2, username3@domain2
```

- Click 'More actions' > 'Import alias from CSV file' to assign alias for users from a CSV file.

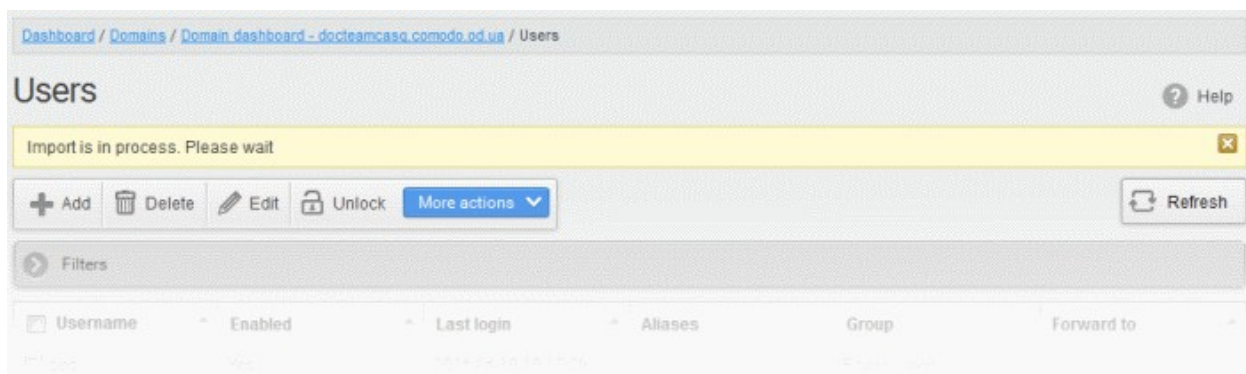


The Upload dialog will be displayed.

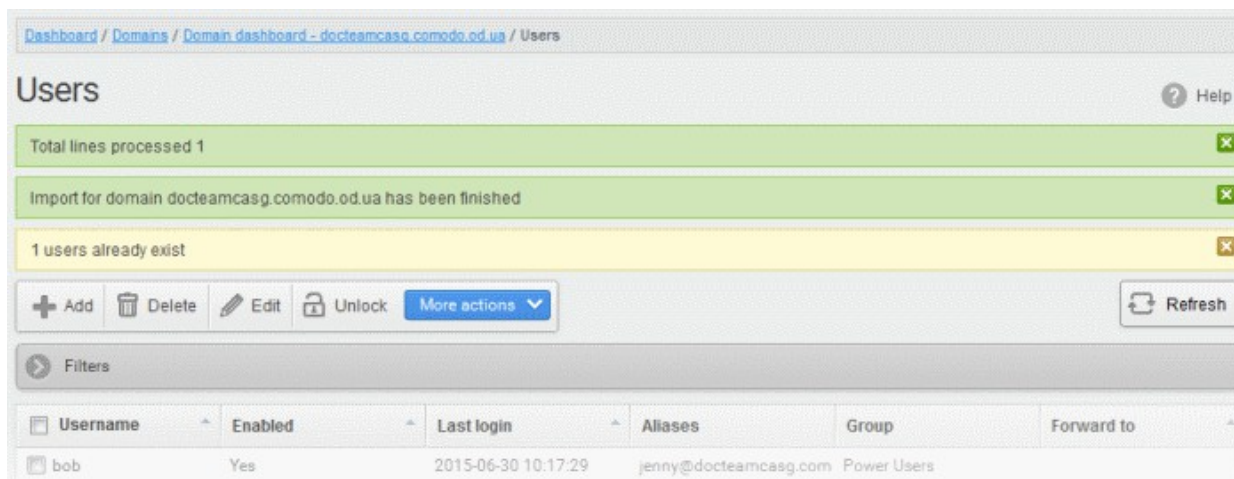


- Click the 'Upload' button and navigate to the location where the file is saved and click the 'Open' button.

The upload progress will be displayed...



...and when completed, the results will be displayed.

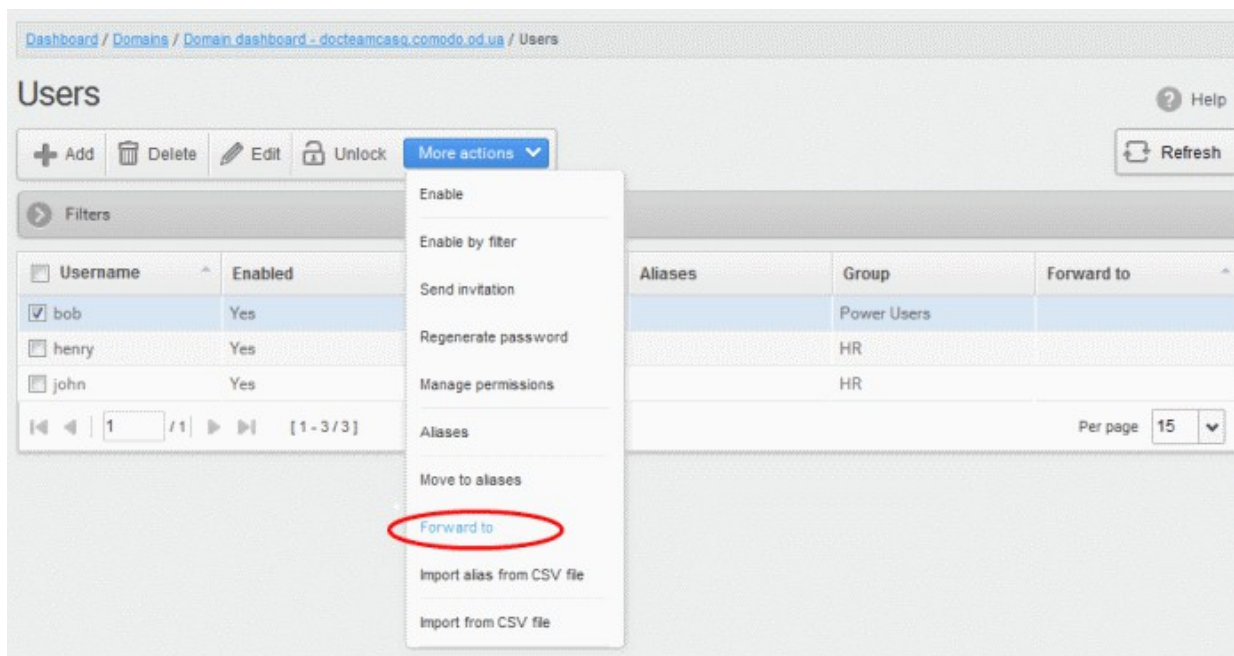


The administrator who carried out the task will receive a notification about the import task completion.

Forwarding mails to another user

CASG allows administrators to add a forwarding address for a user. This is useful when a user is on vacation or unavailable for sometime but the mails addressed to him should be attended immediately. Please note the forwarded user should also be in the same domain.

- Select the user whose mails have to be forwarded to another user and then click 'More actions' > 'Forward to'



The 'Forward settings...' dialog will be displayed:

- Select the 'Enable forwarding' check box
- Enter the user name of the recipient to whom the mails have to be forwarded in the 'Forward all user messages to' field
- Click the 'Save' button

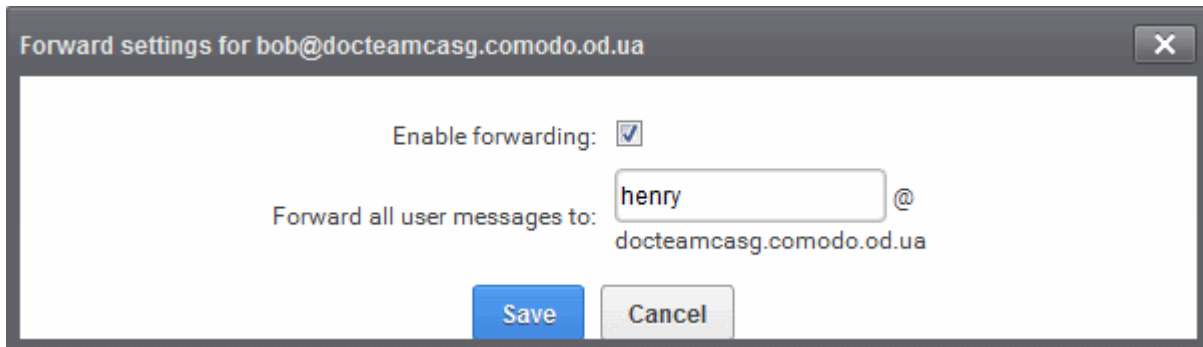
The forwarded user will be added and a success message will be displayed.

Username	Enabled	Last login	Aliases	Group	Forward to
bob	Yes	2015-06-30 10:17:29		Power Users	henry@docteamcasg.com
henry	Yes			HR	
john	Yes	2015-06-30 10:27:45		HR	

The incoming mails of the selected user will be automatically forwarded to the added user in the domain. When the selected user logs in to his/her CASG account, an alert will be displayed at the top of the interface.

- To remove the forwarded mail address for a user, select the user, click 'More actions' > 'Forward to'

The 'Forward settings...' dialog will be displayed:



- Deselect the 'Enable forwarding' check box
- Delete the username in the 'Forward all user messages to' field
- Click the 'Save' button

The forwarded user will be removed and a success message will be displayed.

Other Actions

- To allow user to access to CASG interface, click the 'More actions' > 'Enable'. A confirmation dialog will be displayed.
- If you want to allow access to user selected by applying filter, apply filters and click 'More actions' > 'Enable by filter'. A confirmation dialog will be displayed.
- Click the 'More actions' and select the 'Regenerate password'. The password will be reset for the user in case it is forgotten. The new password will be sent to the user's email automatically. The user has to use this new password to access CASG. A confirmation dialog will be displayed.
- To send invitation to new created users, select users and click 'More actions' > 'Send invitation'. A confirmation dialog will be displayed.

3.2.1.1.4.7.2 Managing User auto-import

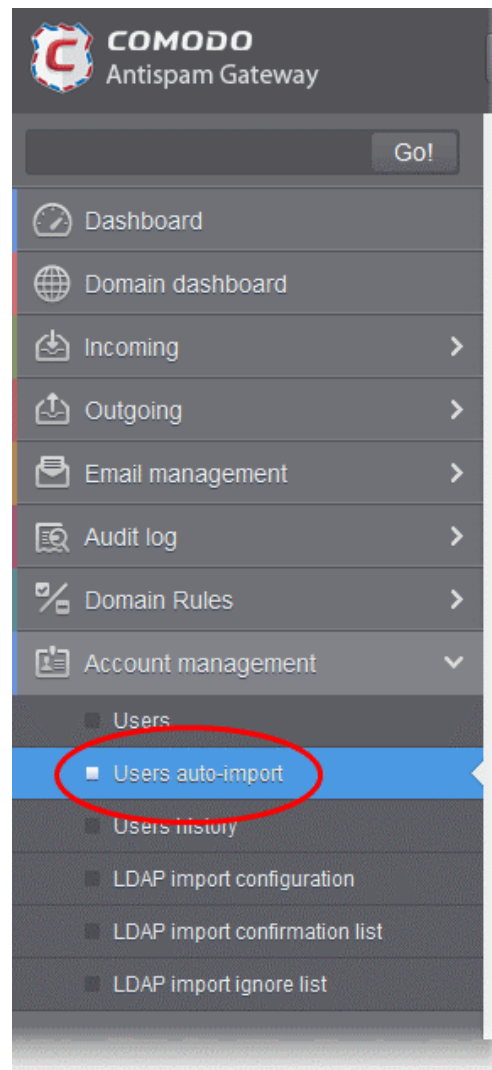
CASG has the ability to automatically import new users belonging to the managed domain, upon receiving the first accepted incoming mail, addressed to the new user at the mail server.

The administrator can enable the auto-import feature and configure it from the 'User auto-import' interface.

Each new user discovered, will be auto-imported in 30 minutes and will be sent with an invitation mail containing an activation link and credentials for their CASG user account. The new users need to activate their CASG User account by clicking the link in the invitation mail or logging-in to CASG User interface using the credentials provided in the mails. The administrators will also get a notification mail whenever a new user is auto-imported into CASG, if configured.

To access the Users Auto-Import interface

- Select 'Account management' from the left hand side navigation to expand it and choose 'Users auto-import' from the options



The 'Users auto-import' interface of the selected domain will be displayed.

[Dashboard](#) / [Domains](#) / [Domain dashboard - docteamcasg.comodo.od.ua](#) / Users auto-import

Users auto-import

Enable auto-import
 Automatically enable imported users
 Send invitation to imported users
 Notify administrators about imported users

Notification recipients:

- **Enable auto-import** - Select this option to enable the auto-import feature.
- **Automatically enable imported users** - Select this option, If you wish all the auto-imported new users to be 'Enabled' and their accounts with CASG are to be automatically activated, without

them having to login to CASG user interface.

- **Send invitation to imported users** - Sends invitation mails to newly imported users. The mail will contain the activation link and their login credentials.
- **Notify administrators about imported users** - Select this option if the administrator are to be notified whenever a new user is auto imported. You can specify administrators (including self) to whom the notification mails are to be sent in the 'Notification recipients' textbox. The notification contains the imported user name and a domain name.
- **Notification recipients** - Enter the email addresses of the administrators to whom the notification emails are to be sent. You can enter multiple address, separated by commas.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.ua / Users auto-import

Users auto-import

- Enable auto-import
- Automatically enable imported users
- Send invitation to imported users
- Notify administrators about imported users

Notification recipients:

- Click the 'Save' button for your settings to take effect.

Successfully saved

3.2.1.1.4.7.3 Viewing User History

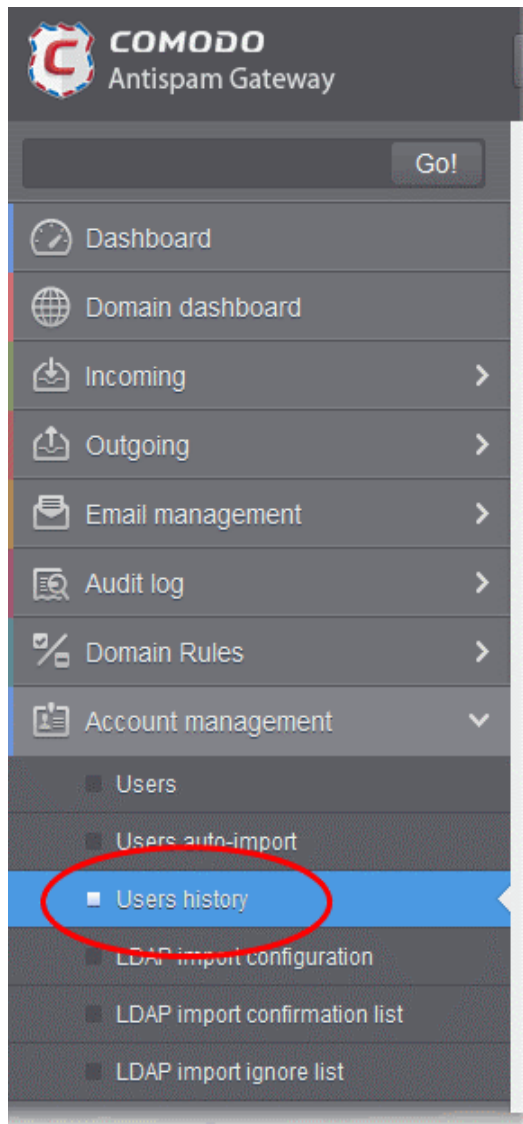
The 'Users History' area contains a record of user account connections within a particular date range. You can filter users by IP address, last login, domain, username and/or location.

Note: This interface will show user connections to the current domain only (the domain that is shown near the top of the interface). If required, you can view user connections for all domains in the '**Account Management section**' (click 'Dashboard' then in the 'Account Management' section, click 'User's History' sub tab).

The remainder of this page explains how to access the history interface and how to use filters to create custom searches.

Accessing the user history interface

- Click the 'Account management' tab on the left hand side navigation to expand and then click the 'Users history' sub tab.



The 'Users history' interface of the selected domain will be displayed.

Dashboard / Domains / Domain dashboard - docteamcasg.comodo.od.u / Users history

Users history Help

Filters

Username	Domain	IP	Location	Last login	Login duration (min)
bob	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-29 08:24:00	Currently logged in
bob	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-29 08:22:03	<1
john	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-26 07:36:41	25
john	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-26 05:57:04	1
john	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-26 05:17:08	38

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. The sorting option is not available for 'Login duration' column.

Using the filter option to search users

Click anywhere on the Filters tab to open the filters area.

The screenshot shows the 'Users history' page with a 'Filters' section. A single filter is applied: 'Username' with the condition 'contains'. Below the filters is a table with columns: Username, Domain, IP, Location, Last login, and Login duration (min). The table contains two rows of data for user 'bob'.

Username	Domain	IP	Location	Last login	Login duration (min)
bob	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-29 08:24:00	Currently logged in
bob	docteamcasg.comodo.od.u	125.17.11.121	India	2015-06-29 08:22:03	<1

You can add more filters by clicking  for narrowing down your search.

The screenshot shows the 'Users history' page with two filters applied. The second filter's dropdown menu is open, showing options: Username, Domain, IP, Location, and Last login. The table below shows the same data as the previous screenshot.

User	Domain	IP	Location	Last login	Login duration (min)
bob	eamcasg.comodo.od.u	125.17.11.121	India	2015-06-29 08:24:00	Currently logged in
bob	eamcasg.comodo.od.u	125.17.11.121	India	2015-06-29 08:22:03	<1

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.
- **Domain:** Will execute a search of domains according to the text in the text box (column 3) and the condition selected in column 2.
- **IP:** Will execute a search of IP addresses according to the number in the text box (column 3) and the condition selected in column 2.
- **Location:** Will execute a search of locations according to the text in the text box (column 3) and the condition selected in column 2.

If any of the above options is selected in the first drop-down, the following conditions are available:

- **Equals:** Displays all entries that match the text entered in the text box.
- **Not Equals:** Displays all entries except the one entered in the text box.
- **Contains:** Displays all entries that contain the words entered in the text box.
- **Not Contains:** Displays all entries that do not contain the words entered in the text box.
- **Starts With:** Displays all entries that start with the words entered in the text box.
- **Ends With:** Displays all entries that end with the words entered in the text box.

Other options available in the first drop-down in the filters area:

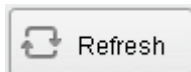
- **Last Login:** Sorts the results based on the last login details of users.

If 'Last Login' is selected, the following conditions are available:

- **Equals:** Displays the users whose last login is same as the selected date in the third box from the calendar
- **Less than:** Displays the users whose last login dates are less than the selected date in the third box from the calendar
- **Greater than:** Displays the users whose last login dates are greater than the selected date in the third box from the calendar
Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.



Click the  button to display all the users.

Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

3.2.1.1.4.7.4 Importing Users from LDAP

In addition to adding users manually and importing users from CSV file, CASG enables the administrators to import the users from the Active Directory (AD) server of the domain. You can configure CASG to access your AD server through Lightweight Directory Access Protocol (LDAP) to import the email users and to periodically synchronize with the AD server for automatic addition or removal of the users based on the changes made to the AD server.

Click the following links for more details:

- [LDAP Import Configuration](#)
- [LDAP Import Confirmation List](#)
- [LDAP Import Ignore List](#)
- [Troubleshooting LDAP](#)

LDAP Import Configuration

The LDAP Import Configuration interface allows the administrators to configure CASG to import the email users from the Domains's Active Directory and to set for periodical synchronization. Once Active Directory has been configured, CASG imports the users into its interface and updates it periodically. For example if a new user is added in the Active Directory, CASG can automatically add the new user to CASG.

Accessing the LDAP import configuration interface

- Open the 'Domains' interface and select the domain into which you want to import users.
- Select the domain from the list, click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' tab > 'LDAP import configuration' sub tab.

Comodo strongly recommends that a separate LDAP/AD account be created for the purposes of the ASG login and that this user account should be allocated read-only permissions.

The 'LDAP import configuration' interface will be displayed:

Dashboard / Domains / Domain_dashboard - docteamcasg.comodo.od.ua / LDAP import configuration

LDAP import configuration ? Help

Connection settings

Host (IP address or name):

Port: LDAP(389) | LDAPS(636)

Use SSL to connect?: Yes

Login/Query settings

LDAP login name:

Password: Remember credentials

Synchronization interval:

BaseDN:

Filter:

Mail attribute:

Override existing records

Allow CASG to create user accounts as found on LDAP server

Allow CASG to delete user accounts not found on LDAP server

Information

Send reports: Yes

Last synchronization time (GMT):

Connection Settings

- **Host (IP Address or Name)** - Enter the external hostname or external IP address of the AD server. If your Organization uses the same physical server for AD server and the Mail Exchange server, then enter the host name or IP address of the mail server.
- **Port** - Enter the port number of Active Directory Server's LDAP port.
 - 389 is the default port for non-SSL connection ('Use SSL To Connect' box NOT checked)
 - 636 is the default port if SSL connection is active ('Use SSL To Connect' box checked)
- **Use SSL To Connect?** - Select the 'Yes' check box if you wish us to use secure LDAP. In order to use secure LDAP, you need to install an SSL certificate from a Certification Authority (CA) like Comodo CA in your AD server. Self Signed certificates are not allowed.

Note: SSL access should have been enabled for AD Server before opting for SSL usage.

Login/Query Settings

- **LDAP login name:** - Enter the username of the user account using which CASG server can access the AD server. Preferably, a new user account can be created for the CASG server in the AD server with a new user name and password. The User account should have 'read' privileges to the AD server. The username can be of the format 'username' or 'username@domainname.com'
- **Password** - Enter the password of the LDAP user account.
- **Remember Credentials** - Enable this option if you wish CASG server to remember the username/password of the user account, in order to automatically login.

Note: If you are configuring for automatic periodic synchronization, CASG will store the username and password by default to connect to the AD server at the set time interval to update the user base, hence the option 'Remember Credentials' will not be visible. The option will be visible for you to enable or disable if 'Synchronization Interval' setting is set as 'no auto updates'.

- **Synchronization interval** - If you wish to configure CASG to automatically connect to the AD server and synchronize the user base, select the time interval for synchronization from the drop-down. Else, select 'No auto updates'.
- **BaseDN** - Distinguished Name of the user object in Active Directory. By default, the BaseDN field will contain the Domain Component (DC) values based on the domain name for which LDAP is configured. You can add/change the values of the strings 'Container Name (CN)', 'Organizational Unit (OU)' and 'domain name' depending on the users to be imported from the Active Directory.

Example: For adding users from Container 'Users', Organizational unit 'Organization' and domain 'example.com', the administrator has to enter the following:

CN=Users, OU = Organization, DC=example, DC=com

- **Filter** - Enables the Administrator to specify filter parameters users/addresses to be imported from the AD server. Each filter parameter should be defined within parentheses. Common filter parameters are explained below:
(objectClass=<AD user type>) - Specifies the user accounts to look for from the domain's Active Directory.
(Default = (objectClass=User))

(mail=*<domain name>) - Instructs CASG to import only the users that have a defined SMTP account within the domain. By default, the filter is pre-added with the parameter (mail=*@<current domain name>) to import the users that have email addresses on the current domain.

You can add any number of (mail=) filters if you wish to add several domain names

Example: (mail=*@domainname1.com)(mail=*@domainname2.com)

To import all email enabled users from the Active Directory irrespective of any specific domain name, enter the parameter as '(mail=*)'.

To modify a filter parameter to be exclusive rather than inclusive, add an exclamation mark (!) before the opening parenthesis of any parameter. This will instruct the query to ignore any users which fall into that category. For example, if one wanted to configure a query to find users with mail enabled at any domain EXCEPT domainname.com, the filter should include the following: (mail=*)!
(mail=*@domainname.com).

To import all email enabled users from the Active Directory irrespective of any specific domain name, enter the parameter as '(mail=*)'.

Note:

- CASG can only import LDAP users that have email addresses on domains that you have added to CASG in the **Domains** interface.
- To successfully import users, you must make sure the domain of their email addresses has been added to CASG AND that the LDAP Import is configured for each individual domain from the **Domain Management Area** of the respective domain.

- **Mail attribute** - Enter the LDAP display name of the contact email address attribute of the AD Server. By default, this attribute name will be 'mail' for AD servers or the distinguished name (DN) or common user login name for the AD server. On other servers like Novel or OpenLDAP this attribute may be different and server specific.

Override existing records:

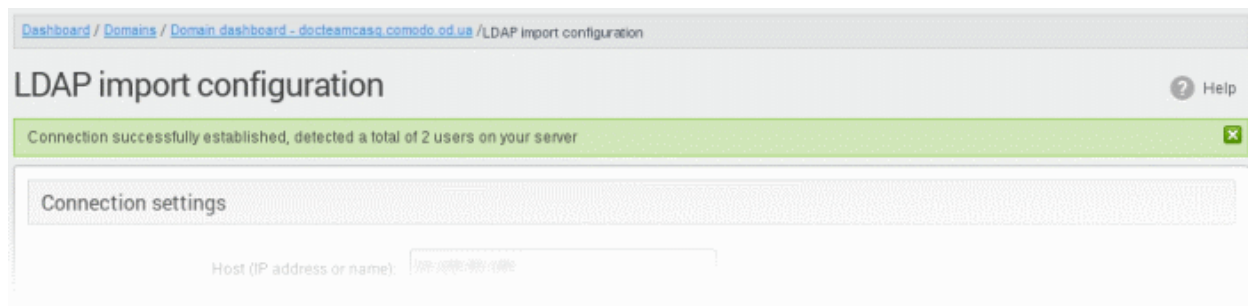
- **Allow CASG to create user accounts as found on LDAP server** - Select this checkbox if you wish new

users added in the AD server to be automatically added to CASG during synchronization. If you do not select this option, you can manually import the new users from the [LDAP import confirmation page](#).

- **Allow CASG to delete user accounts not found on LDAP server** - Select this checkbox if you wish users removed from AD server, to be automatically removed from CASG during synchronization. If you do not select this option, you can manually remove users from the [LDAP import confirmation page](#).

Information Settings

- **Send Reports** - If enabled, CASG will send email notifications to the administrator whenever new users are created or users are removed either automatically, (if 'Allow to create users?'/ 'Allow to delete users?' are enabled) or manually from the LDAP import confirmation page.
- **Last synchronization time (GMT)** - Displays the date and time of last manual or scheduled synchronization with AD server, in GMT.
- **Notification area** - Contains information about errors that occurred during synchronization. In most cases, this will contain the same information that is provided with the "Test connection" feature. Note - this area is only visible if errors occur.
- To check the configuration and connectivity, click 'Test Connection'. If the connection is established successfully then the success message will be displayed with the total number of users detected from the AD server.



- To save your configuration, click 'Save'.
- To Save your configuration and run a manual synchronization of user base with the AD server instantly, click 'Save and run synchronization' now

LDAP Import Confirmation List

The LDAP import confirmation list interface displays the list of:

- Users created at the AD server and not yet been imported into CASG
- Users not present on AD server and not yet been removed from CASG

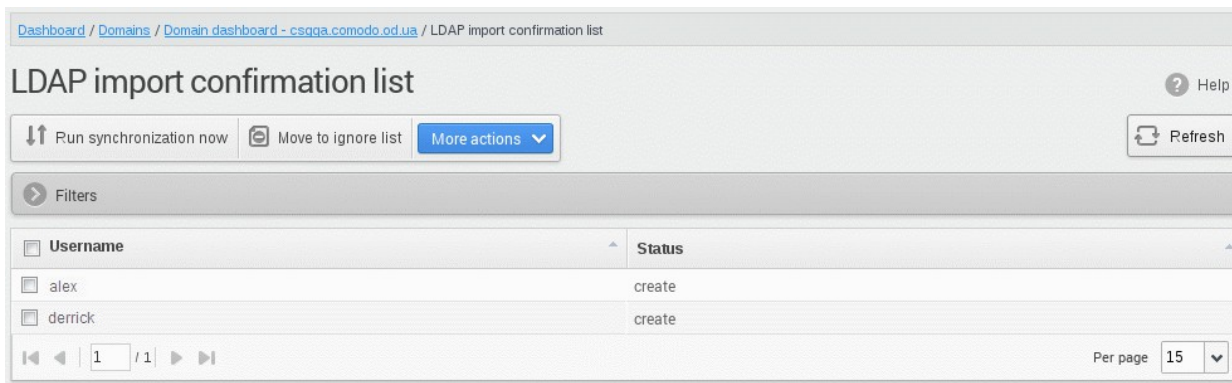
... if "**Allow to create users?**" / "**Allow to delete users?**" are not enabled in [LDAP import configuration interface](#), along with the list of users created in CASG. The administrator can import the users created at AD server into CASG manually and remove existing users from this interface.

Also, the administrator can initiate an on-demand synchronization from this interface.

Accessing the LDAP import confirmation list interface

- Open the 'Domains' interface and select the domain into which you want to import users.
- Select the domain from the list, click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' tab > 'LDAP import confirmation list' sub tab.

The 'LDAP import confirmation list' interface will be displayed:

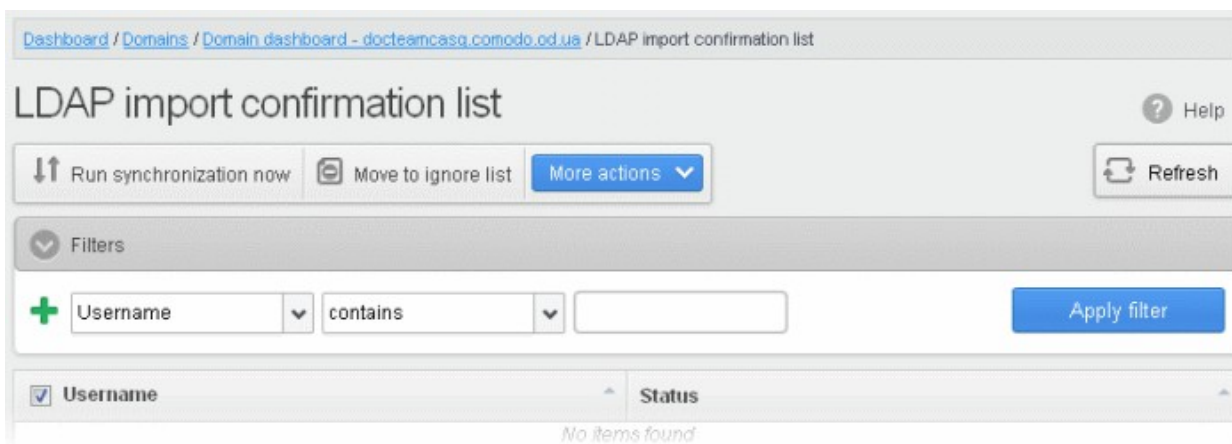


The list of users added to and deleted from the AD server with the existing users created at CASG will be displayed. This list reflects difference between CASG users and AD users, considering **LDAP ignore list**.

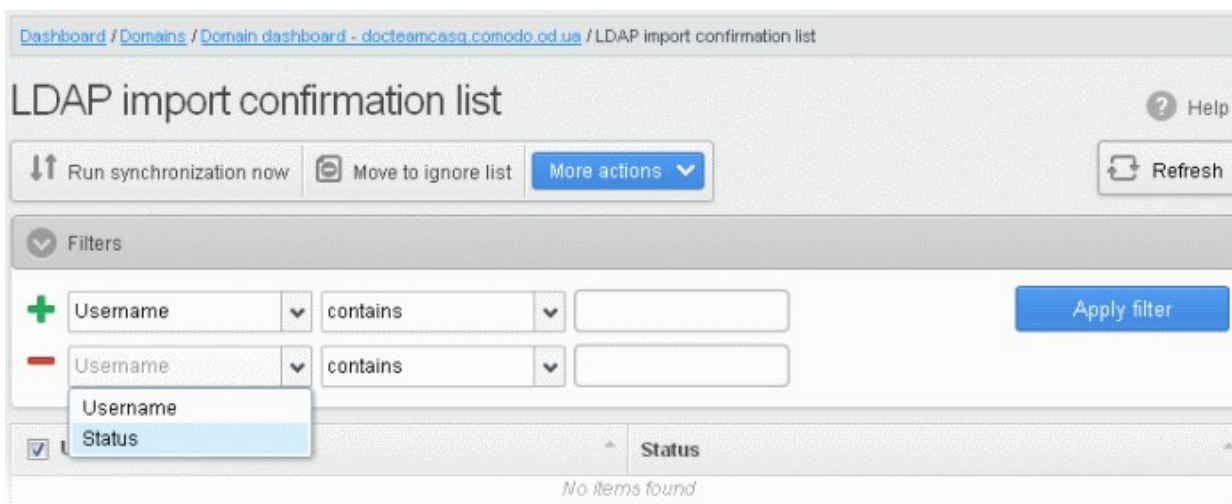
- Users created at the AD server and not present in CASG will be displayed with the status 'Create'
- Users not present on the AD server but present in CASG will be displayed with the status 'Delete'

Using the filter option to search users

Click anywhere on the Filters tab to open the filters area.



You can add more filters by clicking **+** for narrowing down your search.



You can remove a filter by clicking the **-** icon beside it.

Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

If 'Username' is selected, the following conditions are available:

- **Equals:** Displays all usernames that match the text entered in the text box.
- **Not Equals:** Displays all users except the one entered in the text box.
- **Contains:** Displays all username(s) that contain the words entered in the text box.
- **Not Contains:** Displays all username(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all username(s) that start with the words entered in the text box.
- **Ends With:** Displays all the username(s) that end with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Status:** Sorts the results based on whether a user's status is 'Create' or 'Delete' selected from third column and condition selected from second column.

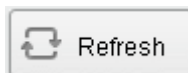
If 'Status' is selected, the following conditions are available:

- **Equals:** Displays the users whose status is as chosen in third column
- **Not Equals:** Displays the users whose status is opposite to that chosen in third column

Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

Click anywhere on the Filters tab to close the filters area.



Click the  button to display all users.

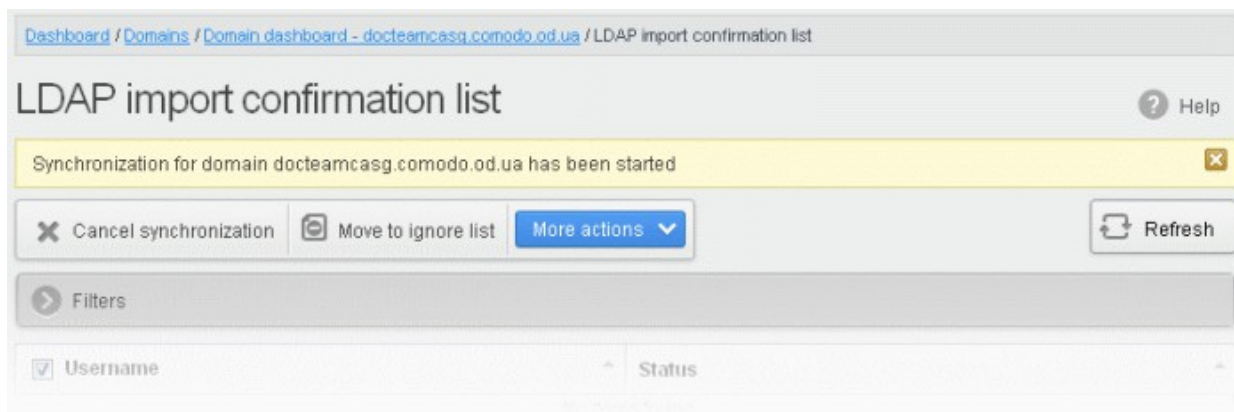
Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

- To run a manual on-demand synchronization, click 'Run synchronization now'

If you have not selected the option **Remember credentials** in **LDAP Import Configuration interface**, you will be asked to enter the username and password for CASG to access the AD server.

A dialog box titled 'Connection credentials' with a close button (X) in the top right corner. It contains two text input fields: 'LDAP login name:' and 'Password:'. Below the fields are two buttons: 'OK' (blue) and 'Cancel' (grey).

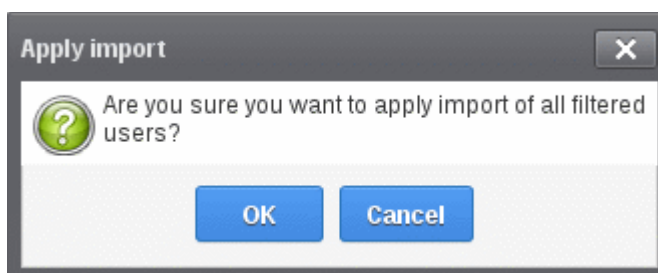
- Enter the LDAP login credentials and click 'OK'.



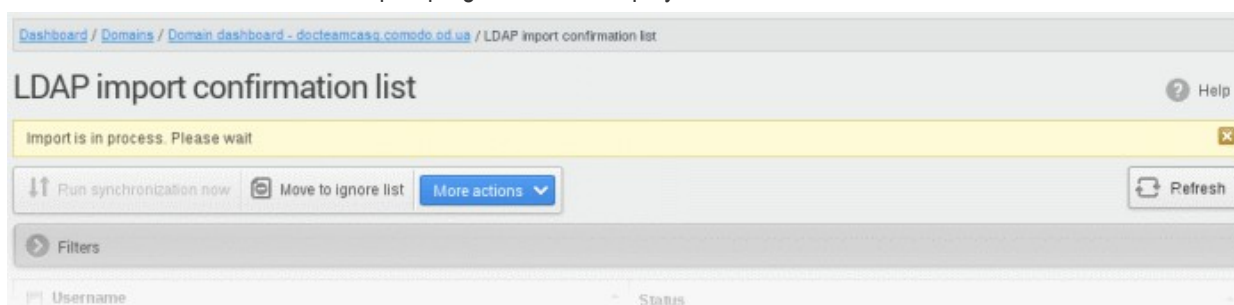
CASG server will connect to your AD server and start detecting the changes in the users in the AD server.

All the users added to the AD server will be displayed as a list.

- To import or delete users selected by applying filter, apply filters as described **above** and click 'More actions' > 'Apply import by filter'.
- To import or delete a set of selected users, select the users and click 'More actions' > 'Apply import by selection'.
- To import all users created at the AD server and to delete all the users removed from AD server at once, clear all the filters and click 'More actions' > 'Apply import by filter'. A confirmation dialog will be displayed.



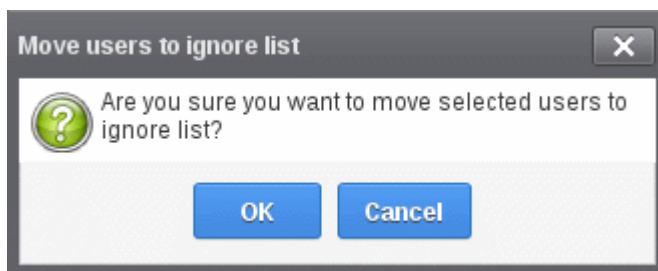
- Click OK. The import progress will be displayed.



On completion, the selected users will be imported or deleted in synchronization with the AD server.

Note: The number of users that you can add for all the domains belonging to your account depends on your subscription plan. For example, if the subscription plan for your account allows you to add 1000 users and you have three domains, then you can add 300 users for domain 1, 300 users for domain 2 and 400 users for domain 3. You can set any value between 0 and 999999 in the 'Max. number of users' field in the **Add Domains / Edit Domains / Domain Settings** interface, but CASG checks if the total number of users for all domains is within your license limit.

- To move selected users to Ignore List, select the users and click 'Move to ignore list'



... and click 'OK' in the confirmation dialog.

Users moved to **ignore list** will be skipped from next synchronization with the AD server.

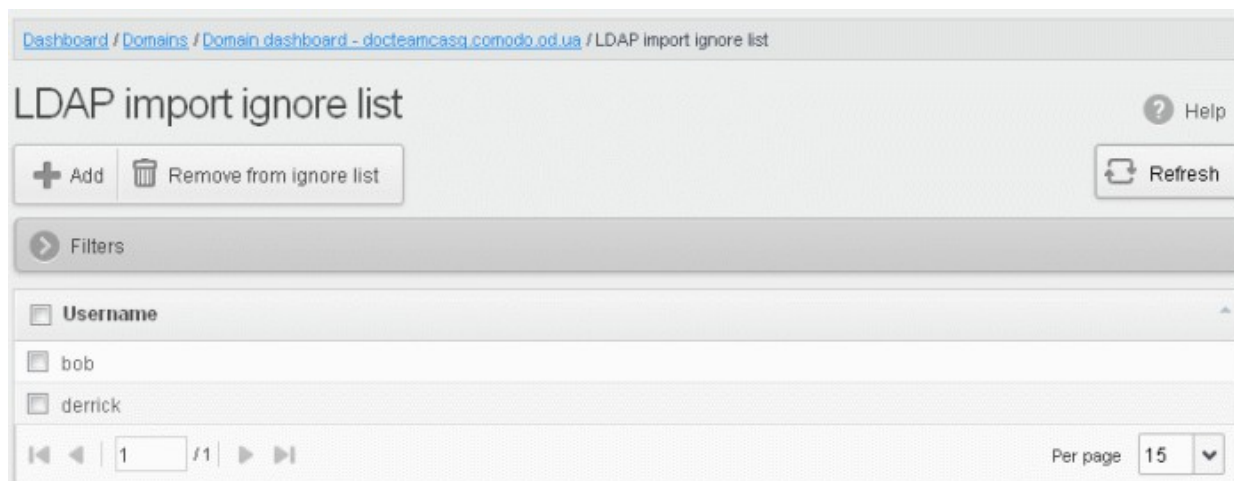
LDAP Import Ignore List

The LDAP import ignore list interface displays a list of users to be skipped from being created or deleted in CASG during synchronization with the AD server. Users can be moved to ignore list from the LDAP Import Confirmation List interface or manually added. Once added to the ignore list, the user will be skipped from the AD server from the next synchronization operation.

Accessing the LDAP import ignore list interface

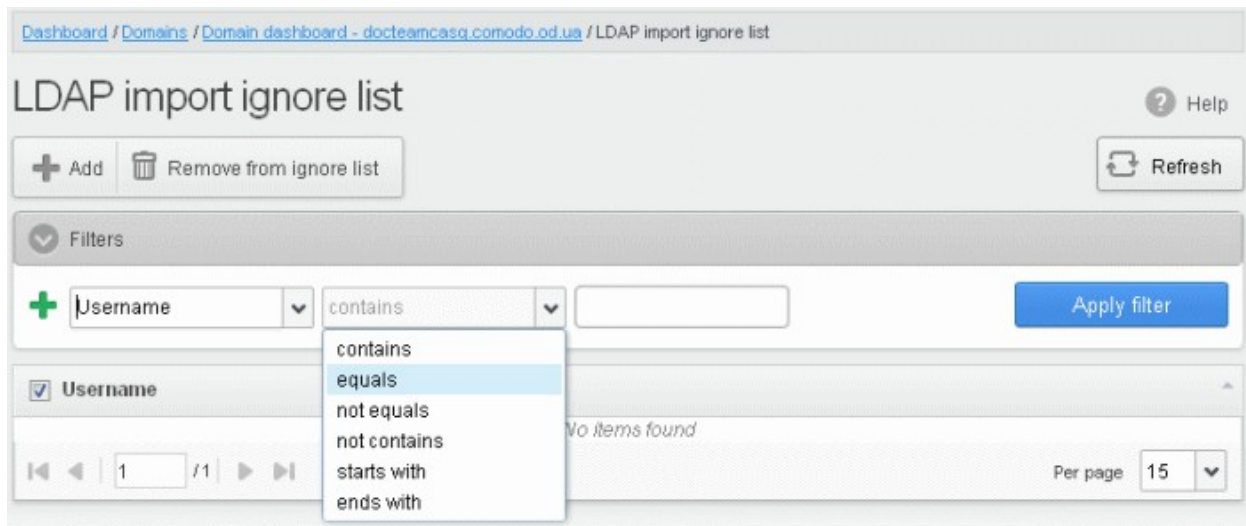
- Open the 'Domains' interface and select the domain into which you want to import users.
- Select the domain from the list, click the 'Manage Domain' button to open the 'Domain Management' interface.
- Click 'Account management' tab > 'LDAP import ignore list' sub tab.

The 'LDAP import ignore list' interface will be displayed.



Using the filter option to search users

- Click anywhere on the Filters tab to open the filters area.



Available filters are:

- **Username:** Will execute a search of usernames according to the text in the text box (column 3) and the condition selected in column 2.

The following conditions are available:

- **Equals:** Displays all usernames that match the text entered in the text box.
- **Not Equals:** Displays all users except the one entered in the text box.
- **Contains:** Displays all username(s) that contain the words entered in the text box.
- **Not Contains:** Displays all username(s) that do not contain the words entered in the text box.
- **Starts With:** Displays all username(s) that start with the words entered in the text box.
- **Ends With:** Displays all the username(s) that end with the words entered in the text box.
- Click 'Apply Filter' after selecting the filters.

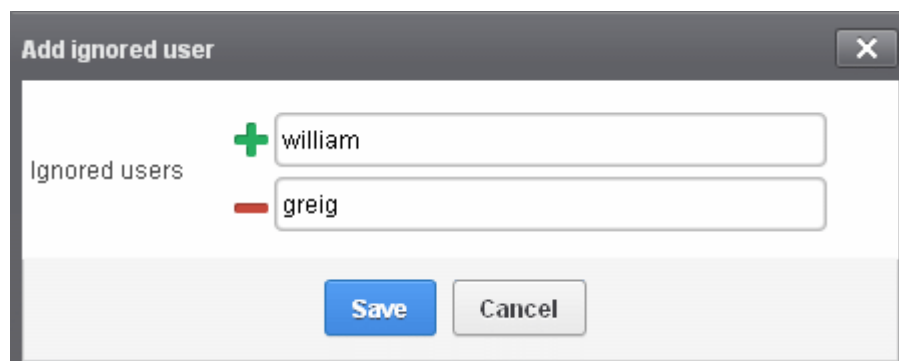
The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.
- Click the  button to display all users.

Note: To display all the users after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add users to ignore list

- Click 'Add'. The Add ignored user dialog will be displayed.



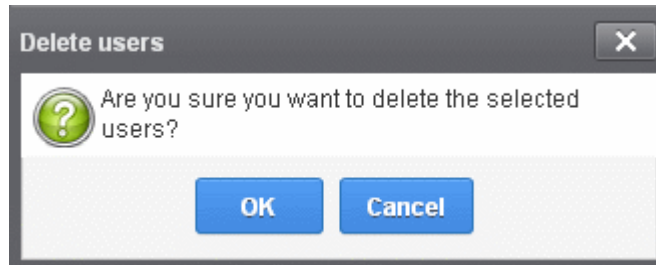
- Enter the user names to be added to the ignore list

- Click the **+** icon to add more users
- Click Save to add the users.

A 'Successfully added' message will be displayed at the top.

To remove the users from the ignore list

- Select the users and click 'Remove from ignore list'. A confirmation dialog will be displayed.



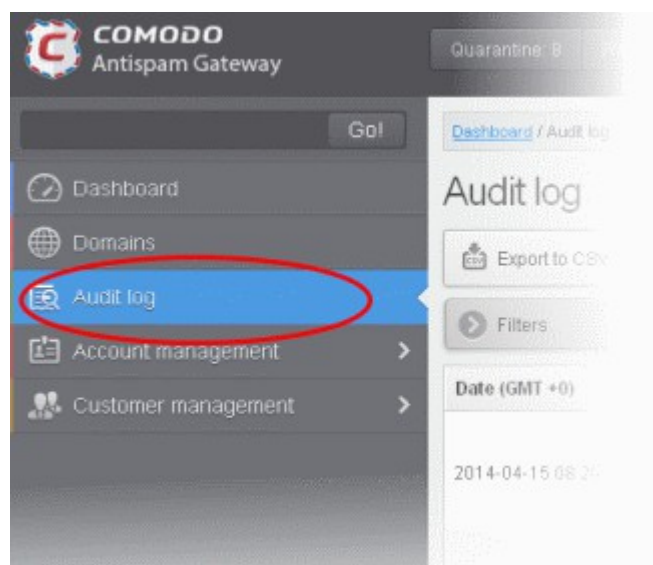
- Click OK.

The users will be removed from the list and a 'Successfully deleted' message will be displayed at the top.

- Users removed from the ignore list will be imported to or deleted from CASG based on changes in the AD server, during the next synchronization if '**Allow to create users?/Allow to delete users?**' are enabled in **LDAP import configuration interface**.
- Users removed from the ignore list will be listed in the LDAP import confirmation list interface based on changes in the AD server, during the next synchronization if '**Allow to create users?/Allow to delete users?**' are not enabled in **LDAP import configuration interface**.

3.2.2 Audit Log

CASG keeps a record of actions initiated by users and administrators for all domains belonging to an account. The Audit Log area allow administrators with appropriate privileges to view these log reports. CASG also keeps logs of domains separately for each domain. For more details on selected domain audit log, refer to the section **Domain Audit Log**. This section explains about the consolidated log for all domains available in the account.



The log details for all the domains will be displayed.

Dashboard / Audit log

Audit log

Export to CSV by filter Refresh

Filters

Date (GMT +0)	Domain	Role	Login	Operation key	Operation description	Details
2014-10-28 16:30:52	docteamcasg.comodo.od.ua	system		ACCEPT_AND_J	Accept and archive message	Recipients: john@docteamcasg.comodo.od.ua; Sender: admin@antispamgateway.comodo.com; Date: Tue Oct 28 14:53:04 GMT 2014; Subject: New account registered
2014-10-28 16:30:51	docteamcasg.comodo.od.ua	system		ACCEPT_AND_J	Accept and archive message	Recipients: john@docteamcasg.comodo.od.ua; Sender: admin@antispamgateway.comodo.com; Date: Tue Oct 28 14:53:04 GMT 2014; Subject: New account registered
2014-10-28 16:30:29	docteamcasg.comodo.od.ua	system		ACCEPT_AND_J	Accept and archive message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: admin <demo@csg.comodo.od.ua>; Date: Tue Oct 28 13:37:58 GMT 2014; Subject: Re: DQ demo
2014-10-28 16:28:51	docteamcasg.comodo.od.ua	system		ACCEPT_AND_J	Accept and archive message	Recipients: demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua; Sender: admin <demo@csg.comodo.od.ua>; Date: Tue Oct 28 13:38:30 GMT 2014; Subject: DQ demo 2

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column. The sorting option is not available for 'Operation description' column.

Using Filter options to search particular event(s)

- Click anywhere on the 'Filters' tab to open the filters area.

Dashboard / Audit log

Audit log

Export to CSV by filter Refresh

Filters

+ Domain contains

Apply filter

Date (GMT +0)	Domain	Role	Login	Operation key	Operation description	Details
2014-04-7 12:02:13	csg-arch-qa.comodo.od.ua	superadmin		DELETE_EMAIL_FF	Delete archived message	Recipients: user@csg-arch-qa.comodo.od.ua; Sender: Elogvinenko

You can add more filters by clicking  for narrowing down your search.

Dashboard / Audit log

Audit log

Export to CSV by filter

Filters

+ Domain contains

- Date equals

Date
Domain
Role
Login
Operation description
Details

Date	Domain	Role	Login	Operation key
2014	g-arch-qa.comodo.od.ua	superadmin		DELETE_EMAIL

You can remove a filter by clicking the  icon beside it.

Available filters are:

- **Domain:** Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Login:** Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.
- **Details:** Will execute a search of log entries according to the text entered in the text box (column 3) and the condition selected in column 2.

When you select any one of the above options in the first drop-down, the following conditions are available:

- **Contains:** Displays all log entries that contain the words entered in the text box
- **Equals:** Displays all log entries that contain only the words entered in the text box
- **Not Equals:** Displays all log entries that do not contain only the words entered in the text box
- **Not Contains:** Displays all log entries that don't contain the words entered in the text box
- **Starts with:** Displays all log entries that starts with the words entered in the text box
- **Ends with:** Displays all log entries that ends with the words entered in the text box

Other options available in the first drop-down in the filters area:

- **Date:** Will execute a search of log entries according to the date selected in the calendar box (column 3) and the condition selected in column 2.
- **Role:** Will execute a search of log entries according to the role selected in the third field (column 3) and the condition selected in column 2.
- **Operation Description:** Will execute a search of log entries according to the action selected in the third field (column 3) and the condition selected in column 2.

If 'Date' is selected, the following conditions are available:

- **Equals:** Displays the entries that have the same date as the selected date in the third box from the calendar
- **Less than:** Displays the entries with dates less than the selected date in the third box from the calendar
- **Greater than:** Displays the entries with dates greater than the selected date in the third box from the calendar

If 'Role' is selected, the following conditions are available:

- **Equals:** Displays all log entries that is equal to the role selected in column 3.
- **Not Equals:** Displays all log entries that except the role selected in column 3.

If 'Operative description' is selected, the following conditions are available:

- **Equals:** Displays all log entries that is equal to the event selected in column 3.
- **Not Equals:** Displays all log entries that except the event selected in column 3.

- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all the entries.

The following table provides the details of actions initiated by user/administrator and shown under Operation Key and Operation Description columns in the log report:

S.No.	Operation Key	Operation Description
1	DELETE_EMAIL_FROM_QUARANTINE_BY_FILTER	Delete quarantined messages by filter
2	DELETE_EMAIL_FROM_QUARANTINE	Delete quarantined message
3	RELEASE_EMAIL_FROM_QUARANTINE	Release quarantined message
4	WHITELIST_RECIPIENT	Whitelist recipient
5	BLACKLIST_RECIPIENT	Blacklist recipient
6	UNWHITELIST_RECIPIENT	Remove recipient from the whitelist
7	UNBLACKLIST_RECIPIENT	Remove recipient from the blacklist
8	WHITELIST_SENDER	Whitelist sender
9	BLACKLIST_SENDER	Blacklist sender
10	UNWHITELIST_SENDER	Remove sender from the whitelist
11	UNBLACKLIST_SENDER	Remove sender from the blacklist
12	RESET_TO_DEFAULT_WHITELISTED_SENDERS	Reset senders whitelist
13	RESET_TO_DEFAULT_WHITELISTED_RECIPIENTS	Reset recipients whitelist
14	RESET_TO_DEFAULT_BLACKLISTED_SENDERS	Reset senders blacklist
15	RESET_TO_DEFAULT_BLACKLISTED_RECIPIENTS	Reset recipients blacklist
16	WHITELIST_SENDER_DOMAIN	Whitelist all senders of the domain
17	WHITELIST_RECIPIENT_DOMAIN	Whitelist all recipients of the domain

18	BLACKLIST_SENDER_DOMAIN	Blacklist all senders of the domain
19	BLACKLIST_RECIPIENT_DOMAIN	Blacklist all recipients of the domain
20	USER_WHITELIST_REQUEST_PER_USER	Request whitelist sender for user
21	USER_BLACKLIST_REQUEST_PER_USER	Request blacklist sender for user
22	USER_RELEASE_REQUEST	Release request
23	USER_CANCEL_WHITELIST_REQUEST_PER_USER	Cancel request whitelist sender for user
24	USER_CANCEL_BLACKLIST_REQUEST_PER_USER	Cancel request blacklist sender for user
25	USER_CANCEL_RELEASE_REQUEST	Cancel release request
26	ACCEPT_WHITELIST_REQUEST_PER_USER	Accept request whitelist sender for user
27	ACCEPT_BLACKLIST_REQUEST_PER_USER	Accept request blacklist sender for user
28	ACCEPT_RELEASE_REQUEST	Accept release request
29	REJECT_WHITELIST_REQUEST_PER_USER	Reject request whitelist sender for user
30	REJECT_BLACKLIST_REQUEST_PER_USER	Reject request blacklist sender for user
31	REJECT_RELEASE_REQUEST	Reject release request
32	SPAM_DETECTION_SETTINGS	Update spam detection settings
33	SPAM_DETECTION_SETTINGS_RESET_TO_DEFAULT	Reset spam detection settings
34	DELETE_EMAIL_FROM_ARCHIVE_BY_FILTER	Delete archived messages by filter
35	DELETE_EMAIL_FROM_ARCHIVE	Delete archived message
36	RESEND_EMAIL_FROM_ARCHIVE	Resend archived message
37	REPORTS_AS_SPAM	Reports archived message as a SPAM
38	QUARANTINE_EMAIL	Quarantine message
39	ACCEPT_AND_ARCHIVE_EMAIL	Accept and archive message
40	MARK_EMAIL_AS_SPAM	Mark message as spam
41	ACCEPT_EMAIL	Accept message
42	WHITELIST_USER_SENDER	Whitelist sender for user
43	BLACKLIST_USER_SENDER	Blacklist sender for user
44	UNWHITELIST_USER_SENDER	Remove sender from the user whitelist
45	UNBLACKLIST_USER_SENDER	Remove sender from the user blacklist

46	QUARANTINE_REPORT_SUBSCRIPTION_UPDATE	Quarantine report subscription update
47	QUARANTINE_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Quarantine report subscription reset to default
48	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_UPDATE	Domain report subscription update
49	DOMAIN_STATISTICS_REPORT_SUBSCRIPTION_RESET_TO_DEFAULT	Domain report subscription reset to default
50	DOMAIN_ADD	Add domain
51	DOMAIN_DELETE	Remove domain
52	ADMIN_ADD	Add admin
53	ADMIN_EDIT	Edit admin settings
54	ADMIN_DELETE	Remove admin
55	ADMIN_UNLOCK	Unlock admin
56	ADMIN_REGENERATE_PASSWORD	Regenerate password for admin
57	ADMIN_PASSWORD_UPDATE	Update password for admin
58	SYSTEM_NOTIFICATIONS_TEMPLATE_CHANGE	System notifications template change
59	ADMIN_PERMISSIONS_GROUP_ADD	Add admin permission group
60	ADMIN_PERMISSIONS_GROUP_DELETE	Remove admin permission group
61	ADMIN_PERMISSIONS_GROUP_UPDATE	Update admin permission group
62	ADMIN_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default admin permission group
63	ADMIN_PERMISSIONS_ASSIGN_GROUP	Assign admin permission group by selection
64	REPORT_SPAM_BY_FILE	Report delivered message as spam
65	DOMAIN_DESTINATION_ROUTES_UPDATE	Update destination routes
66	DOMAIN_LOCAL_RECIPIENTS_ADD	Add local recipient
67	DOMAIN_LOCAL_RECIPIENTS_DELETE	Remove local recipient
68	DOMAIN_LOCAL_RECIPIENTS_STATE_CHANGE	Local recipients state change
69	DOMAIN_ALIASES_ADD	Add domain alias
70	DOMAIN_ALIASES_DELETE	Remove domain alias
71	DOMAIN_SETTINGS_UPDATE	Update domain settings
72	DOMAIN_SETTINGS_RESET_TO_DEFAULT	Reset domain settings to default
73	DOMAIN_RELAY_RESTRICTIONS_ADD	Add relay restriction
74	DOMAIN_RELAY_RESTRICTIONS_UPDATE	Update relay restriction

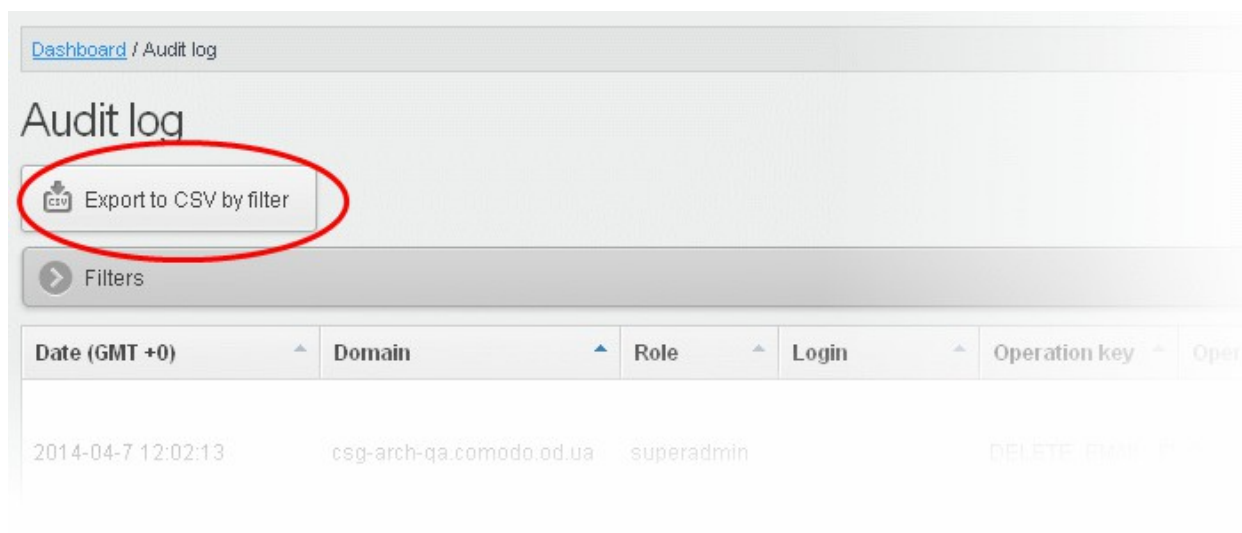
75	DOMAIN_RELAY_RESTRICTIONS_DELETE	Remove relay restriction
76	DOMAIN_RELAY_RESTRICTIONS_STATE_CHANGE	Relay restriction state change
77	DOMAIN_OUTGOING_USER_ADD	Add outgoing user
78	DOMAIN_OUTGOING_USER_SETTINGS_UPDATE	Edit outgoing user
79	DOMAIN_OUTGOING_USER_DELETE	Remove outgoing user
80	DOMAIN_OUTGOING_USER_LOCK	Lock outgoing user
81	DOMAIN_OUTGOING_USER_UNLOCK	Unlock outgoing user
82	DOMAIN_OUTGOING_USER_PASSWORD_UPDATE	Update password for outgoing user
83	DOMAIN_EMAIL_SIZE_RESTRICTION_CHANGE	Email size restriction change
84	DOMAIN_BLOCKED_EXTENSIONS_UPDATE	Update blocked extensions
85	DOMAIN_BLOCKED_EXTENSIONS_RESET_TO_DEFAULT	Reset blocked extensions to default
86	DOMAIN_AUDIT_CONFIGURATION_CHANGE	Audit configuration change
87	DOMAIN_LDAP_CONFIGURATION_CHANGE	LDAP configuration change
88	DOMAIN_INCOMING_USER_ADD	Add incoming user
89	DOMAIN_INCOMING_USER_EDIT	Edit incoming user
90	DOMAIN_INCOMING_USER_DELETE	Remove incoming user
91	DOMAIN_INCOMING_USER_UNLOCK	Unlock incoming user
92	DOMAIN_INCOMING_USER_REGENERATE_PASSWORD	Regenerate password for incoming user
93	DOMAIN_INCOMING_USER_PASSWORD_UPDATE	Update password for incoming user
94	DOMAIN_INCOMING_USER_ALIASES_UPDATE	Update incoming user aliases
95	DOMAIN_INCOMING_USER_MOVE_USER_TO_ALIAS	Move user to alias
96	DOMAIN_INCOMING_USER_MOVE_ALIAS_TO_USER	Move alias to incoming user
97	USER_PERMISSIONS_GROUP_ADD	Add user permission group
98	USER_PERMISSIONS_GROUP_DELETE	Remove user permission group
99	USER_PERMISSIONS_GROUP_UPDATE	Update user permission group
100	USER_PERMISSIONS_CHANGE_DEFAULT_GROUP	Change default user permission group
101	USER_PERMISSIONS_ASSIGN_GROUP	Assign user permission group by selection

Export Log Report to CSV

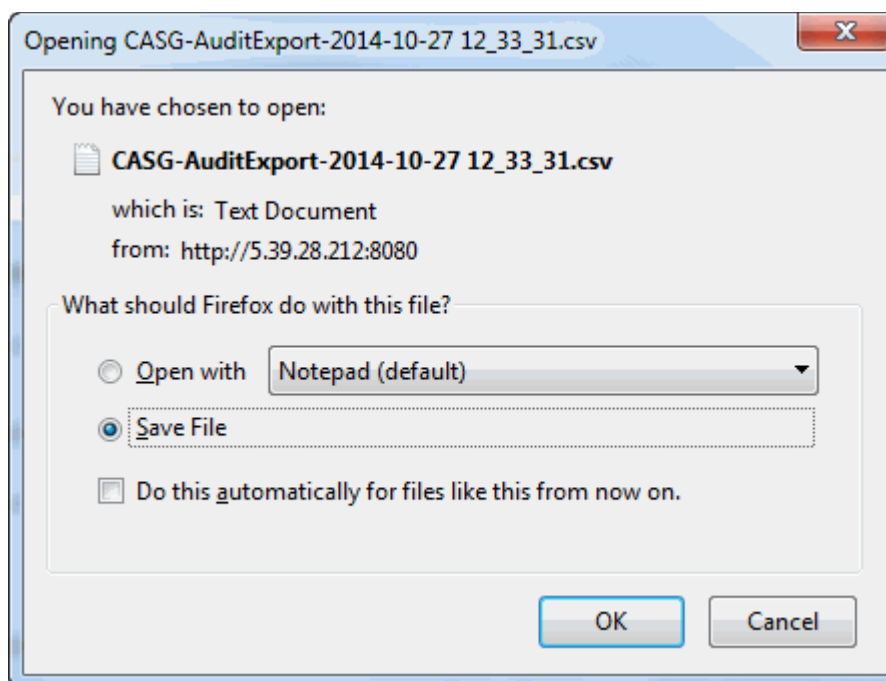
The log report can be exported to a comma separated value (CSV) file and is limited to 10,000 entries per file. If the entries exceed this value, exporting cannot be done and a warning will be displayed. Please note that exported file will display the entries in the same sorted order as in the interface.

To export log report to csv file

- Click the 'Export to CSV by filter' button.



The 'File Download' dialog will be displayed.

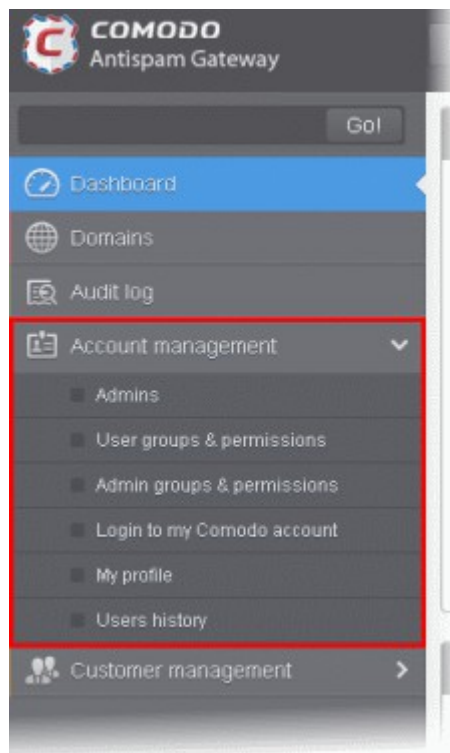


- Click 'Open' to view the file with an appropriate application or click 'OK' to save the file to your computer.

The values in the log report will be separated by commas and this file can be opened with appropriate application such as Excel or Openoffice Calc for easy analysis.

3.2.3 Administrator Account Management

The Account Management area of CASG allows an administrator with appropriate privileges to add new administrators for the same account. This area also allows the administrator to configure permissions for users and administrators, reset passwords and change the login status from enabled to disabled and vice-versa. If you have logged in using the CAM credentials, this area will have an additional icon 'Login to my Comodo account' through which you can access your CAM account. If logged in as an administrator, the 'Account Management' area will differ depending on the privileges configured for the administrator. Refer to the section '[Admin Groups & Permissions](#)' for more details.



Click the following links for more details:

- [Managing Administrators](#)
- [User Groups & Permissions](#)
- [Admin Groups & Permissions](#)
- [Managing Comodo Account](#)
- [My Profile](#)
- [Users History](#)

3.2.3.1 Administrators

In this interface, an administrator with appropriate privileges can add new administrators, delete existing administrators, set permission levels as well as edit the login status and regenerate new password for existing administrators. Refer to the section '[Admin Groups & Permissions](#)' for more details on administrative privileges.

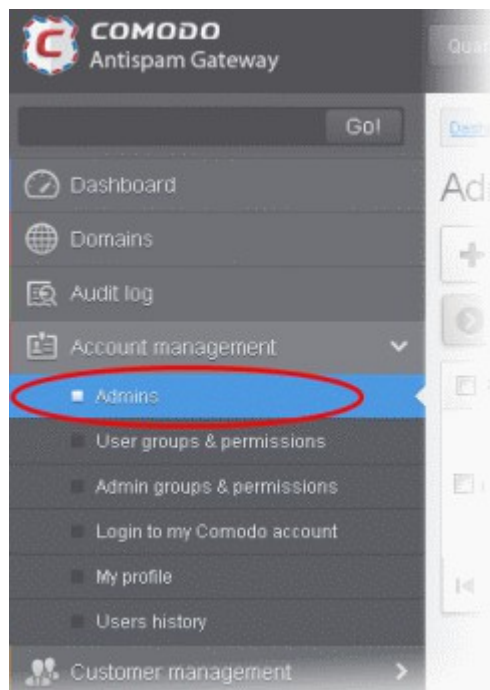
Click the following links for more details:

- [Managing Administrators](#)
- [Adding New Administrators](#)
- [Deleting Administrators](#)

- **Editing Administrators**
- **Managing Permissions for Administrators**

Managing Administrators

- Click the 'Account management' tab on the left hand side navigation to expand and then click the 'Admins' sub tab.



The 'Admins' configuration interface will be displayed:

Dashboard / Admins

Admins

Filters

<input type="checkbox"/> Login	<input type="checkbox"/> Enabled	<input type="checkbox"/> Last login	<input type="checkbox"/> Group	<input type="checkbox"/> Target
<input type="checkbox"/> john@docteamcasg.comodo.od.ua	true	Apr 16, 2014 4:13:58 AM	Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csg-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]

/ 1
 Per page 15

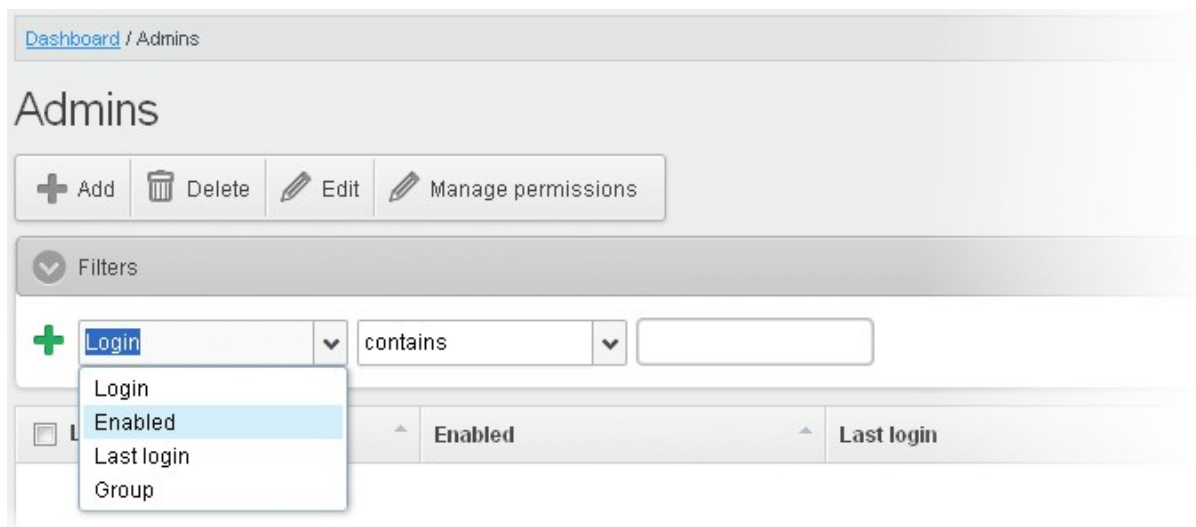
The 'Admins' interface displays a list of administrators with their CASG enabled/disabled status, their last login date and time, to which group they belong and the domains that they can manage. You can sort the entries in ascending or descending order based on the login, enabled status or last login time by clicking the up/down arrows in the respective column headers.

Using the filter option to search administrators

Click anywhere on the Filters tab to open the filters area.



You can add more filters by clicking **+** for narrowing down your search.



You can remove a filter by clicking the **-** icon beside it.

Following are the options in the first drop-down in the filters area:

- **Login:** Will execute a search of admins according to the text in the text box (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available in the second drop-down:

- **Equals:** Displays the results based on the administrator name that was entered in full in the text box.
- **Not Equals:** Displays all administrator(s), except the one entered in the text box.
- **Contains:** Displays all administrator(s) that contains the words entered in the text box.
- **Not Contains:** Displays all administrator(s) that does not contain the words entered in the text box.
- **Starts With:** Displays all administrator(s) that starts with the words entered in the text box.
- **Ends With:** Displays all administrator(s) that ends with the words entered in the text box.

Other options available in the first drop-down in the filters area:

- **Enabled:** Sorts the results based on administrators' enabled / disabled status.

When you select this option in the first drop-down, 'equals' is the only option available in the second drop-down:

- **Equals:** Displays the results of enabled administrator(s) when the checkbox beside it is selected. When the checkbox is not selected, it displays the list of administrator(s) who are not enabled.
- **Last Login:** Will execute a search of admins according to the date selected in the calendar (column 3) and the condition selected in column 2.

When you select this option in the first drop-down, the following filters are available:

- **Equals:** Displays the list of administrator(s) that has the last logged in on the same date as the selected date in the third box from the calendar.
- **Less than:** Displays the list of administrator(s) that has the last logged in on dates less than the selected date in the third box from the calendar.
- **Greater than:** Displays the list of administrator(s) that has the last logged in on dates greater than the selected date in the third box from the calendar.
- **Group:** Will execute a search of admins according to the group selected in last drop-down (column 3) and the condition selected in column 2.
 - **Equals:** Displays the results based on the group name that is selected in the drop down list from the third box.
 - **Not Equals:** Displays all administrator(s), except the one selected in the drop down list from the third box.
- Click 'Apply Filter' after selecting the filters.

The application will search the respective column(s) according to the filter(s) set and display the result.

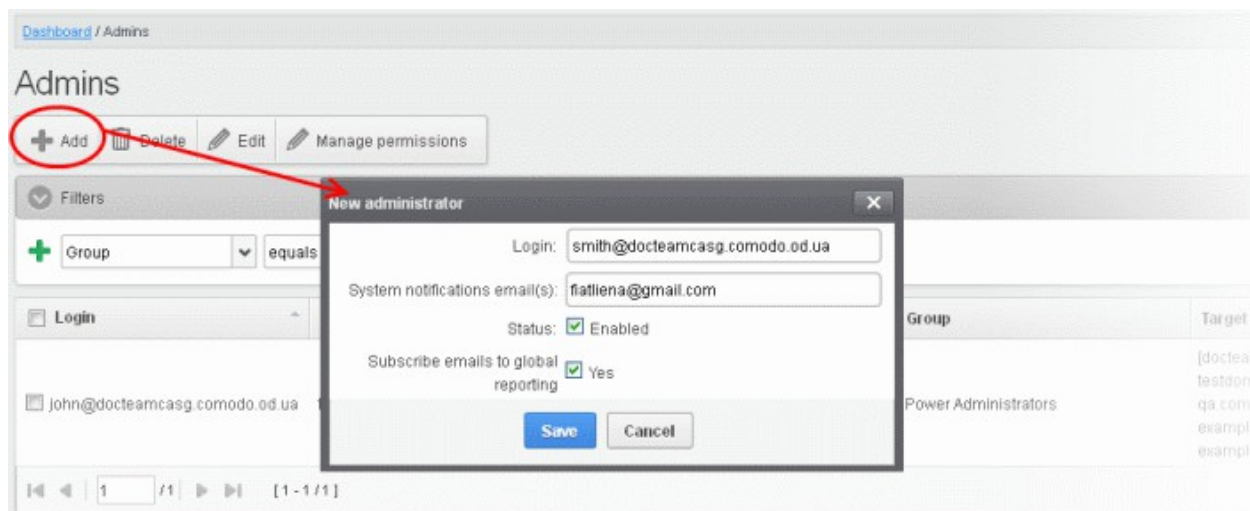
- Click anywhere on the Filters tab to close the filters area.

- Click the  button to display all administrators.

Note: To display all the administrators after using the filters option, you have to first click anywhere on the Filters tab to close the filters area and then click the 'Refresh' button.

To add a new administrator

- Click the Add button.

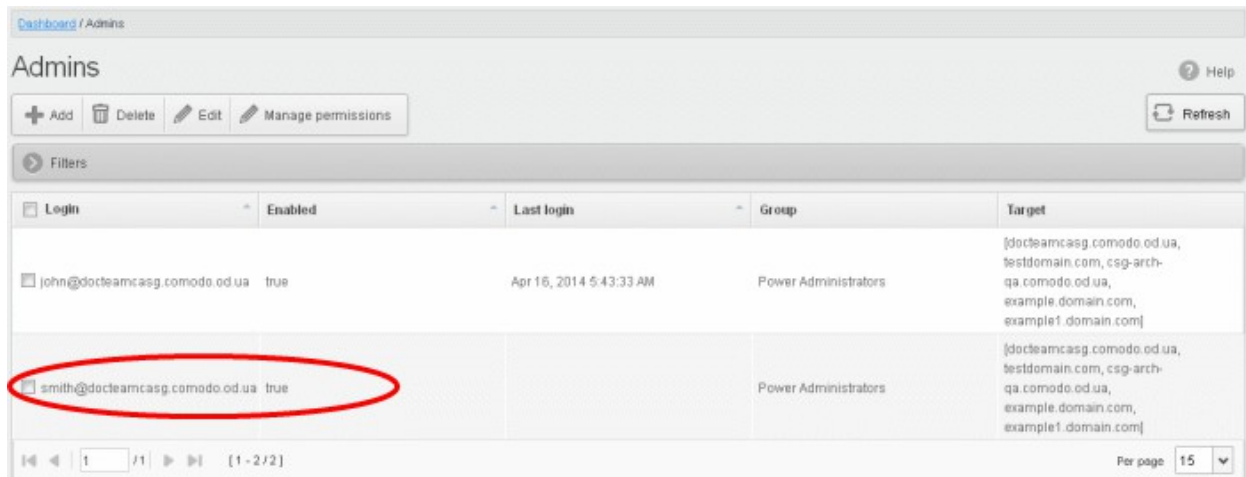


The 'New administrator' dialog will be displayed.

- **Login** - Enter the new administrator's valid email address as login username.
- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CASG notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. Refer to the section **Email Management** for more details.
- **Status** - Enables to change the login status of the new administrator. By default, this box is selected, that is, the new administrator can access CASG interface.

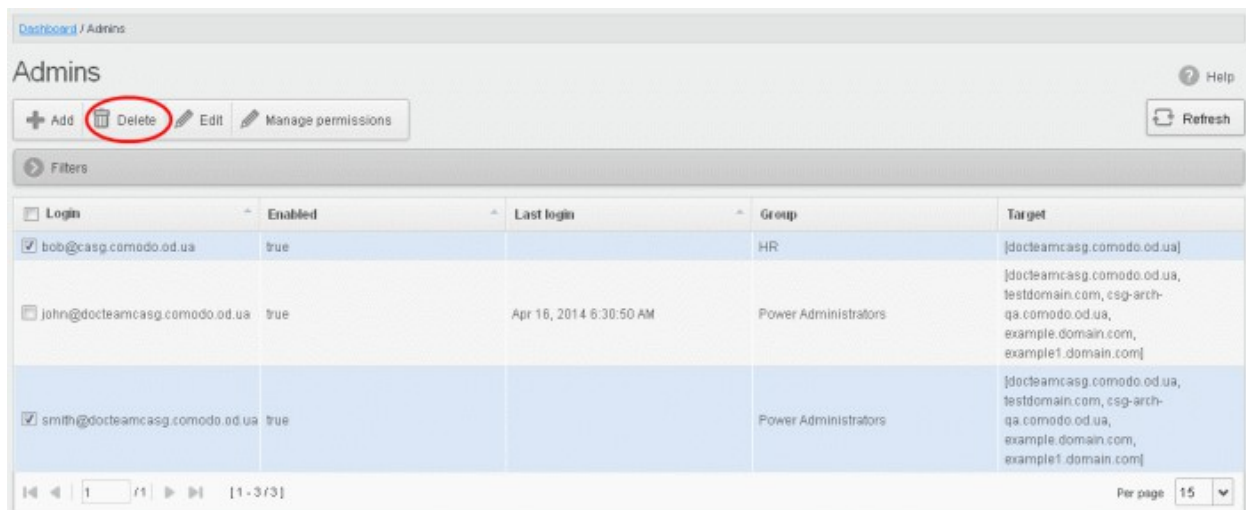
- **Subscribe emails to global reporting** - Selecting this checkbox enables the new administrator to receive the periodical domain and quarantine summary reports of all domains belonging to the account at the email address specified as login user name. Refer to **CASG Reports - an Overview** for more details.
- Click the 'Save' button.

The administrator will be added to the list and be placed in the default group. The privileges to the administrator can be configured according to his/her role. Refer to the section '**Managing Permissions for Administrators**' for more details. An email to the added administrator will be sent automatically containing password to access CASG. The password can be reset in the **edit interface**. The added administrator will be displayed in the list.

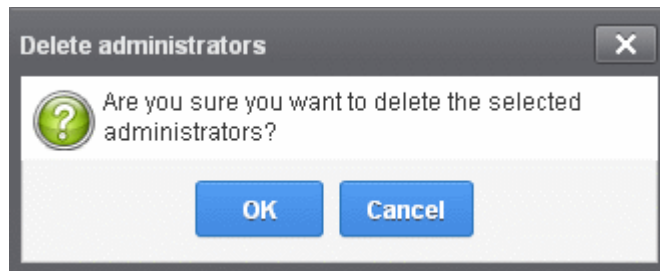


To delete an administrator

- Select the administrator to be removed and click the 'Delete' button.



A confirm dialog will be displayed warning you that the selected administrators will be deleted.



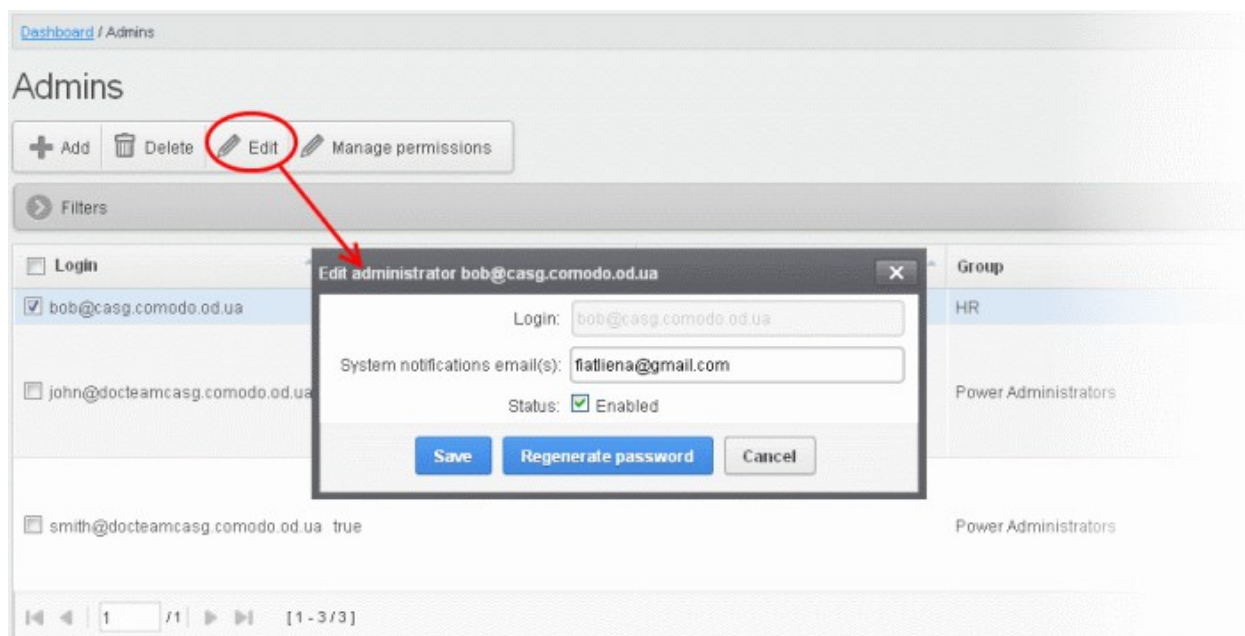
- Click 'OK' to confirm the deletion.

The selected administrator(s) will be deleted from the list.

To edit an existing administrator

You can reset the password, change the CASG notification email address(es) and allow or deny permission for the administrators to access their CASG account in the edit interface.

- Select the administrator you want to edit from the list and click the 'Edit' button.



The 'Edit administrator' dialog box will be displayed.

- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CASG notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. Refer to the section **Email Management** for more details.

Tip: The currently logged-in administrator can configure the Quarantine notification email address through **Dashboard > Account Management > My Profile > Change Settings** dialog.

- **Status** - Enables to change the login status of the administrator.
- **Regenerate password** - Click this button to reset the password for the administrator in case it is forgotten. The new password will be sent to the administrator's email automatically. The administrator has to use this new password to access CASG.

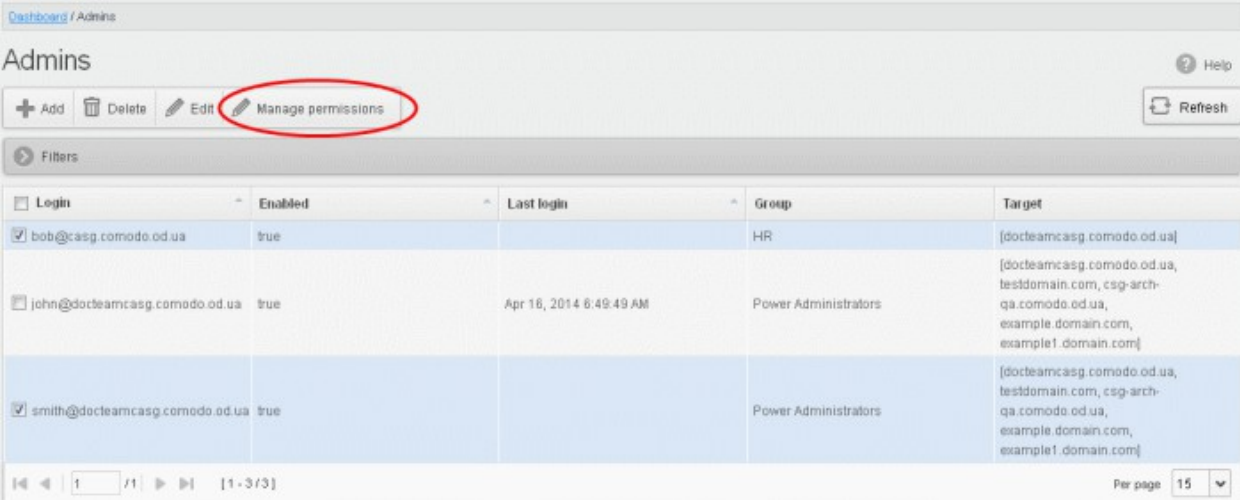
- Click the 'Save' button to confirm your changes.

Managing Permissions for Administrators

CASG allow administrators with appropriate privileges to assign permissions for other administrators that will determine what he/she can do and cannot do while logged into their respective CASG admin interface. The administrators can create policies and assign them to other administrators from this interface. See the section '[Admin Groups & Permissions](#)' for more details on how to create groups and policies for administrators. A new administrator will be automatically assigned default permission settings.

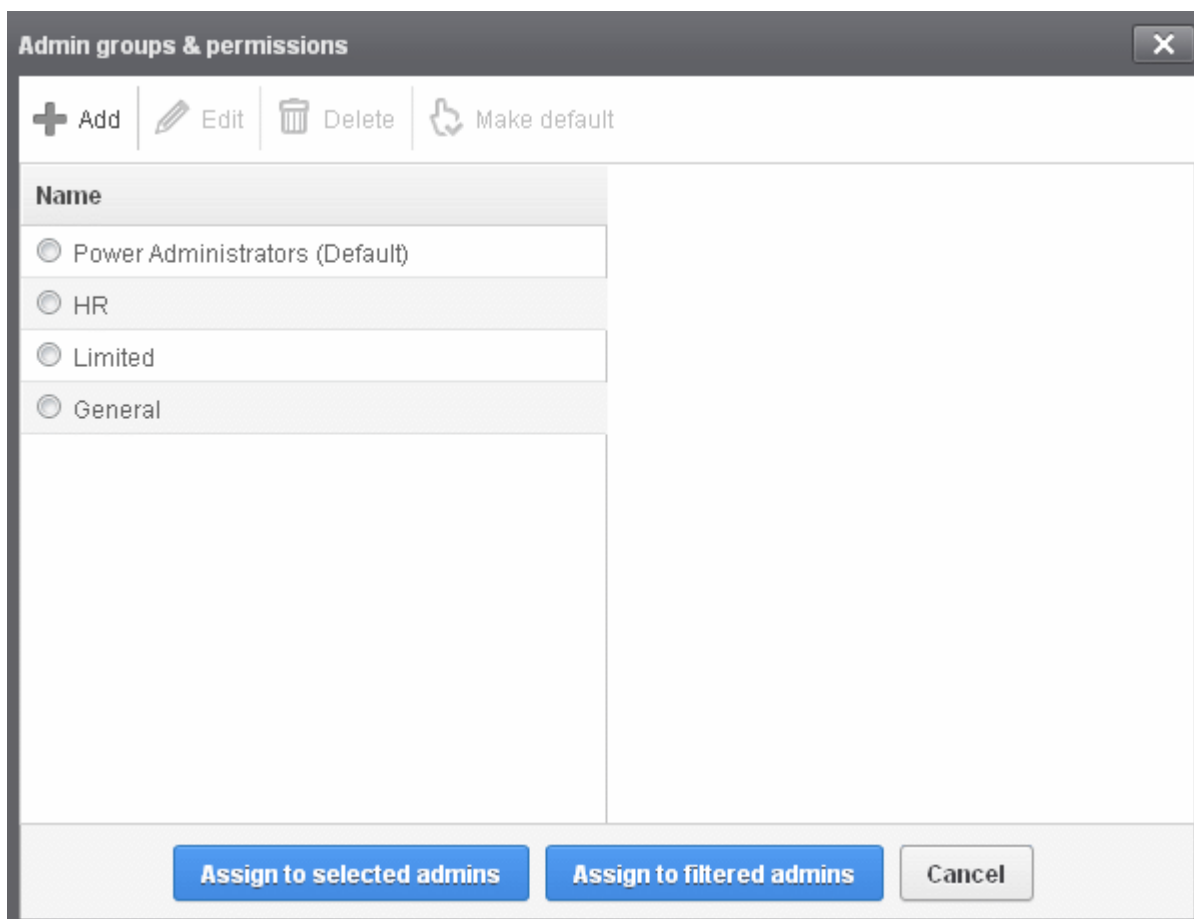
To assign permissions for an administrator

- Select the administrator or multiple administrators that you want assign permissions and click the 'Manage permissions' button.



<input type="checkbox"/>	Login	Enabled	Last login	Group	Target
<input checked="" type="checkbox"/>	bob@casg.comodo.od.ua	true		HR	[docteamcasg.comodo.od.ua]
<input type="checkbox"/>	john@docteamcasg.comodo.od.ua	true	Apr 16, 2014 6:49:49 AM	Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csq-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]
<input checked="" type="checkbox"/>	smith@docteamcasg.comodo.od.ua	true		Power Administrators	[docteamcasg.comodo.od.ua, testdomain.com, csq-arch-qa.comodo.od.ua, example.domain.com, example1.domain.com]

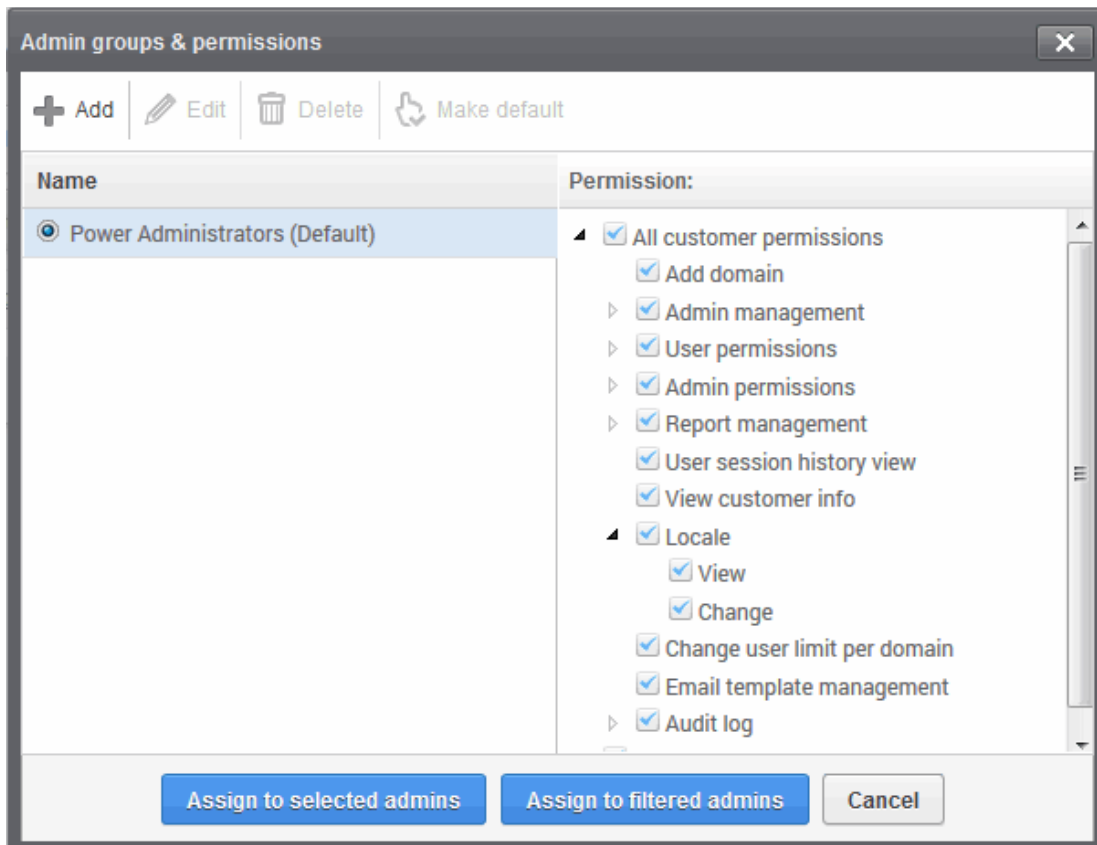
The 'Admin Groups & Permissions' interface will be displayed.



The interface displays the list of groups available with same or different permission levels for each group. By default, 'Power Administrators (Default) group will be available and administrators can add, edit groups and assign permissions to other administrators. See the section '[Admin Groups & Permissions](#)' for more details.

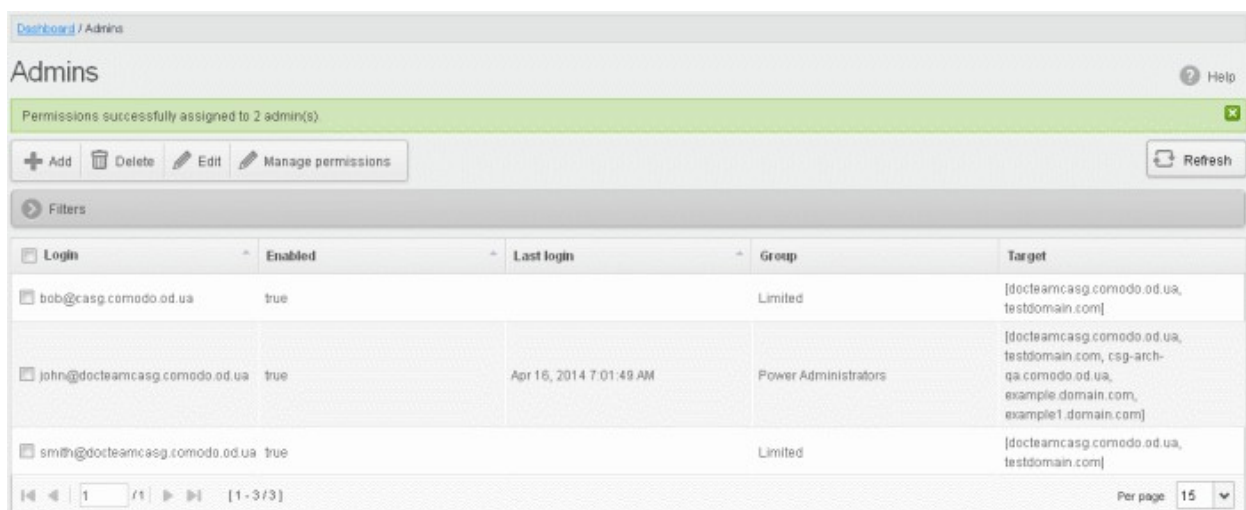
- Select the group from the list.

The permissions set for this group will be displayed on the right side.



- Click the 'Assign to selected admins' button to set permissions for selected admin(s).
- Click 'Assign to filtered admins' button to set permissions for administrators found by filter.
- Click 'OK' in the confirmation dialog.

The selected admin(s) will be added to the group and a confirmation message will be displayed.



The interface also displays the new group assigned for the selected admin(s) under the 'Group' column.

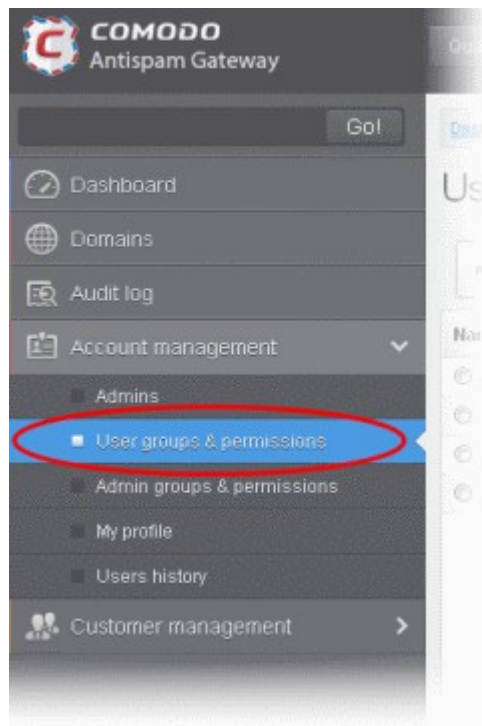
3.2.3.2 User Groups & Permissions

The User Groups & Permissions interface allows the administrators with appropriate privileges to create email user groups according to the needs of the organization. Each group can be configured with different permission levels. This simplifies the process of configuring permission levels for each user meaning new or existing users belonging to

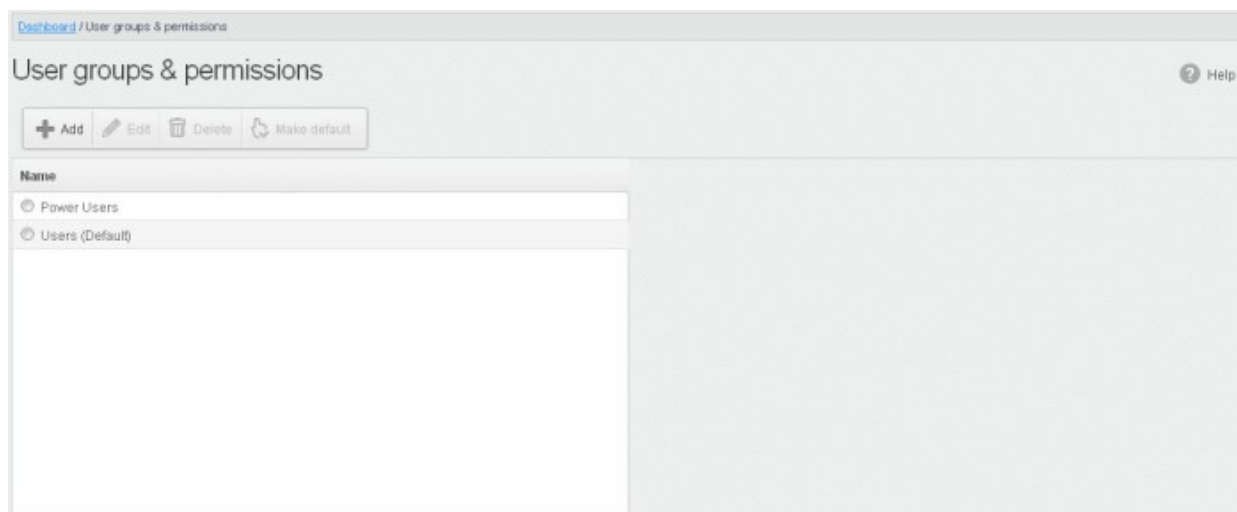
all domains for the account can be simply assigned a group with a preset policy. The user interface will vary according to his/her permission level. See the section '**Managing Permissions for Users**' in '**User Account Management**' on how to add users to predefined groups.

To create user groups

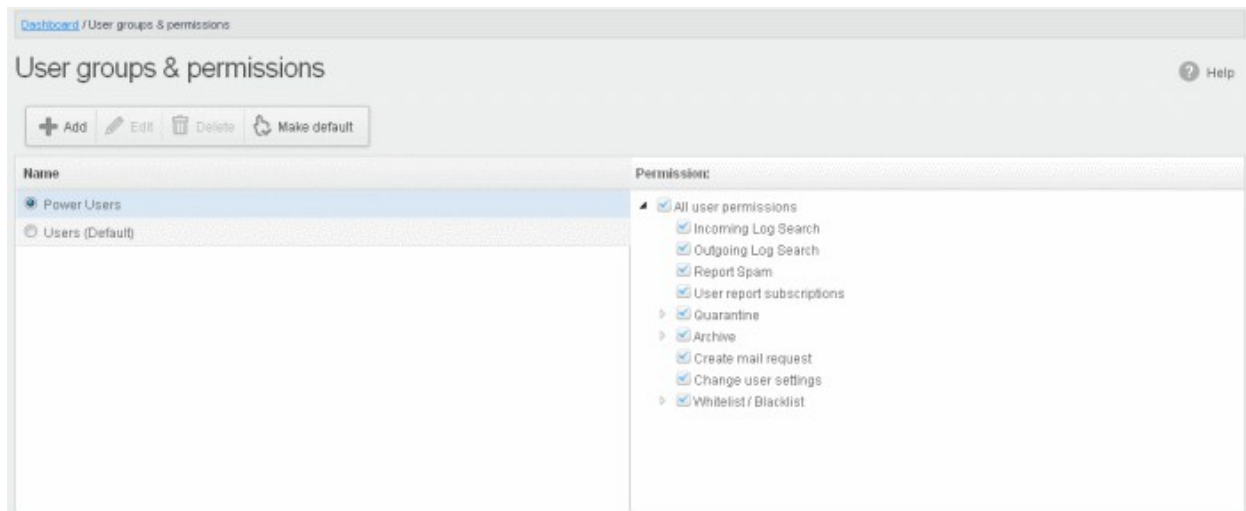
- Click the 'Account management' tab on the left hand side navigation to expand and then click the 'User groups & permissions' sub tab.



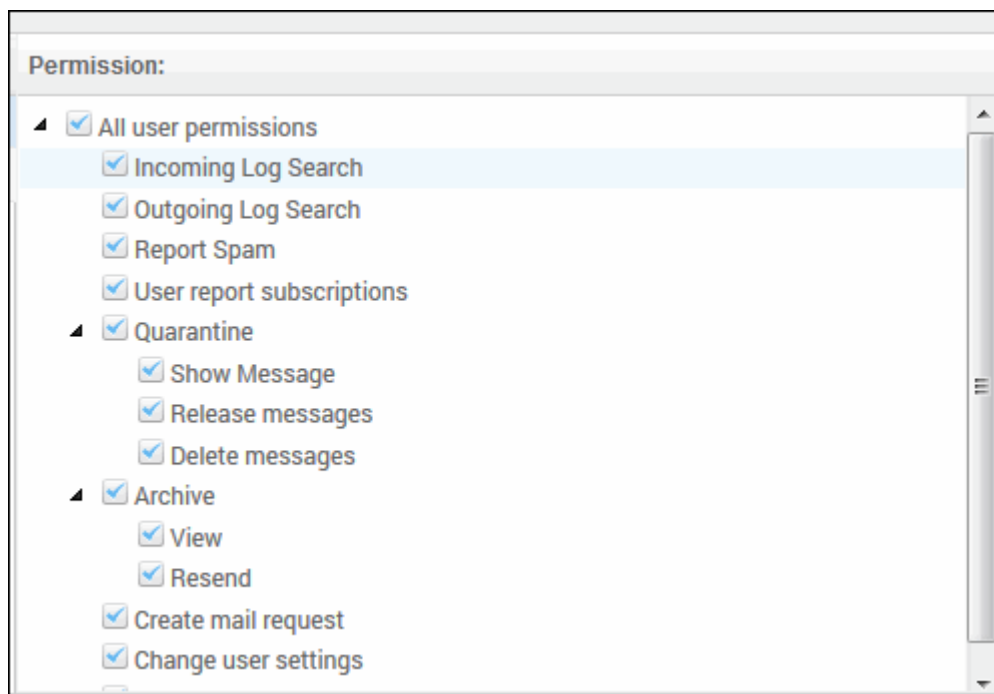
The 'User Groups & permissions' interface will be displayed.



By default, two user groups, Power User and Users (Default), will be available. These two groups cannot be either edited nor deleted. Clicking any one of them will display the permission levels assigned for the group in the right side.



Clicking on the arrow beside a permission will display the tree structure of second level of permissions, if available.



For users in the 'Power User' group, all permission levels will be enabled. The 'Release quarantine messages' option will not be available to users in the regular 'Users' group. This means that if a user is assigned to the 'Power User' group, he / she can release quarantined messages from the quarantined mails list without approval from the administrator. See the section **Released Requests** in **Email Management** for more details.

Permission Levels

- **Incoming Log Search** - Allows a user to search and view the log of all incoming mails.
- **Outgoing Log Search** - Allows a user to search and view the log of all outgoing mails.
- **Report Spam** - Allows a user to report a mail as spam mail.
- **User report subscriptions** - Allows a user to configure periodical quarantine report generation.
- **Quarantine**
 - **Show Message** - Allows a user to view quarantined emails in same window or separate window.
 - **Release messages** - Allows a user to release a quarantined mail without approval from the administrator.

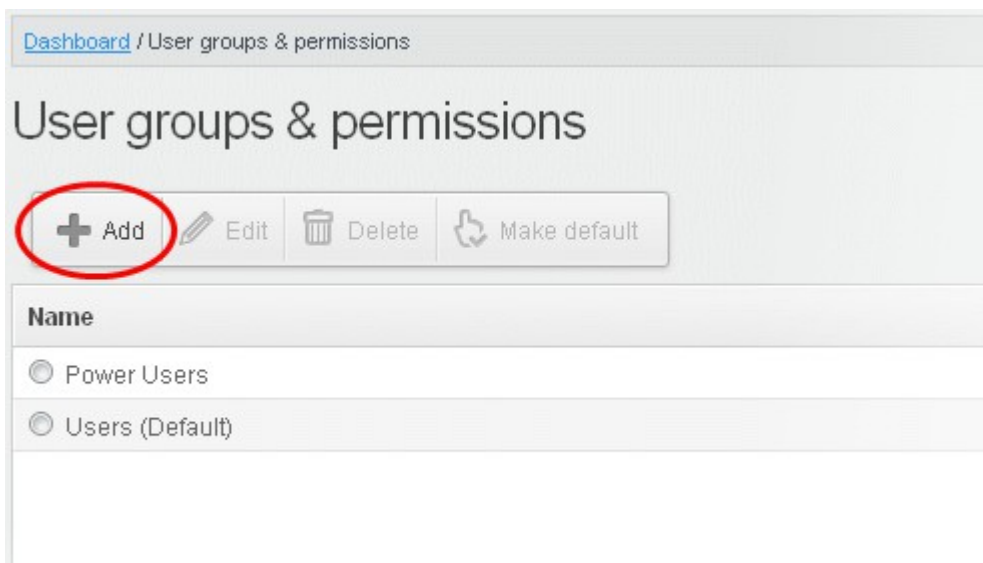
- **Delete messages** - Allows a user to delete a quarantined mail without approval from the administrator.
- **Archive**
 - **View** - Allows a user to view archived emails in same window or separate window.
 - **Resend** - Allows a user to resend archived emails to himself / herself.
- **Create mail request** - Allows a user to configure email request for CASG notifications.
- **Change user settings** - Allows a user to configure himself / herself as recipient whitelist.
- **Whitelist / Blacklist**
 - **Manage whitelist senders per user** - Allows a user to manage sender whitelist for his / her mail account
 - **Manage blacklist sender per user** - Allows a user to manage sender blacklist for his / her mail account

Click the following links for more details.

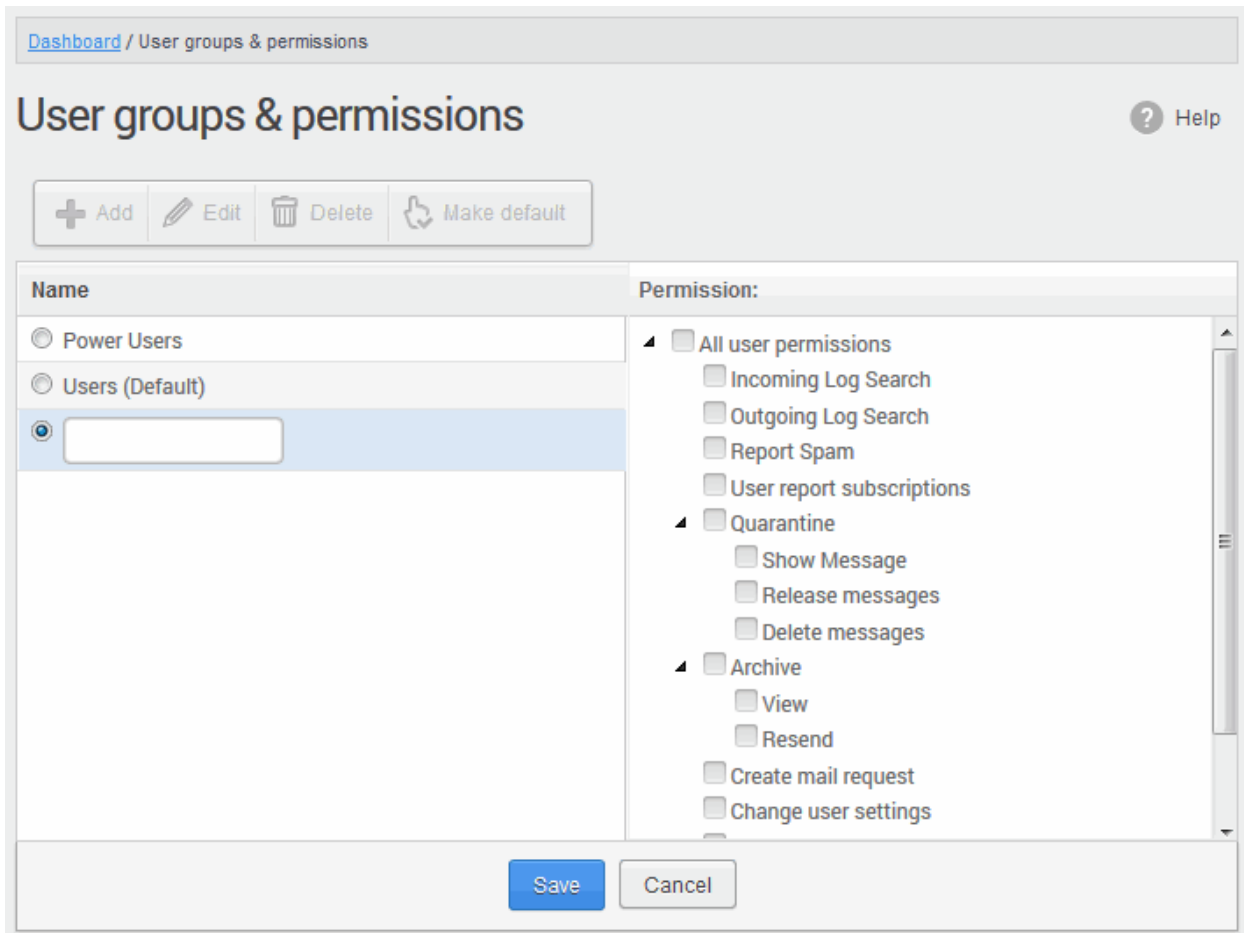
- [Adding a new group](#)
- [Editing a group](#)
- [Deleting a group](#)
- [Making a group as default](#)

Adding a New Group

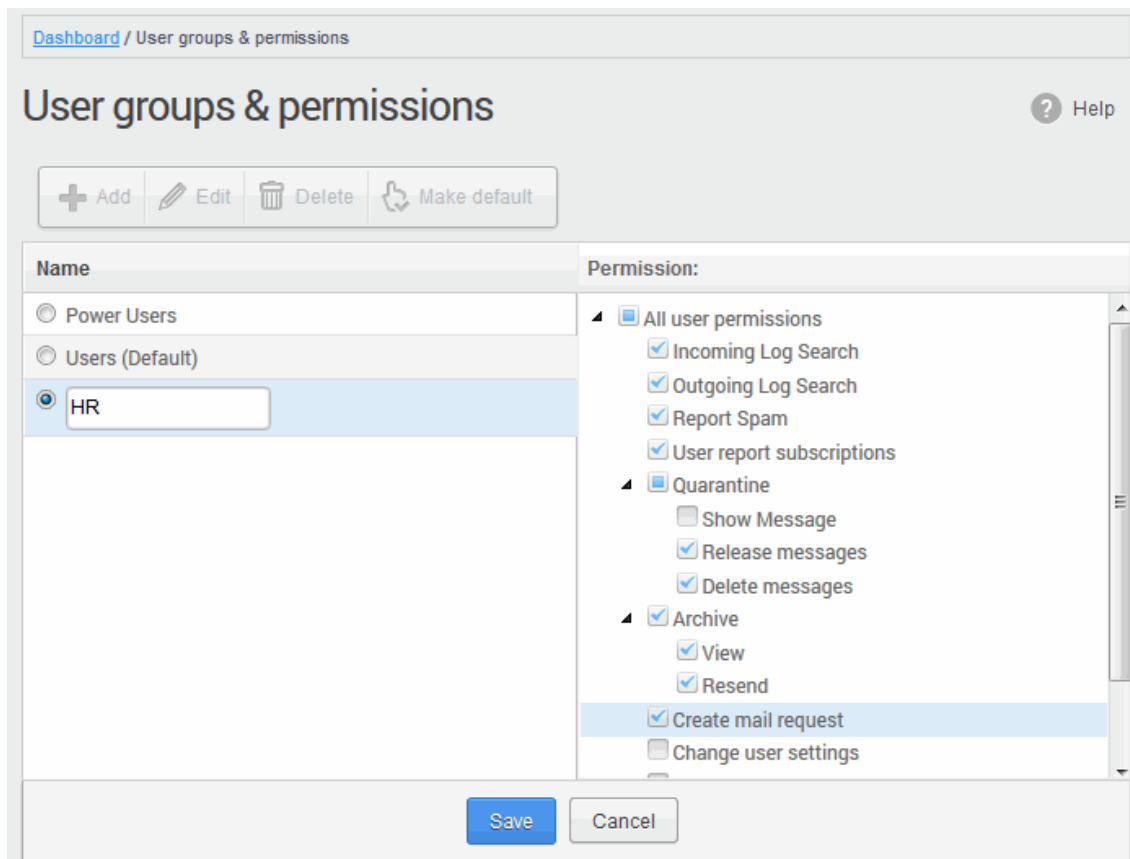
- To add a new group and configure permission levels, click the 'Add' button.



A new group creating page will be displayed.

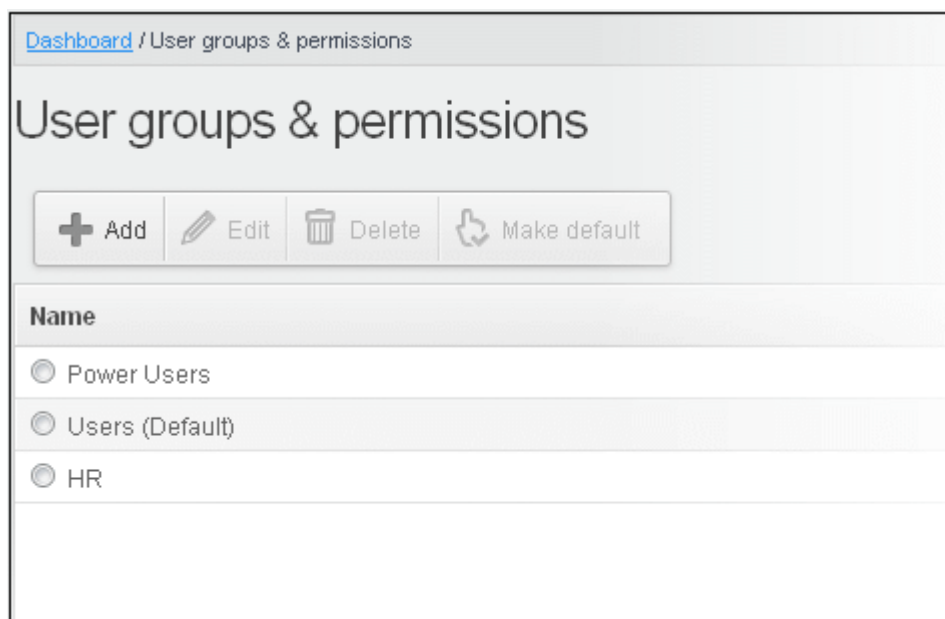


- Enter the name of the group in the text field under the 'Name' column and enable the permission levels in the right side required for that group.



- Click the 'Save' button.

The newly created group will be displayed in the interface.

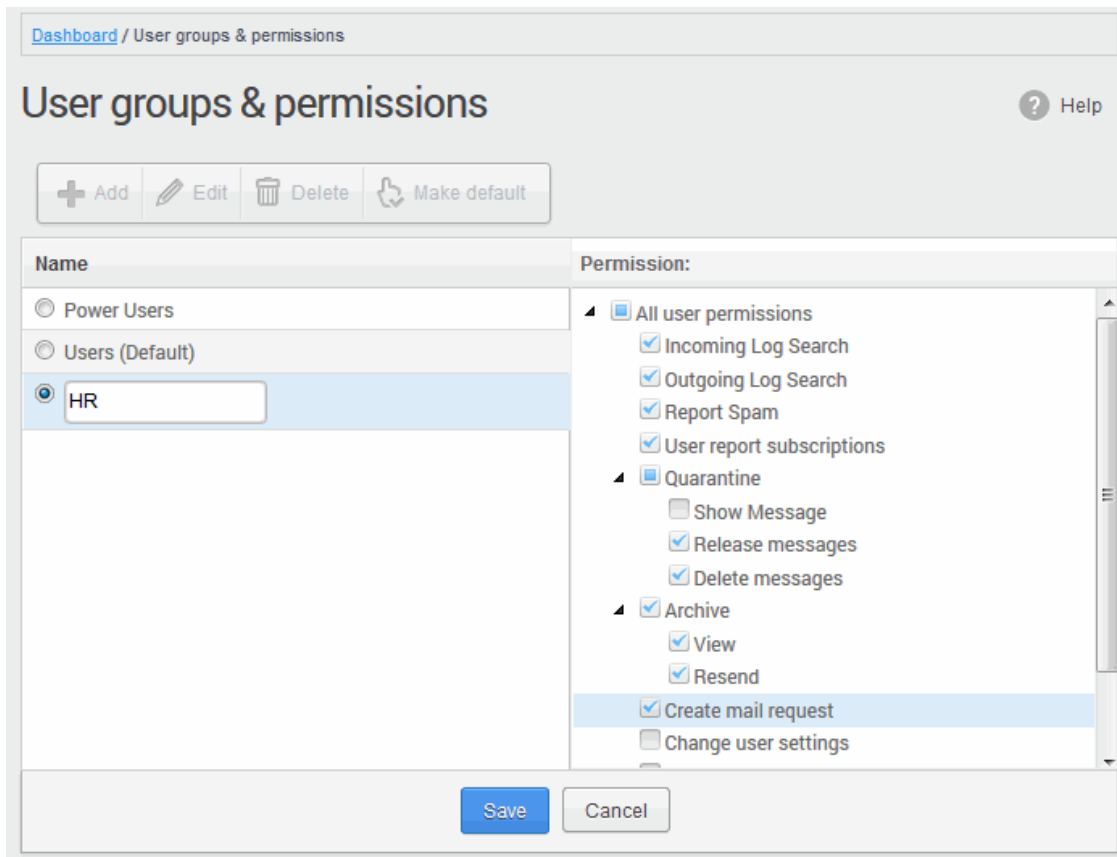


Now, users of domains belonging to the account can be assigned to this newly created group. See the section **'Managing Permissions for Users'** in **'User Account Management'** on how to add users to predefined groups.

Editing a Group

You can edit the name of an existing group and / or change the permission levels.

- To edit an existing group, select the group from the list and click the 'Edit' button.

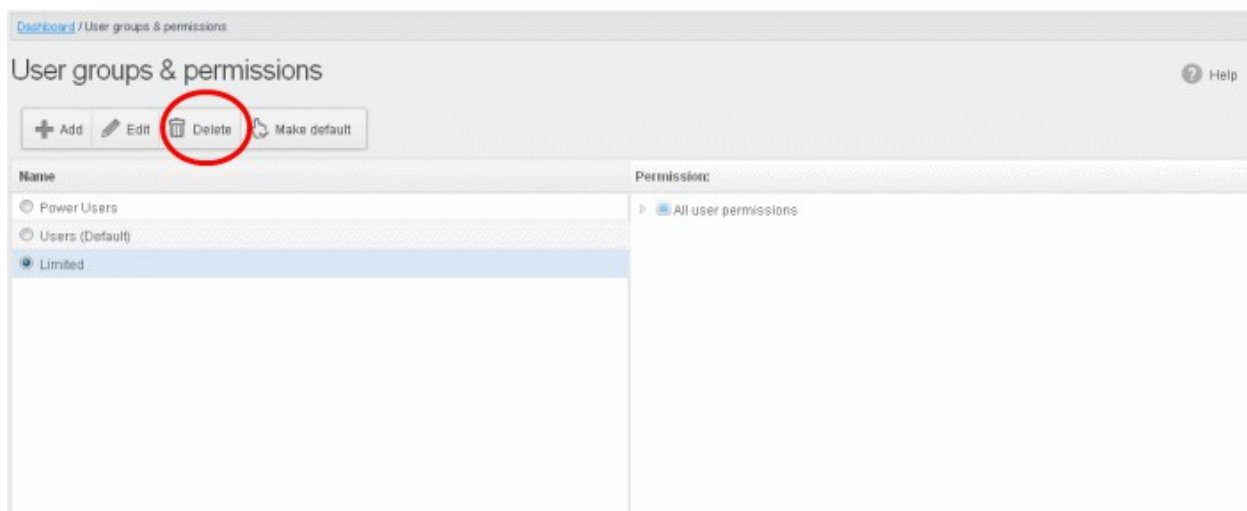


- Change the permission levels and / or the name of the group.
- Click the 'Save' button for the changes to take effect.

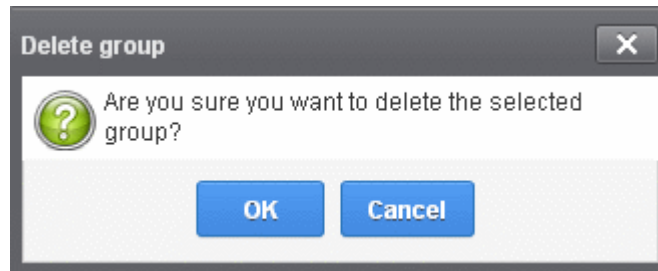
The users in the group that is edited will be automatically reassigned to the edited group.

Deleting a Group

- To delete a group, select it from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.



The selected group will be deleted from the list.

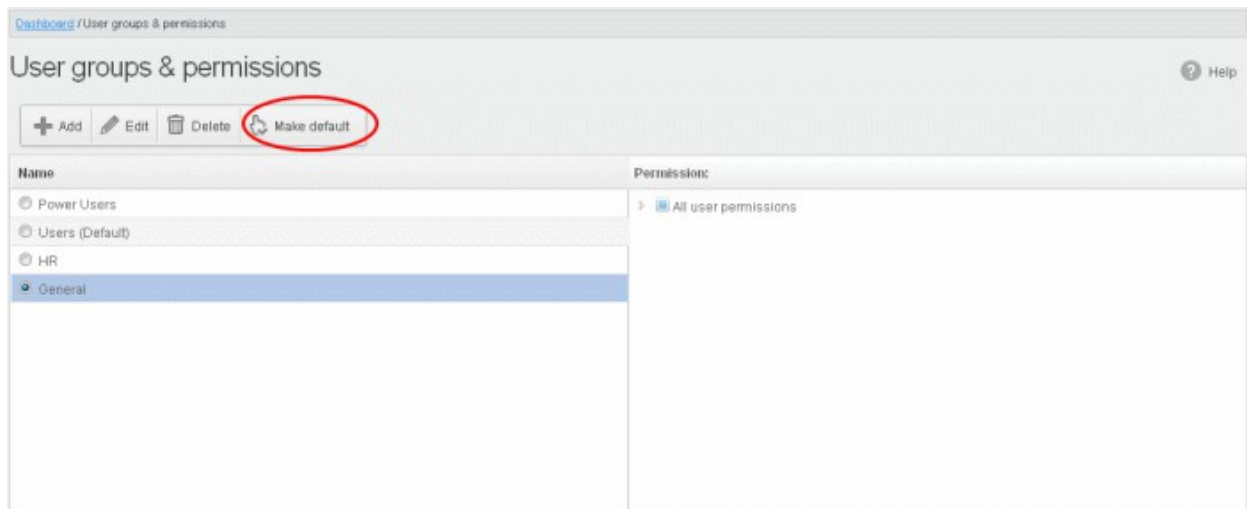
Note 1: If you delete a group, users assigned to that group will be automatically moved to default group. You have to reassign the users if required.

Note 2: If you delete a user group created by the administrator and marked as default, then the 'Users' group that was shipped with the product will be set as default. All the users from the deleted group will be automatically migrated to the 'Users' group.

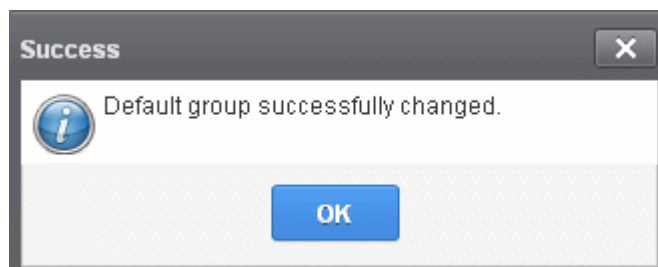
Making a Group as Default

CASG allows administrators to make an existing group as default group. Newly added users and users belonging to an existing group whose name was deleted will be automatically moved to this default group.

- To make an existing group as a default group, select it from the list and click the 'Make default' button.

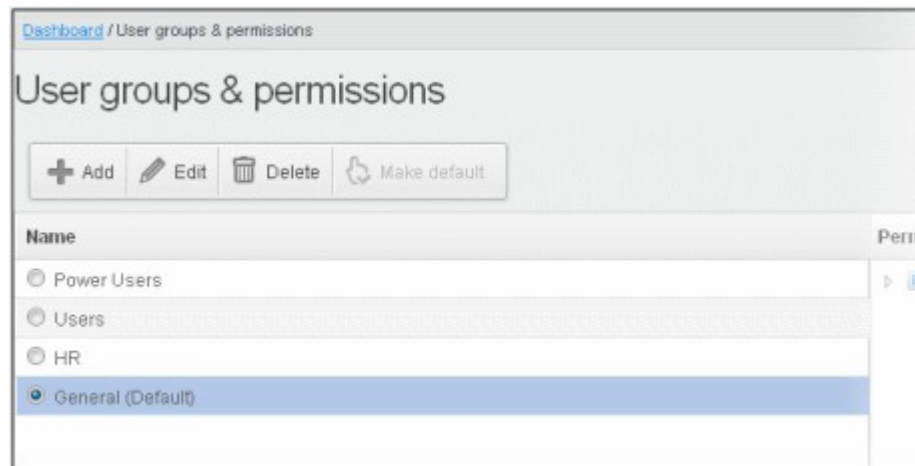


A success dialog will be displayed.



- Click 'OK'.

The selected group will be displayed as default group.



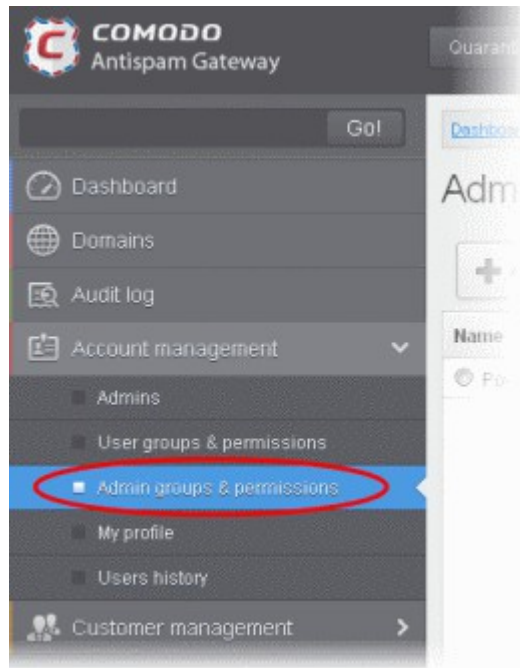
Note: If you delete a user group created by the administrator and marked as default, then the 'Users' group that was shipped with the product will be set as default. All the users from the deleted group will be automatically migrated to the 'Users' group.

3.2.3.3 Admin Groups & Permissions

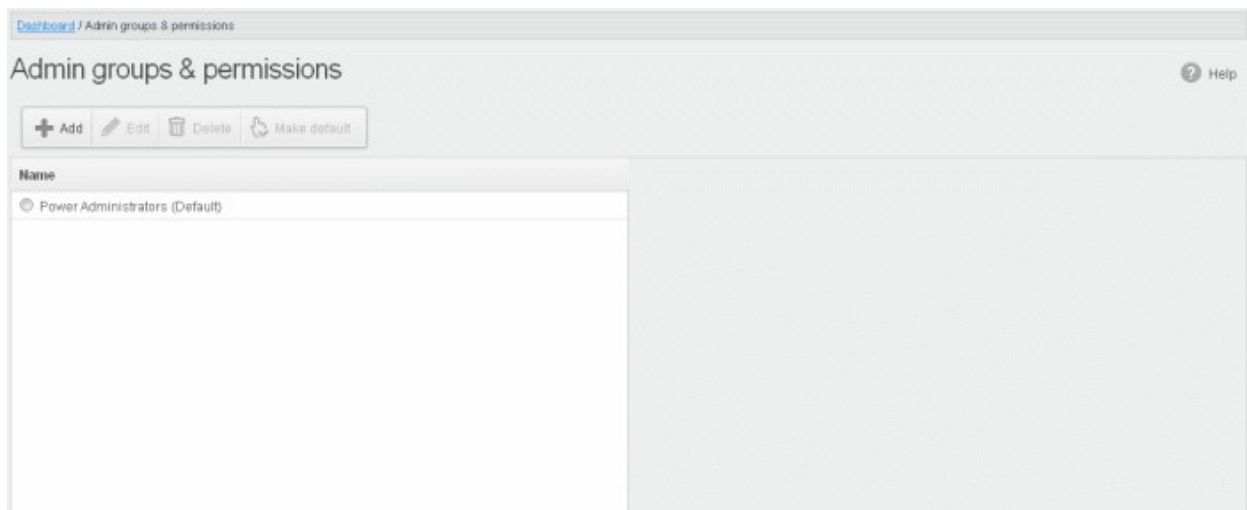
The Admin Groups & Permissions interface allows the administrators with appropriate privileges to create administrator groups according to the needs of the organization. Each group can be configured with different permission levels. This simplifies the process of configuring permission levels for each administrator meaning new or existing administrators belonging to the account can be simply assigned a group with a preset policy. The admin interface will vary according to his/her permission level. See the section '**Managing Permissions for Administrators**' in '**Administrators**' on how to add administrators to predefined groups.

To create admin groups

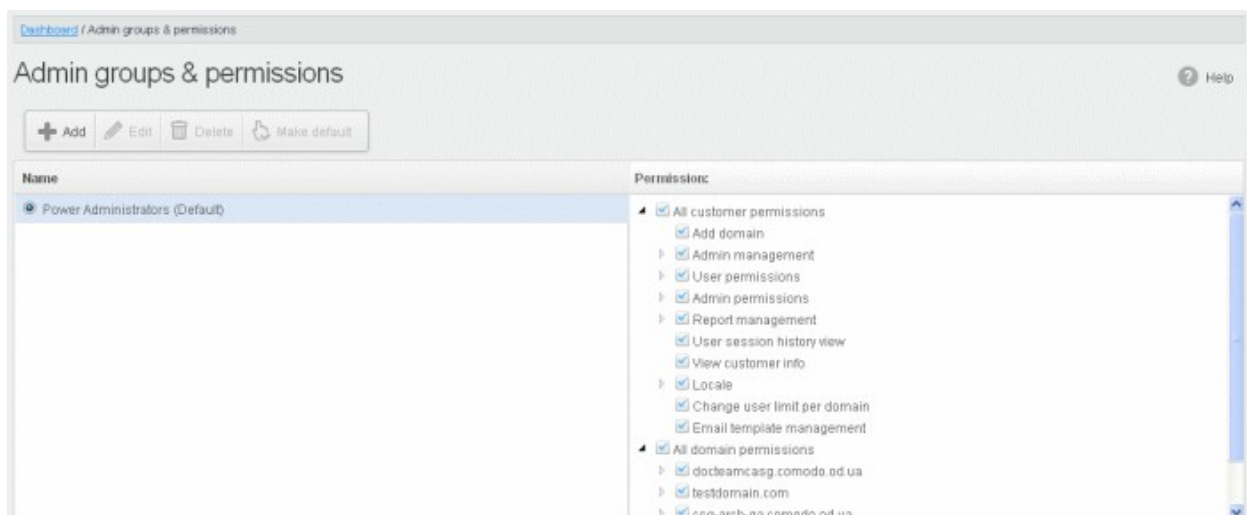
- Click the 'Account management' tab on the left hand side navigation to expand and then click the 'Admin groups & permissions' sub tab.



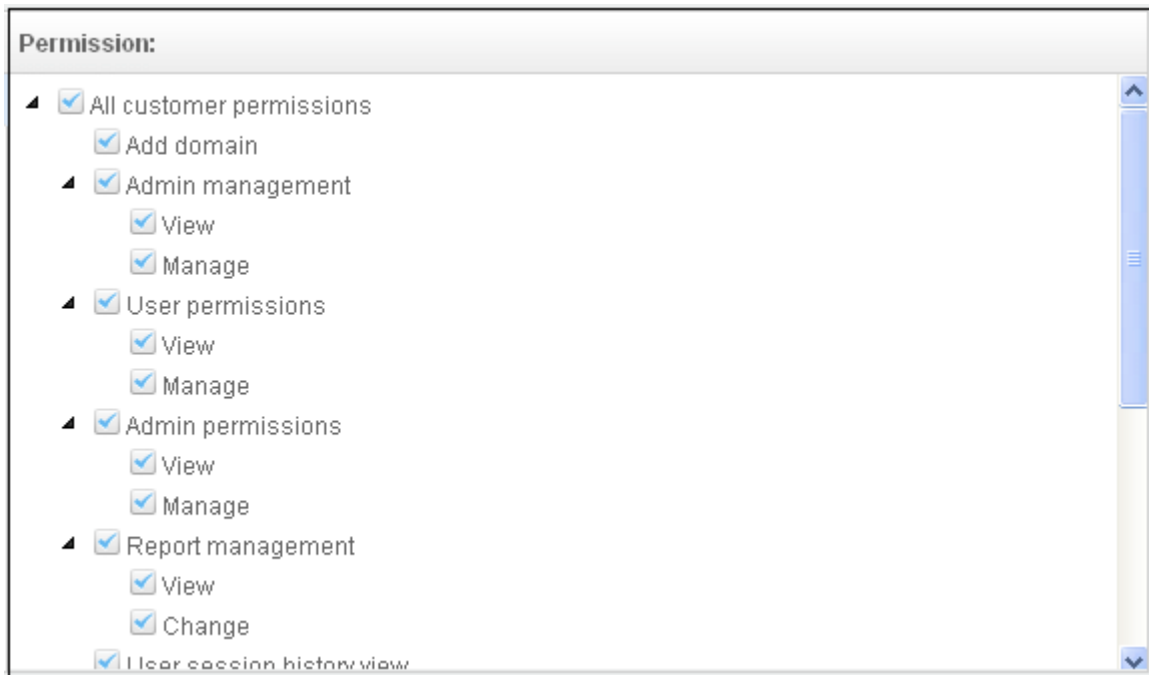
The 'Admin Groups & Permissions' interface will be displayed.



By default, Power Administrator group will be available. This default group cannot be either edited nor deleted. Clicking on it will display the permission levels assigned for the group in the right side.



Clicking on the arrow beside a permission will display the tree structure of second level of permissions, if available.



For administrators in the 'Power Administrators' group, all permission levels will be enabled. The Permission level is divided into two categories, 'All Customer permissions' and 'All domain permissions'. While the former deals with providing privileges for managing customer related tasks such as adding domains, configuring email user permissions, report management and so on, the domain permission level deals with providing access to particular domain(s). This is very useful if you want to restrict administrators to manage selected domains only.

Permission Levels

- **All customer permissions** - View and manage all customer related tasks.
 - Add domain - Add new domain(s)
 - Admin management - View and manage administrators for the account.
 - View - Only view the list of administrators.
 - Manage - Manage administrators for the account.
 - User permissions - View and manage 'User Groups & Permissions'
 - View - Only view 'User Groups & Permissions'.
 - Manage - Manage 'User Groups & Permissions'
 - Admin permissions - View and manage 'Admin Groups & Permissions'
 - View - Only view 'Admin Groups & Permissions'
 - Manage - Manage 'Admin Groups & Permissions'
 - Report management - View and manage report subscriptions
 - View - Only view report subscriptions
 - Change - View and manage report subscriptions
 - User session history view - View user sessions history for all domains in the account.
 - View customer info - View information about the customer.
 - Change user limit per domain - Configure the number of users for each domain in the account.
 - Email template management - Edit the email template for user's notification emails.
 - Audit log - Configure and view log for the permitted domain.
 - Log - View and export the log for the permitted domain.
- **All domain permissions** - Assign domain(s) management.

- Assigned Domain(s) - Manage domains, incoming and outgoing users, emails, audit log and reports.
 - View - Only view the assigned domains.
 - Change - Edit the assigned domain(s)
 - Remove - Remove the assigned domain(s).
- User Management - View and manage incoming users, outgoing users, whitelist recipients and blacklist recipients.
 - Incoming user - View, manage and unlock incoming users.
 - View - Only view list of incoming users.
 - Manage - View and manage incoming users.
 - Unlock - Unlock users immediately without waiting for the timeout period to end.
 - Outgoing user - View, manage, lock/unlock and import from incoming users.
 - View - Only view list of outgoing users.
 - Manage - View and manage outgoing users.
 - Outgoing settings - Configure a list of outgoing users.
 - Lock/Unlock - Lock or unlock outgoing users from sending out mails.
 - Import from incoming - Import outgoing users from the list of incoming users.
 - Whitelist recipients - View and manage whitelist recipients.
 - View - Only view list of whitelisted recipients.
 - Manage - View and manage whitelist recipients.
 - Blacklist recipients - View and manage blacklist recipients.
 - View - Only view list of blacklisted recipients.
 - Manage - View and manage blacklist recipients.
 - Users auto-import - Automatically import all new incoming users bases on incoming email flow
 - View - Only view list of users auto-import recipients.
 - Manage - View and manage users auto-import recipients.
 - Domain geolookup restrictions - View and manage CASG web interface access control policies
 - View - Only view the access control polices
 - Manage - View and manage access control policies
- Domain management - View and manage all domain related tasks.
 - Local recipients - View and manage local recipients.
 - View - Only view list of local recipients.
 - Manage - View and manage local recipients.
 - Domain alias - View and manage domain aliases
 - View - Only view the list of domain aliases.
 - Manage - View and manage domain aliases.
 - Email filter settings - View and configure incoming spam detection settings.
 - View - Only view incoming spam detection settings.
 - Manage - View and configure incoming spam detection settings.
 - Threshold - Configure changes for "Spam threshold" and "Probable spam threshold" fields in the Incoming Spam detection settings
 - Change - View and configure "Spam threshold" and "Probable spam threshold" fields.
 - Domain settings - View and change domain settings.
 - View - Only view the list of domain settings.
 - Change - View and configure domain settings.
 - LDAP - View and configure LDAP settings for importing users.

- View - Only view LDAP settings and list of imported users.
- Change - View and configure LDAP settings for importing users.
- Quarantine - View and manage quarantined mails.
 - View - Only view the list of quarantined mails.
 - Delete - Deleted quarantined mails from the list.
 - Release - Release quarantined mails to the recipients.
- Archive - View and manage copy of incoming mails in archive.
 - View - Only view archived mails.
 - Resend - Resend archived mails to recipients.
 - Retain - Retains archived mails from being purged automatically.
 - Delete - Delete archived mails.
- Incoming delivery queue - View and manage queued mails.
 - View - Only view queued mails.
 - Retry - Retry to send queued mails to recipients.
- Incoming Log Search - Search incoming mails log.
- Outgoing Log Search - Search sent mails log.
- Clear incoming cache - Clear incoming callout cache.
- Clear outgoing cache - Clear outgoing callout cache.
- User session history view - View user sessions history for the assigned domain(s).
- Email Management - View and configure all Email management related settings and tasks.
 - Email size - View and configure email size settings.
 - View - Only view email size settings.
 - Change - View and configure email size settings.
 - Blocked extensions - View and manage blocked extensions.
 - View - Only view the list of blocked extensions.
 - Change - View and manage blocked extensions.
 - Whitelist senders - View and manage sender whitelist.
 - View - Only view sender whitelist.
 - Change - View and manage sender whitelist.
 - Blacklist senders - View and manage sender blacklist.
 - View - Only view sender blacklist.
 - Change - View and manage sender blacklist.
 - Release requests - View and manage requests from users for release of quarantined mails.
 - View - Only view the list of requests from users for release of quarantined mails.
 - Manage - View and manage requests from users for release of quarantined mails.
 - Whitelist requests - View and manage requests from users to whitelist senders.
 - View - Only view the list of requests from users for adding senders to whitelist.
 - Manage - View and manage requests from users to whitelist senders.
 - Blacklist requests - View and manage requests from users to blacklist senders.
 - View - Only view the list of requests from users for adding senders to blacklist.
 - Manage - View and manage requests from users to blacklist senders.
 - Report spam - Upload mails to CASG for reporting them as spam.
 - Whitelist sender rule - View and manage rules for adding senders to whitelist.
 - View - Only view the whitelist sender rules
 - Manage - View and manage whitelist sender rules

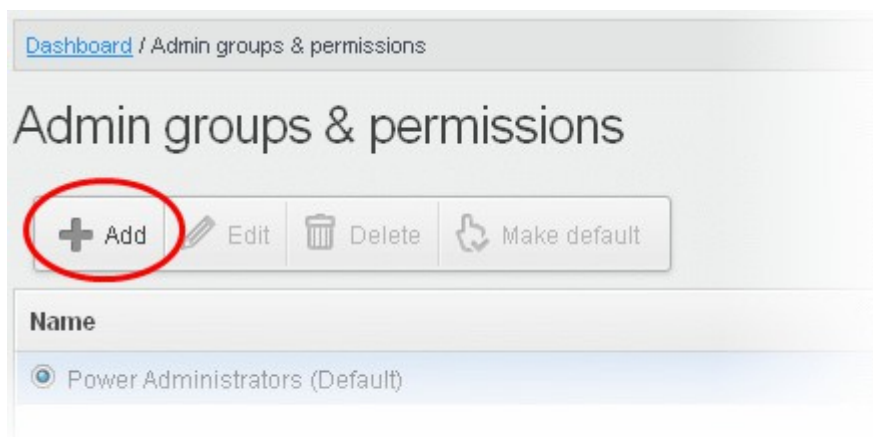
- Blacklist sender rule - View and manage rules for adding senders to blacklist
 - View - Only view the blacklist sender rules
 - Manage - View and manage blacklist sender rules
- Whitelist senders per user - View and manage whitelisted senders per user.
 - View - Only view list of whitelisted senders per user.
 - Manage - View and manage whitelisted senders per user.
- Blacklist senders per user - View and manage blacklisted senders per user.
 - View - Only view list of blacklisted senders per user.
 - Manage - View and manage blacklisted senders per user.
- Domain relay restrictions - View and configure email relay restriction rules
 - View - Only view relay restriction rule
 - Manage - View and manage relay restriction rules
- Audit log - Configure and view log for the permitted domain.
 - Configuration - Configure the log settings for the permitted domain.
 - Log - View and export the log for the permitted domain.
- Report management - View and configure settings for periodical domain and quarantine summary reports for the permitted domain.
 - View - Only view the configured settings for periodical domain and quarantine summary reports for the permitted domain.
 - Change - View and configure settings for periodical domain and quarantine summary reports for the permitted domain.

Click the following links for more details.

- [Adding a new admin group](#)
- [Editing a admin group](#)
- [Deleting a admin group](#)
- [Making a admin group as default](#)

Adding a New Admin Group

- To add a new admin group and configure permission levels, click the 'Add' button.



A new admin group creating page will be displayed.

Dashboard / Admin groups & permissions

Admin groups & permissions ? Help

Name	Permission:
<input type="radio"/> Power Administrators (Default)	<input type="checkbox"/> All customer permissions
<input checked="" type="radio"/> <input type="text" value=""/>	<input type="checkbox"/> Add domain
	<input type="checkbox"/> Admin management
	<input type="checkbox"/> User permissions
	<input type="checkbox"/> Admin permissions
	<input type="checkbox"/> Report management
	<input type="checkbox"/> User session history view
	<input type="checkbox"/> View customer info
	<input type="checkbox"/> Locale
	<input type="checkbox"/> Change user limit per domain
	<input type="checkbox"/> Email template management
	<input type="checkbox"/> Audit log
	<input type="checkbox"/> All domain permissions
	<input type="checkbox"/> docteamcasg.comodo.od.ua

- Enter the name of the group in the text field under the 'Name' column and enable the permission levels in the right side required for that group.

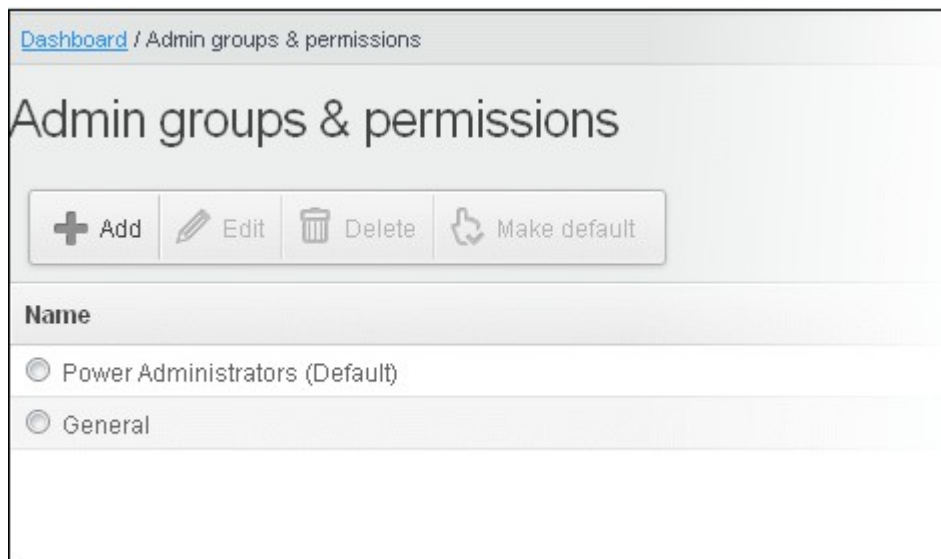
Dashboard / Admin groups & permissions

Admin groups & permissions ? Help

Name	Permission:
<input type="radio"/> Power Administrators (Default)	<input checked="" type="checkbox"/> All customer permissions
<input checked="" type="radio"/> General	<input checked="" type="checkbox"/> Add domain
	<input checked="" type="checkbox"/> Admin management
	<input checked="" type="checkbox"/> User permissions
	<input checked="" type="checkbox"/> Admin permissions
	<input checked="" type="checkbox"/> Report management
	<input checked="" type="checkbox"/> User session history view
	<input checked="" type="checkbox"/> View customer info
	<input checked="" type="checkbox"/> Locale
	<input checked="" type="checkbox"/> Change user limit per domain
	<input checked="" type="checkbox"/> Email template management
	<input checked="" type="checkbox"/> Audit log
	<input type="checkbox"/> All domain permissions
	<input type="checkbox"/> docteamcasg.comodo.od.ua

- Click the 'Save' button.

The newly created group will be displayed in the interface.

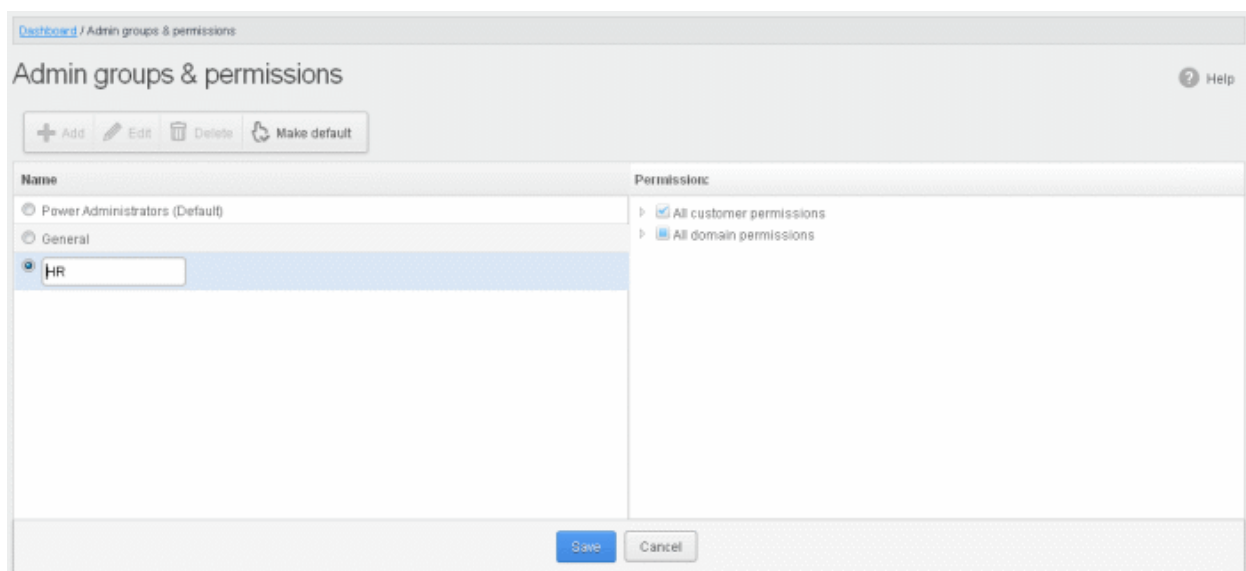


Now, administrators belonging to the account can be assigned to this newly created group. See the section '**Managing Permissions for Administrators**' in '**Administrators**' on how to add users to predefined groups.

Editing a Admin Group

You can edit the name of an existing group and / or change the permission levels.

- To edit an existing group, select the group from the list and click the 'Edit' button.

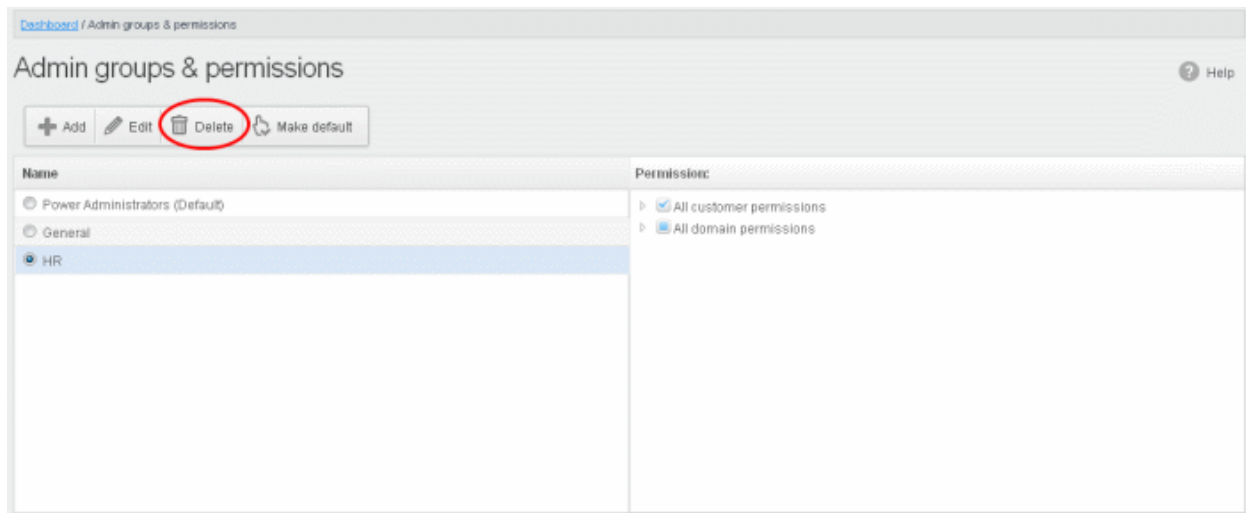


- Change the permission levels and / or the name of the group.
- Click the 'Save' button for the changes to take effect.

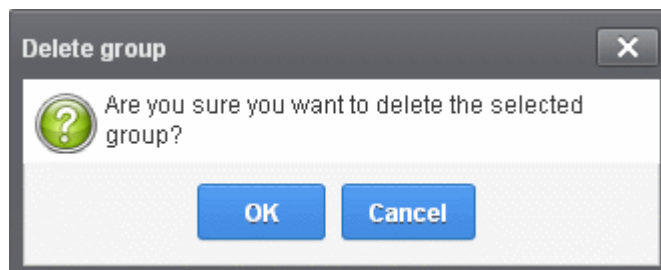
The admins in the group that is edited will be automatically reassigned to the edited group.

Deleting a Admin Group

- To delete a group, select it from the list and click the 'Delete' button.



- Click 'OK' in the confirmation dialog.



The selected group will be deleted from the list.

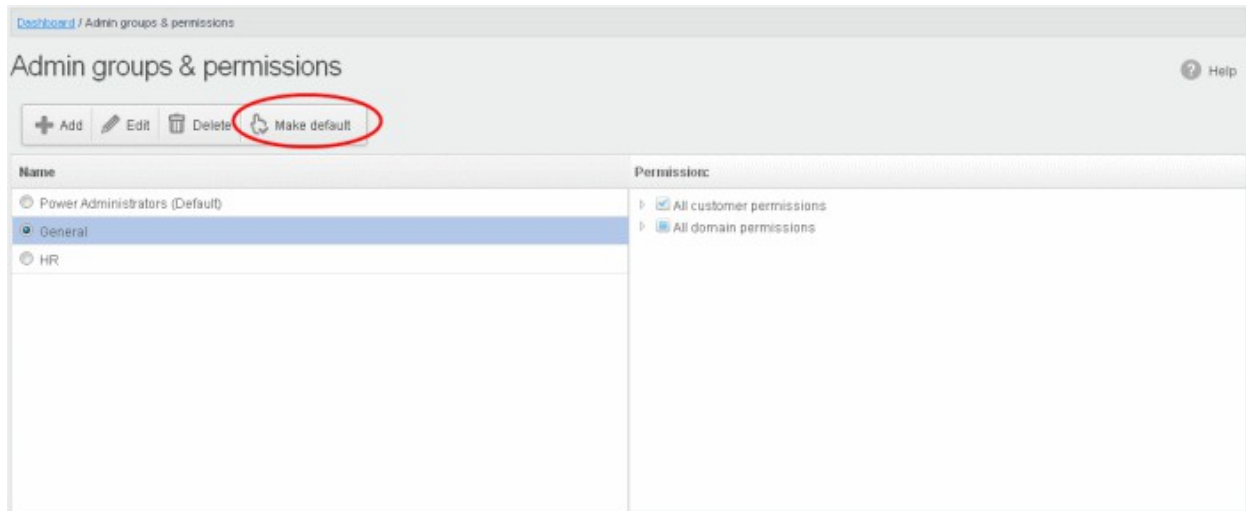
Note 1: If you delete a group, admins assigned to that group will be automatically moved to default group. You have to reassign the administrators if required.

Note 2: If you delete an admin group created by the administrator and marked as default, then the 'Power Administrator' group that was shipped with the product will be set as default. All the admins from the deleted group will be automatically migrated to the 'Power Administrator' group.

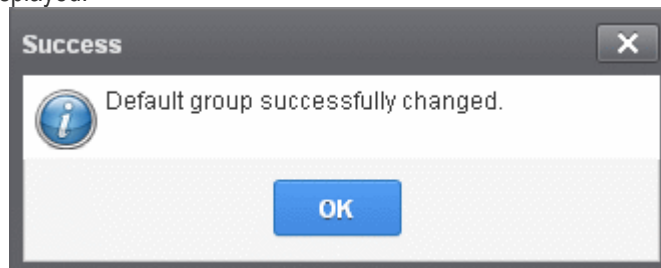
Making an Admin Group as Default

CASG allows administrators to make an existing group as a default group. Newly added administrators and administrators belonging to an existing group whose name was deleted will be automatically moved to this default group.

- To make an existing group as a default group, select it from the list and click the 'Make default' button.

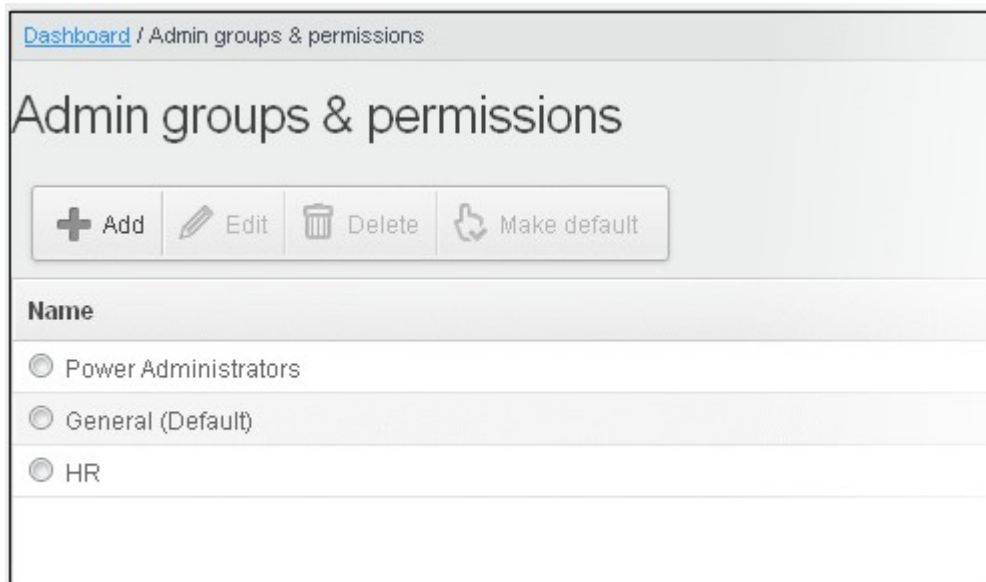


A success dialog will be displayed.



- Click 'OK'.

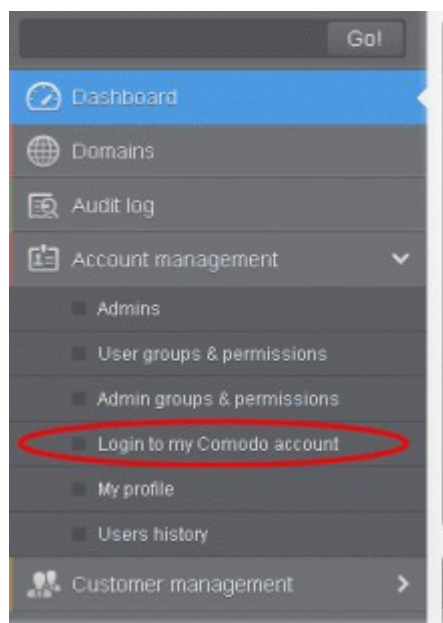
The selected group will be displayed as default group.



Note: If you delete an admin group created by the administrator and marked as default, then the 'Power Administrator' group that was shipped with the product will be set as default. All the admins from the deleted group will be automatically migrated to the 'Power Administrator' group.

3.2.3.4 My Comodo Account

This feature will be available in the 'Account management' tab if you have logged in to CASG using CAM account credentials.



Clicking the 'Login to my Comodo account' sub tab will take you to <https://accounts.comodo.com/login> page. From here you can...

- Add more subscriptions for CASG account
- Change your password
- Change contact information
- Sign up to other Comodo products

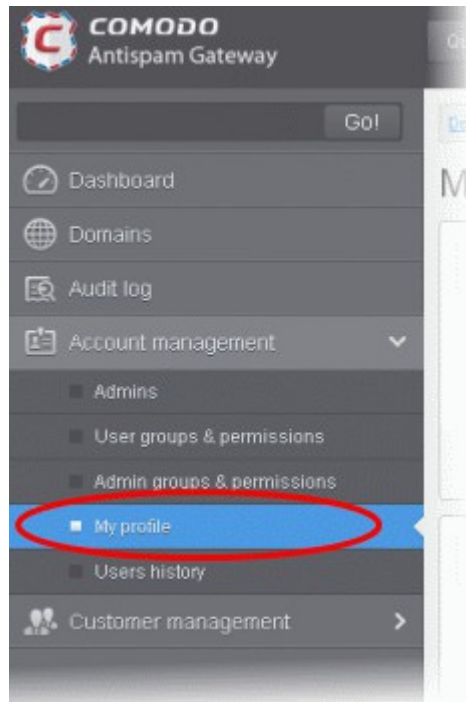
...and many more.

For more details on CAM account, visit our online website at help.comodo.com/topic-211-1-513-5907—Introduction-To-Comodo-Accounts-Manager.html.

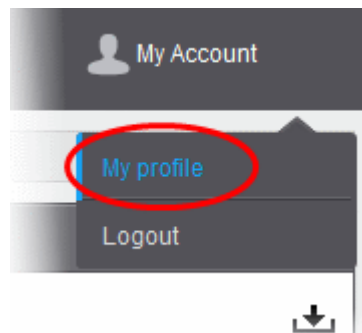
3.2.3.5 My Profile

The My Profile interface allows the currently logged-in administrator to change his / her login password to CASG as well as to change settings for idle session timeout and CASG notification email address.

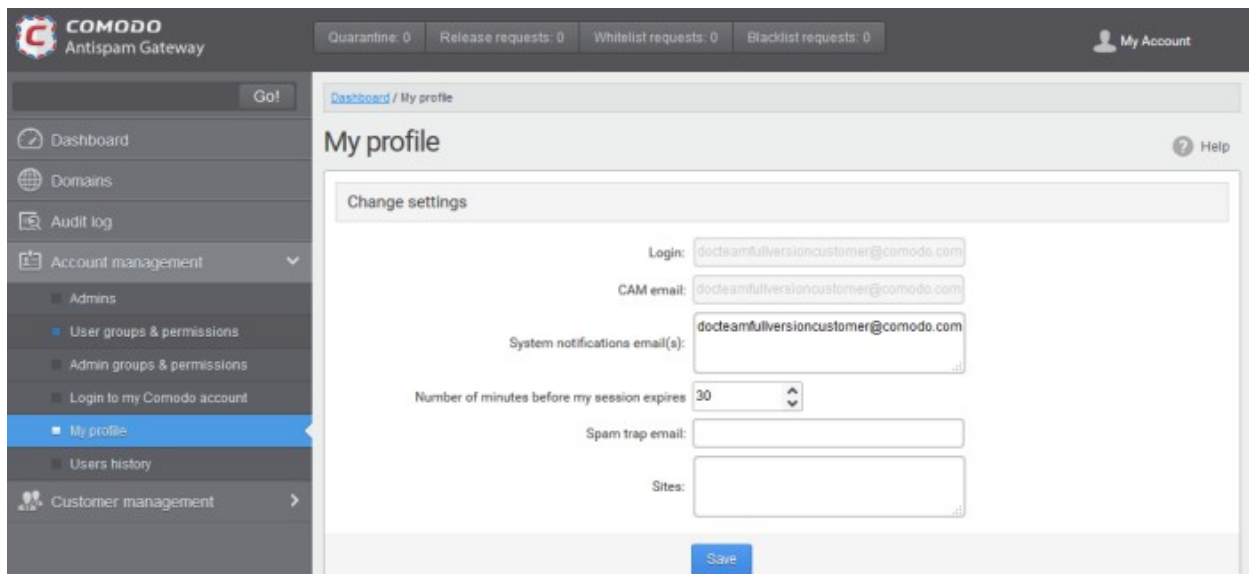
- Click the 'Account management' tab on the left hand side navigation to expand and then click the 'My profile' sub tab.



Alternatively, the My Profile interface can be accessed by clicking 'My Account' > 'My Profile' at the top right of the interface.



The My Profile interface will be displayed.



Note: The interface will vary depending on the login credential that you have used to access CASG. The password

can be changed after logging in to the CAM account.

Click the following links for more details:

- [Changing settings for idle session timeout and CASG notification emails](#)

3.2.3.5.1 Change Settings

The 'Change settings' area in the My Profile interface allows the currently logged-in administrator to configure various general settings.

To set idle session timeout and change system notifications email address

- Click the 'Account management' tab on the left hand side navigation to expand and then click the 'My profile' sub tab.

The 'Change settings' section will be displayed in the lower portion of the My Profile interface.

The screenshot shows a 'Change settings' form with the following fields and values:

- Login:** docteamfullversioncustomer@comodo.com
- CAM email:** docteamfullversioncustomer@comodo.com
- System notifications email(s):** docteamfullversioncustomer@comodo.com
- Number of minutes before my session expires:** 30
- Spam trap email:** (empty)
- Sites:** (empty)

A blue 'Save' button is positioned at the bottom center of the form.

- **Login** - Displays the user-name of the currently active user. Administrators can use this to log in to CAM to purchase additional licenses and renew existing licenses.
- **CAM email:** Displays the email address for the account as registered at Comodo Accounts Manager (CAM).
- **System notifications email(s)** - Enter the email addresses at which the new administrator should receive CASG notification emails. It can be the same email address as the login name and / or alternative email address(es) of up to a maximum of five. The quarantine requests from users, for blacklisting, whitelisting, or releasing quarantined emails and notifications such as of imports of users, local recipients and users via LDAP from CSV files will be sent to the email addresses specified in this field. Refer to the section **Email Management** for more details.
- **Number of minutes before my session expires** - You can set the idle session timeout period in the box. Enter the period in minutes or increase / decrease the period by clicking the up / down arrow. The valid entry is between 1 minute and 120 minutes. Please note this feature will not be available if an administrator is logged into CASG using CAM credentials.
- **Spam trap email** - (Optional) If you already have a special 'spam-trap' email address then please enter it here to further improve CASG message filtering.
- **Sites** - (Optional) Enter the URLs of all websites owned by your company in order to further improve spam filtering.

Click Save for your changes to take effect.

3.2.3.6 Users History

The 'Users History' area in 'Administrator Account Management' allows the administrators to view user history for all domains within a particular date range. You can filter users by IP address, last login, domain, username and/or location. By default, the most recent 15 records will be displayed.

Use of filters to create custom searches is covered in more detail [here](#).

3.2.4 Customer Management

The Customer Management area of CASG allows an administrator to view the details of the account they are logged into. The administrator configure subscriptions for the periodical Domain and Quarantine summary reports for domains; create an account; update the product and extend your license term. The administrator can also customize the 'support information' area in the notification emails that are generated for activities such as while adding a new user, password regeneration, quarantine request and quarantine report.

The screenshot shows the Comodo Antispam Gateway Administrator interface. The top navigation bar includes the Comodo logo, the text 'Antispam Gateway', and several status indicators: 'Quarantine: 0', 'Release requests: 0', 'Whitelist requests: 0', and 'Blacklist requests: 0'. A 'My Account' link is visible on the right. The left sidebar contains a 'Go!' button and a menu with items: Dashboard, Domains, Audit log, Account management, Customer management (expanded), End User License/Subscription Agreement (selected), License Management, Manage report subscriptions, System messages locale, and Email template settings. The main content area displays the 'End User License/Subscription Agreement' page. The page title is 'End User License/Subscription Agreement' with a 'Help' icon. Below the title, there is a section for 'Comodo AntiSpam Gateway 2' with a warning: 'THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS.' The main body of the agreement includes sections for '1. License', '1.1. Grant of License', '1.2. Restrictions', '1.3. Account', '1.4. Updates', and '1.5. Open Source And Third Party Licenses'.

Click the links for more details:

- [End user license agreements](#)
- [Viewing customer information](#)
- [Managing subscriptions for reports](#)
- [Configuring language for messages from CASG](#)
- [Notification email settings](#)

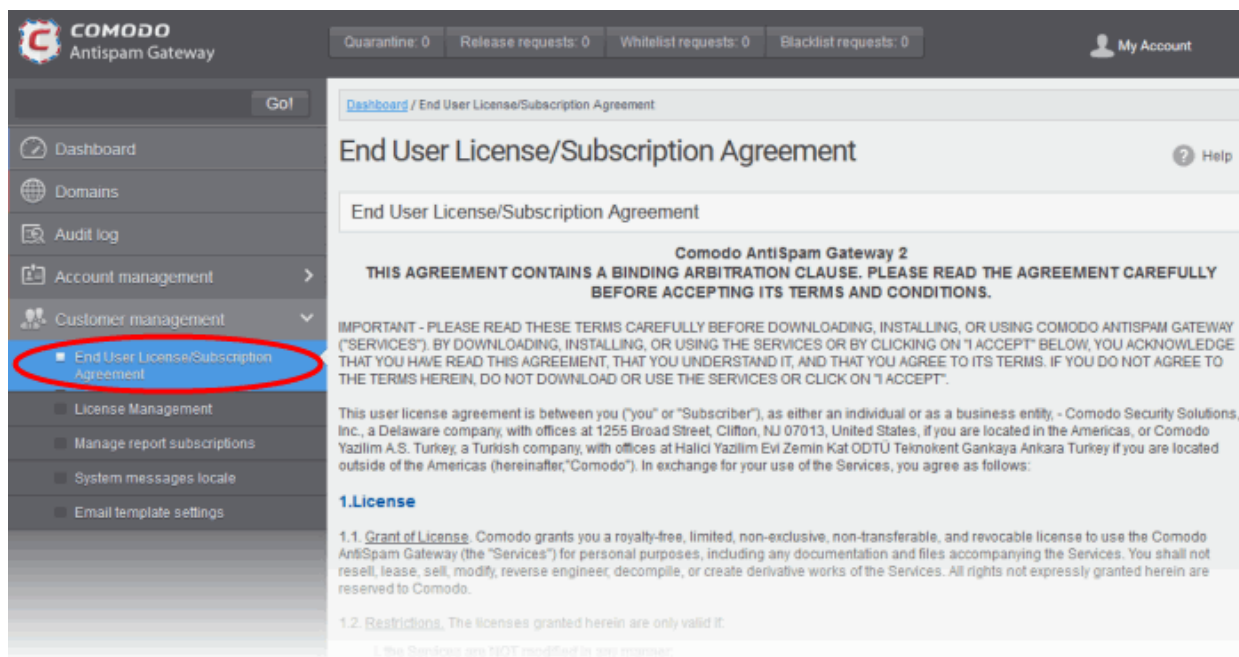
3.2.4.1 End User License and Subscriber Agreements

The 'End User License / Subscription Agreement' interface displays the complete Comodo Antispam Gateway End-User License and Subscriber Agreement.

To view End User License/Subscription Agreement

- Click 'Customer management' tab from the left hand side navigation to expand it and then click the 'End-User License/Subscriber Agreement.' tab from the sub menu.

The 'EULA/ Subscription Agreement' interface will be displayed:



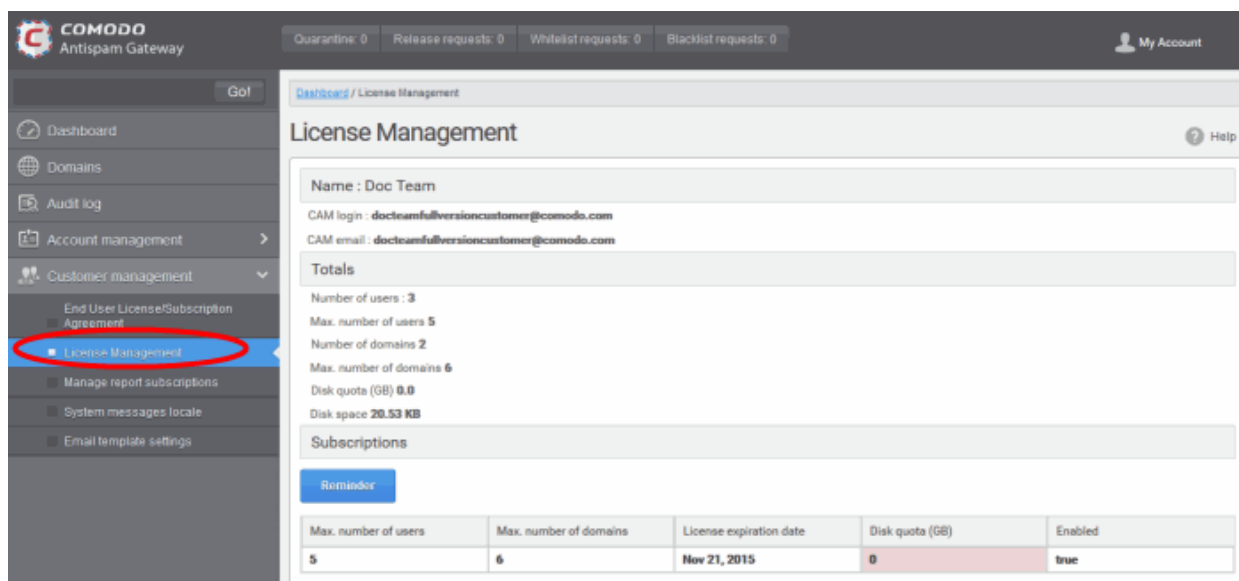
3.2.4.2 Viewing License Information

The License Management interface provides administrators with usage information.

To view the license management screen:

- Click 'Customer Management' on the left navigation then 'License Management'

The example below shows a customer with multiple licenses:



In the 'License Management' panel you will find the details of subscription(s) for your account. For multiple licenses, the number of users and domains that are allowed for all the licenses purchased will be added and displayed at the bottom most subscription column.

From the 'License Management' panel the administrator can get the details of subscription(s) for the CASG account. For multiple licenses, the number of users and domains that are allowed for all the licenses purchased will be added and displayed at the bottom most subscription column.

Name

- The name of the account is displayed at the Name title bar
- **CAM Login:** Displays the login user name for the account in Comodo Accounts Manager (CAM) at <https://accounts.comodo.com>. The administrator can use this login username to log in to CAM for purchasing additional licenses and renewal of existing licenses.
- **CAM email:** Displays the email address for the account as registered at CAM.

Totals

- **Number of Users:** Displays the total number of enrolled users belonging to all the domains.
- **Max. Number of Users:** The total number of users that can be added as per all the subscriptions made for the account, that is, number of users cannot exceed the number given in this field for all domains included.
- **Number of Domains:** Displays the number of domains enrolled for account.
- **Max. Number of Domains:** The total number of domains that can be added as per all the subscriptions made for the account.
- **Disk quota:** Displays the total storage space allotted in CASG server for archiving incoming messages as per all the subscribed packages, in GB.
- **Disk space:** Displays the storage space used by the archived mails in the CASG server.

Subscriptions

The following details are displayed for each subscription:

- **Max. Number of Users:** The maximum number of users that can be added to the account as per the subscription, that is, number of users cannot exceed the number given in this field for all domains included.
- **Max. Number of Domains:** The maximum number of domains that can be added as per the subscription.
- **License Expiration Date:** Displays the date till which the license is valid for the subscription.
- **Disk quota:** The maximum storage space allotted for mail archive in the CASG server, as per the subscription.
- **Enabled:** Displays whether the subscription is active or not.

The 'Reminder' button allows you to choose an email address to receive license expiry reminders, and to specify the period of time before expiry that you wish to receive them.

3.2.4.3 Manage Report Subscriptions

The Manage report subscriptions interface allows administrators to configure subscriptions to 'Domain' and 'Quarantine' summary reports of all enrolled domains. Refer to [CASG Reports - an Overview](#) for more details.

To access Manage report subscriptions interface

- Click Customer Management tab from the left hand side navigation to expand it and then click the 'Manage report subscriptions' tab from the sub menu.

The 'Manage report subscriptions' interface will be displayed:

The 'Report recipients' field will be auto-populated with the email addresses of all the administrators available for the account and enabled for the same, at the time of **adding them**. The report recipients can be added or removed from this interface by entering the administrator's email address or deleting them and clicking the 'Save' button at the bottom.

The administrator can configure the subscription for two types of reports from this interface:

- **Quarantine Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly, will contain a detailed statistics of the mails that are identified as spam or containing malicious content and moved to Quarantine of the domain automatically by CASG. Refer to **CASG Reports - An Overview** for more details.
- **Domain Report** - The periodical report which can be configured to be received hourly, daily, weekly or monthly, will contain a detailed statistics of number of users, mails that have been received at and sent from the domain, number of spams identified and blocked and so on. Refer to **CASG Reports - An Overview** for more details.

To configure the subscription of the reports

- You can expand/collapse a report configuration section by clicking on the respective strip.
- If you want the administrators to receive the periodical reports, select the 'Enabled' checkbox in the row of the respective report type. If both the reports are required, you can select both the checkboxes.
- Leave the 'Send empty' checkbox unchecked if reports without any statistics need not to be sent to recipients.
- Select the frequency at which the reports are to be sent to the administrators.

Quarantine Report

▼ 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: 2px;"> <input type="checkbox"/> 0 <input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 </div>	<input checked="" type="radio"/> Every day <input type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 </div>	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input type="checkbox"/> Thursday </div>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Nov 23, 2015 01:00	Next report for 243 day(s) from last run (2015-03-24 16:37)

- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that will be generated depending on the options chosen.

Domain Statistics Report

▼ Domain statistics report

Period	Hour	Day of month	Day of week	Send empty	Enabled	Start date	Report length
Weekly ▼	<input checked="" type="radio"/> Every hour <input type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 </div>	<input checked="" type="radio"/> Every day <input type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 </div>	<input type="radio"/> Every week day <input checked="" type="radio"/> Choose <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday </div>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Nov 23, 2015 00:00	Next report for 4 week(s) from last run (2015-03-24 16:37)

Save
Reset settings to default

- **Period** - Enables you to set the period to be covered in the report. The report will contain the statistics of all the domains in the account for the past one hour, one week, one month or one year, as selected from drop-down from the scheduled report time.
- **Hour** - The reports will be generated and sent to the administrators every hour or at the selected hour(s) of the day or date chosen from 'Day of month' or 'Day of week' columns.
- **Day of month** - The reports will be generated and sent to the administrators every day or on the specific day every month chosen at the hour selected from the 'Hour' column.
- **Day of week** - The reports will be generated and sent to the administrators every day or on the specific day every week chosen at the hour selected from the 'Hour' column.
- **Start date** - Displays the start date of the report generation depending on the options chosen (as per Greenwich Mean Time (GMT)).
- **Report length** - Displays the period of the report that will be generated depending on the options chosen.

- Click 'Save' for your settings to take effect.
- Clicking the 'Reset settings to default' button will disable both Quarantine and Domain statistics reports. The 'Report Recipients' field will not be cleared.

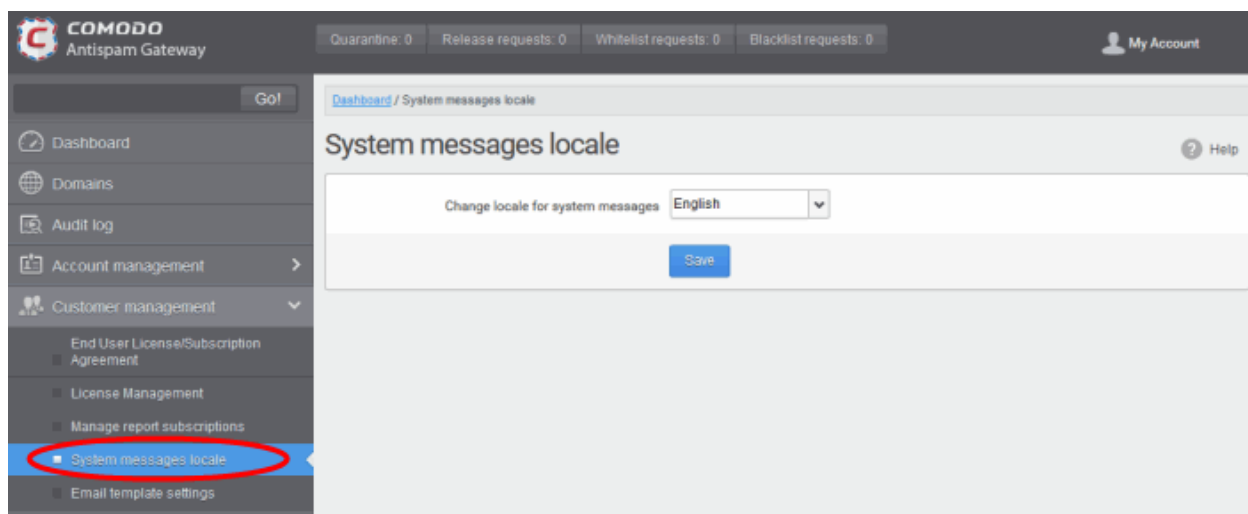
3.2.4.4 Configuring Language for Messages from CASG

The System messages locale interface accessible from the 'Customer management' configuration area of the dashboard allows the administrator to configure for the language of messages displayed and sent to the administrators of the domains by CASG, according to the location of the administrators.

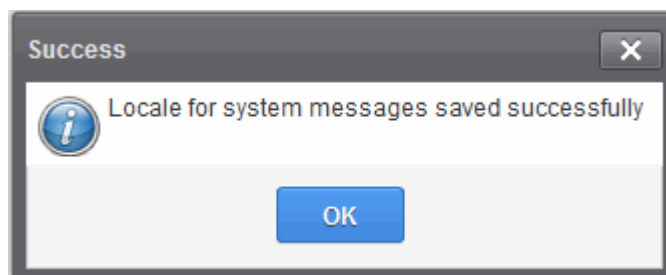
To configure for the language of messages

- Click 'System messages locale' tab from the left hand side navigation to expand it and then click the 'System messages locale' from the 'Customer management' drop-down menu in the menu bar.

The 'System messages locale' interface will be displayed.



- Select the language in which CASG should display and send its messages from the 'Change locale for system messages' drop-down. The messages will be displayed/sent in the selected language to the administrators of the domain managed by the currently logged in administrator.
- Click 'Save' for your settings to take effect.



3.2.4.5 Notification Email Settings

By default, all the notification mails sent to administrators and users on various events like adding a new user, password regeneration, quarantine request or periodical report mails like quarantine report will contain the links to the online help guide and Comodo support in the footer. The administrator can customize the footer for adding their contact and support information, from the Email template settings area.

To customize the notification emails

- Click 'Customer Management' tab from the left hand side navigation to expand it and then click the 'Email template settings' tab from the sub menu.

The 'Email template settings' interface will be displayed:

Please note the customization can be done only in html format.

- Select the check box 'Change default email footer' if you want to edit the details.
- Edit the details in html format as per your requirement and click the 'Save' button.
- Click the 'Reset to default' button to display Comodo support information in the notification emails.

4 CASG Reports - An Overview

Comodo Antispam Gateway can generate three kinds of periodical reports, Quarantine report, Domain statistics report and User import report, and send them to administrators and users as configured.

Reports are generated for account level and domain level:

1. Global reports for all domains covered by the customer account. See the section '**Managing Subscriptions for Reports**' under '**Customer Management**' for more details on customer level.
2. Domain level reports specific for each domain. See the section '**Manage Report Subscriptions for Selected Domain**' under '**Incoming**' section for reports on domain levels.

The reports for these types will be similar except the former will contain reports for all domains while the latter will contain reports for the selected domain. The reports will be sent routinely at the selected times, in the language set for the account.

CASG creates three kinds of reports:

- **Quarantine Report** - A statistical breakdown of mails identified as spam or malicious that were moved to quarantine by CASG. The report can be configured to be received hourly, daily, weekly or monthly.
- **Domain Statistics Report** - A comprehensive report which covers all mail activity for the domain. This includes information covering the number of users; mails that have been received at and sent from the domain; number of mail identified spam/malicious; number of mails blocked and so on. The report can be configured to be received hourly, daily, weekly or monthly by the administrator.
- **Users auto-import report** - The periodical report containing details of new users that were auto-imported into CASG for each domain, based on incoming mails received for them at the mail server. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. The user auto-import

reports are generated only for the domain level and not for the customer account level.

- **Quarantine Release Report** - The periodical report containing details of mails that were released from the quarantine list by both administrators and users with appropriate privileges. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. The quarantine release reports are generated only for the domain level and not for the customer account level.
- **Reported Spam Report** - A detailed report of mails that were reported as spam by administrators as well as users with appropriate privileges. The report also includes details of mails that were uploaded as spam to CASG. The report can be configured to be received hourly, daily, weekly or monthly by the administrator. The reported spam reports are generated only for the domain level and not for the customer account level.
- Reports can be enabled or disabled per administrator in **Dashboard > Account Management > Admin > Add Administrators** or **Edit Administrators**.

4.1 Quarantine Report

The Quarantine Report contains a list of mails that were identified as spam or containing malicious content and were moved to Quarantine automatically by CASG, with the details on sender, receiver, date and attachments. Clicking the subject line in the list will open the respective mail in a new CASG window.

- **Administrator**
 - **Domain Level** - The Report generated for an administrator will contain the details of the mails moved to quarantine of the selected domain.
 - **Customer Level** - The Report generated for an administrator will contain the details of the mails moved to quarantine of all the domains belonging to the account.
- **User** - The Report generated for a user will contain the details of the mails moved to quarantine of the user.

The report can be subscribed to be received hourly, daily, weekly or monthly for an administrator and daily, weekly or monthly for a user.

- **Hourly** - The reports will be generated and sent every hour to the administrators through email.
- **Daily** - The reports will be generated and sent daily to the administrators/user through email.
- **Weekly** - The reports will be generated and sent to the administrators/user through email on every seventh day from the start date set in the 'Start date' field. The report will contain details of the mails quarantined during the past seven days. The first report will be sent on the start date and will contain the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports will be generated and sent to the administrators/user through email on 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. The first report will be sent on the start date and will contain the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.

An example of a Quarantine report is shown below:



Here is the quarantine report for docteamcasg.comodo.od.ua from Apr 02, 2014 14:25 to Apr 11, 2014 00:00

Subject	From	To	CC (to docteamcasg.comodo.od.ua only)	Date	Size	
test_spam_email_1	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua		Wed Apr 02 14:26:40 GMT 2014	8.16 KB	
test_spam_email_2	John Smith <fiatlina@gmail.com>	demo2@docteamcasg.comodo.od.ua		Wed Apr 02 14:27:00 GMT 2014	8.18 KB	
Fw: We have free samples for you, now try before you buy @ your doorsteps!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Mon Apr 07 08:52:31 GMT 2014	3.02 KB	
Fw: We have free samples for you, now try before you buy @ your doorsteps!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Mon Apr 07 08:52:31 GMT 2014	3.02 KB	
Fw: FOLLOW THE INSTRUCTIONS !!	John Smith <fiatlina@gmail.com>	demo2@docteamcasg.comodo.od.ua, demo1@docteamcasg.comodo.od.ua		Wed Apr 09 04:31:41 GMT 2014	231.0 KB	
Fw: FOLLOW THE INSTRUCTIONS !!	John Smith <fiatlina@gmail.com>	demo2@docteamcasg.comodo.od.ua, demo1@docteamcasg.comodo.od.ua		Wed Apr 09 04:31:41 GMT 2014	231.0 KB	
Fw: Register and Get Rs. 5000 to Shop Now! Introducing Pepperfly.com - India's Largest Home and Furniture Online Store!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 04:32:36 GMT 2014	3.05 KB	
Fw: Register and Get Rs. 5000 to Shop Now! Introducing Pepperfly.com - India's Largest Home and Furniture Online Store!	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 04:32:36 GMT 2014	3.05 KB	
Fw: Get Rs. 25 assured recharge + chance to win an IPOD.	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 04:33:22 GMT 2014	3.98 KB	
Fw: Claim your exclusive rewards with the American Express Gold Card	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 08:33:00 GMT 2014	26.5 KB	
Fwd Fw: Send UNLIMITED Emails/Newsletter in Just Rs.2,500/mo. ZERO SETUP COST	John Smith <fiatlina@gmail.com>	demo1@docteamcasg.comodo.od.ua, demo2@docteamcasg.comodo.od.ua		Wed Apr 09 06:40:43 GMT 2014	2.3 KB	

Having Trouble? Support is here to help. Open a Ticket at <https://support.comodo.com> or call 1.888.COMODO (266.6361)

- Clicking on the 'Subject' link will open the respective mail in a new CASG window. You need to login to CASG to read the mail in the new window.

4.2 Domain Statistics Report

The Domain Statistics Report provides details on all the mail activities on the domain. This includes information covering the number of users; mails that have been received at and sent from the domain; number of mail identified spam/malicious; number of mails blocked and so on. The report can be configured to be received hourly, daily, weekly, monthly or yearly by the administrator.

- **Domain Level** - The Report generated for an administrator will contain only the details of domain statistics of the selected domain.
- **Customer Level** - The Report generated for an administrator will contain the details of domain statistics of all the domains belonging to the account.

Note: The Domain Statistics Report is available only to the administrators .

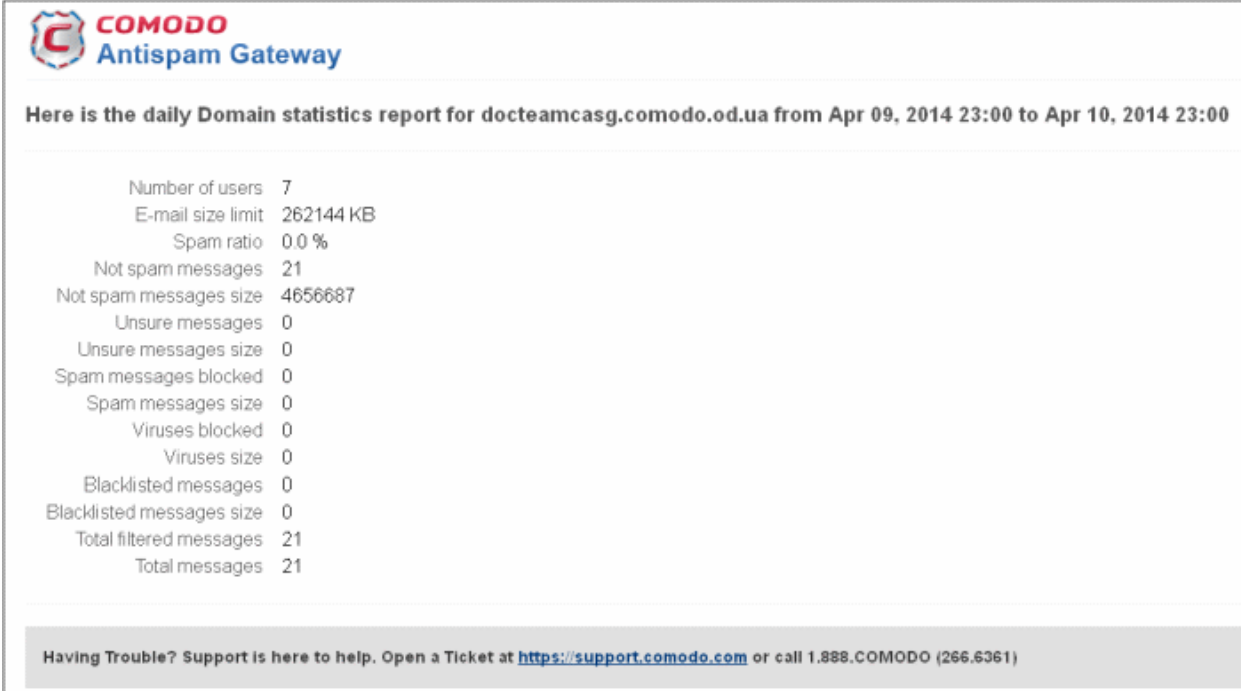
The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports will be generated and sent every hour to the administrators through email.
- **Daily** - The reports will be generated and sent daily to the administrators through email.
- **Weekly** - The reports will be generated and sent to the administrators through email on every seventh day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past seven days. The first report will be sent on the start date and will contain the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports will be generated and sent to the administrators through email on every 30th day

from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 30 days. The first report will be sent on the start date and will contain the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.

- **Yearly** - The reports will be generated and sent to the administrators through email on every 365th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 12 months. The first report will be sent on the start date and will contain the statistics for the remaining months of the year from the day of configuration and subsequently every 12 months.

An example of a Domain Statistics Report is shown below:



COMODO
Antispam Gateway

Here is the daily Domain statistics report for docteamcasg.comodo.od.ua from Apr 09, 2014 23:00 to Apr 10, 2014 23:00

Number of users	7
E-mail size limit	262144 KB
Spam ratio	0.0 %
Not spam messages	21
Not spam messages size	4656687
Unsure messages	0
Unsure messages size	0
Spam messages blocked	0
Spam messages size	0
Viruses blocked	0
Viruses size	0
Blacklisted messages	0
Blacklisted messages size	0
Total filtered messages	21
Total messages	21

Having Trouble? Support is here to help. Open a Ticket at <https://support.comodo.com> or call 1.888.COMODO (266.6361)

4.3 Auto-Imported Users Report

The Users Auto-Import Report provides details on all the new users belonging to a managed domain, that were automatically imported to CASG on receiving an incoming mail addressed to them at the mail server. The auto-imported users are sent with an invitation email containing login credentials for them to access the CASG user interface. For more details on managing auto-import, refer to the section **Managing User auto-import**.

Note: The user auto-import reports are generated only for the domain level and not for the customer account level. The Report is available only to the administrators .

The User Auto-Import Report contains the following details:

- Imported users count - The total number of users automatically imported into CASG for report time period.
- Enabled users count - The number of auto imported users that have activated their account by clicking the link in the invitation mail or logging-in to CASG using the credentials provided in the mail.
- Invited users count - The number of auto imported users that have been sent the invitation mails but yet to activate their account.
- User names list - The list of auto imported users.

An example of a Users Auto-Import Report is shown below:



Here is the users auto-import report for `csgqa.comodo.od.ua` from Nov 21, 2014 09:00 to Nov 21, 2014 10:00

Imported users count 1
Enabled users count 1
Invited users count 0
User names list admin

For help, see the Admin guide: <http://help.comodo.com/topic-157-1-288-3192-introduction-to-comodo-antispam-gateway.html>

Having Trouble? Support is here to help. Open a Ticket at <https://support.comodo.com> or call 1.888.COMODO (256.2608)

4.4 Quarantine Release Report

The 'Quarantine Release Report' provides details of mails that were released from quarantine by the administrators as well as by the users with appropriate privileges. This also includes quarantine release requests accepted by administrators.

Note: The quarantine release reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators .

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports will be generated and sent every hour to the administrators through email.
- **Daily** -The reports will be generated and sent daily to the administrators through email.
- **Weekly** - The reports will be generated and sent to the administrators through email on every seventh day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past seven days. The first report will be sent on the start date and will contain the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports will be generated and sent to the administrators through email on every 30th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 30 days. The first report will be sent on the start date and will contain the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.
- **Yearly** - The reports will be generated and sent to the administrators through email on every 365th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 12 months. The first report will be sent on the start date and will contain the statistics for the remaining months of the year from the day of configuration and subsequently every 12 months.

An example of a Quarantine Release Report is shown below:



Quarantine release report for csgqa4.comodo.od.ua from Jul 01, 2015 09:00 to Jul 01, 2015 10:00

Date	Operation description	Login	Role	Details
Wed Jul 01 09:18:32 GMT 2015	Release quarantined message	admin1@csgqa4.comodo.od.ua	admin	Recipients: user2@csgqa4.comodo.od.ua, user3@csgqa4.comodo.od.ua, user30@csgqa3.comodo.od.ua; Sender: test@test.com; Date: null; Subject: SPAM MAIL
Wed Jul 01 09:18:49 GMT 2015	Release quarantined message	admin1@csgqa4.comodo.od.ua	admin	Recipients: user2@csgqa4.comodo.od.ua; Sender: user12@test.com; Date: null; Subject: test mail from TELNET 16-04-15 16:41
Wed Jul 01 09:42:50 GMT 2015	Release quarantined message	user1@csgqa4.comodo.od.ua	user	Recipients: user1@csgqa4.comodo.od.ua; Sender: alravchenko@csg.comodo.od.ua; Date: null; Subject: test mail 15:47

For help, see the Admin guide: <http://help.comodo.com/topic-157-1-288-3192-introduction-to-comodo-antispam-gateway.html>

Having Trouble? Support is here to help, asgsupport@comodo.com or review the [Administrators Guide](#)

4.5 Reported Spam Report

The 'Reported Spam Report' provides details of mails that were reported as spam by the administrators as well as by the users with appropriate privileges. This also includes details of mails uploaded from the **Report Spam** interface.

Note: The reported spam reports are generated only for the domain level and not for the customer account level. The report is available only to the administrators .

The report can be subscribed to be received hourly, daily, weekly, monthly or yearly.

- **Hourly** - The reports will be generated and sent every hour to the administrators through email.
- **Daily** -The reports will be generated and sent daily to the administrators through email.
- **Weekly** - The reports will be generated and sent to the administrators through email on every seventh day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past seven days. The first report will be sent on the start date and will contain the statistics for the remaining days of the week from the day of configuration and subsequently every seven days.
- **Monthly** - The reports will be generated and sent to the administrators through email on every 30th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 30 days. The first report will be sent on the start date and will contain the statistics for the remaining days of the month from the day of configuration and subsequently every 30 days.
- **Yearly** - The reports will be generated and sent to the administrators through email on every 365th day from the start date set in the 'Start date' field. The report will contain details of the mail activities for the domains during the past 12 months. The first report will be sent on the start date and will contain the statistics for the remaining months of the year from the day of configuration and subsequently every 12 months.

An example of a Reported Spam Report is shown below:



Reported Spam report for csgqa4.comodo.od.ua from Jul 01, 2015 10:00 to Jul 01, 2015 11:00

Date	Operation description	Login	Role	Details
Wed Jul 01 10:06:38 GMT 2015	Report delivered message as spam	admin1@csgqa4.comodo.od.ua	admin	Recipients: user77@csgqa4.comodo.od.ua; Sender: Dagwood Bumpsted <avantistude@gmail.com>; Date: Wed Jul 01 10:01:10 GMT 2015; Subject: Fwd: Get instant Online Personal Loan approval and disbursal in 72 hours
Wed Jul 01 10:39:03 GMT 2015	Report delivered message as spam	user77@csgqa4.comodo.od.ua	user	Recipients: user77@csgqa4.comodo.od.ua; Sender: Dagwood Bumpsted <avantistude@gmail.com>; Date: Wed Jul 01 10:01:10 GMT 2015; Subject: Fwd: Get instant Online Personal Loan approval and disbursal in 72 hours
Wed Jul 01 10:41:54 GMT 2015	Reports archived message as a Spam	user77@csgqa4.comodo.od.ua	user	Recipients: user77@csgqa4.comodo.od.ua; Sender: dagwood bumpsted <avantistude@gmail.com>; Date: Wed Jul 01 10:40:56 GMT 2015; Subject: Fwd: Zero Fees, Attractive Interest Rates and Loans upto 25L
Wed Jul 01 10:52:02 GMT 2015	Reports archived message as a Spam	user77@csgqa4.comodo.od.ua	user	Recipients: user77@csgqa4.comodo.od.ua; Sender: oxford morris minor <mmoxford@yahoo.com>; Date: Wed Jul 01 10:47:33 GMT 2015; Subject: Dr. Jones wake up now
Wed Jul 01 10:55:26 GMT 2015	Reports archived message as a Spam	user2@csgqa4.comodo.od.ua	user	Recipients: user1@csgqa4.comodo.od.ua, user2@csgqa4.comodo.od.ua; Sender: oxford morris minor <mmoxford@yahoo.com>; Date: Wed Jul 01 10:52:00 GMT 2015; Subject: Fw: Dr. Jones wake up now
Wed Jul 01 10:55:52 GMT 2015	Reports archived message as a Spam	user2@csgqa4.comodo.od.ua	user	Recipients: user1@csgqa4.comodo.od.ua, user2@csgqa4.comodo.od.ua; Sender: oxford morris minor <mmoxford@yahoo.com>; Date: Wed Jul 01 10:52:00 GMT 2015; Subject: Fw: Dr. Jones wake up now

Appendix 1 - CASG Error Codes

The most common error codes for CASG are given below:

Error Code	Description
1	Unknown error
100	Import exception
101	Wrong format
102	Wrong outgoing user format IP password. If 'password' is empty then 'username' must be IP address.
103	Communication exception
200	User limit exception
300	Spam engine exception
1000	Customer has no domains
1001	Domains mismatch
1002	Alias already exists
1003	User already exists

Appendix 2 - CASG Comparison Table

Features	Paid Version	Free Version
Number of domains and incoming / outgoing users	Depends on the subscription	5 users and 1 domain
Number of domain aliases	5	Nil
Active Directory / LDAP Synchronization	✓	✗
Create / Modify User Groups	✓	✗
Assign permissions to User Groups	✓	✗
Number of user aliases per user	5	Nil
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	✓	✓
Force Retry (Force Deliver) selected or all 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	1
Report management	✓	✗

Appendix 3 - Troubleshooting LDAP

This section explains how to resolve some common problems that may arise when configuring LDAP.

For full details on working with LDAP, <http://help.comodo.com/topic-157-1-288-5720-Importing-Users-from-LDAP.html>

- **Problem: Unhandled Exception:**

Solution: The exception was not classified.

- **Problem: Size limit exceeded, unable to extract more then users from server. Size limit must be increased on server side or specify more strict query**

Solution: Active Directory server has limitation on the number of search entries which may be iterated during querying. By default, Microsoft Active Directory allows only 1000 search entries. If the server received more than that, the administrator should override the default LDAP search size limit in the Active Directory, or use more strict query

- **Problem: Incorrect filter settings:**

Solution: Filter settings contain incorrect format or AD server doesn't support it.

- **Problem: Incorrect BaseDN settings: ...**

Solution: BaseDN value has incorrect format.

- **Problem: Unable to connect with provided host in BaseDN settings: ...**

Solution: Provided domain name for BaseDN setting cannot be resolved in AD forest tree. Assure a domain name is correct.

- **Problem: Unable to resolve LDAP referral, host unreachable. Users had found before referral might be imported. Possible solution is to use Global Catalog server (port 3268/3269 as default) to avoid resolving referrals.**

Solution: CASG is trying to extract as much as possible information and following referrals to resolve all search entries in a query. If the URL in the referral is unreachable by CASG then the iteration will stop. Only partial result will be provided. That occurs when an administrator uses a private domain and it cannot be accessed with only domain name (the referral contains the list of URLs of the explicit domain names but the information about servers located in the private subnet is absent). To avoid the referrals occurrence in search entries use the Global Catalog server for querying. By default, the port for this server is 3268/3269 and that depends on whether the SSL enabled or not.

- **Problem: Unknown error. Users found before error might be imported. Original exception - ...**

Solution: Search entries has been terminated within the replication process. Please contact support to find a solution.

- **If you do not know your BaseDN, here's a step-by-step guide to determining your BaseDN.**

Most organizations follow a similar convention for their determined BaseDN when the organization sets up its Active Directory. For a company with the domain of example.com, the typically BaseDN is **cn=Users,dc=example,dc=com**

Appendix 4 - Useful Links

This page contains links to external webpages which provide detailed explanations of LDAP features.

What Is the Global Catalog?

<http://technet.microsoft.com/en-us/library/cc728188%28v=ws.10%29.aspx>

Global Catalog and LDAP Searches

<http://technet.microsoft.com/en-us/library/cc978012.aspx>

LDAP Referrals

<http://technet.microsoft.com/en-us/library/cc978014.aspx>

Click the following links for more details <http://help.comodo.com/topic-157-1-288-5720-Importing-Users-from-LDAP.html>

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ, 07013

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: EnterpriseSolutions@Comodo.com